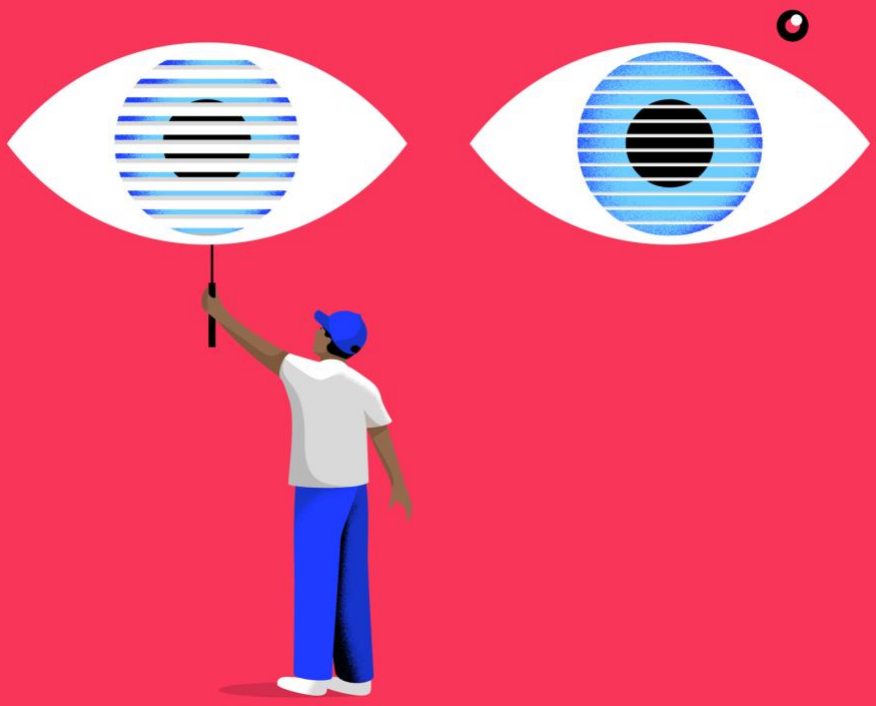
# Approaches to children's data protection

A comparative international mapping



5RIGHTS FOUNDATION

**About 5Rights Foundation**

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change, and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses and children, so that digital products and services can impact positively on the lived experiences of young people.

## Foreword

Personal data drives our digital economies. It can open doors and build connections, but it also can be exploited or misused. Privacy laws have provided a bulwark against careless or malicious actors for more than twenty years now. Only recently, however, have we seen laws designed around the special vulnerabilities of young people.

Two years ago, we had the pleasure of working together to develop and introduce the world's first law for children's data protection, grounded in the EU General Data Protection Regulation. The UK Age Appropriate Design Code (AADC) consists of 15 enforceable standards. Taken together, they hold tech companies accountable for children's experiences on their platforms. Under the Code, firms cannot use children's data in ways known to cause damage, such as by recommending harmful content or sharing profiles with strangers. At its core, the Age Appropriate Design Code mandates that companies put the interests of children first, by design and by default.

Within months of the Code coming into effect, the big names in tech made positive changes. Instagram banned adults from messaging children. It also turned off location tracking and introduced prompts that encourage children to take breaks from scrolling. Google made SafeSearch the default browsing mode for children and turned off YouTube's autoplay function. TikTok recently made accounts for those under 16 years private by default.

Reasonable, even obvious modifications like these are long overdue. And they have yet to be implemented universally.

This looks set to change sooner rather than later. In September 2022, the California Age Appropriate Design Code was signed into law, making the same set of principles enforceable in the home State of Silicon Valley and on both sides of the Atlantic. Ireland's Data Protection Commission also finalised its Fundamentals, which are "entirely consistent" with the AADC, as is the Dutch Code for Children's Rights. France and Sweden have produced guidelines based on the same fundamental principles.

With discussions at the EU level and interest from other US states well as countries around the world, we now have the opportunity to set a global standard for regulating tech towards children's privacy, safety, and autonomy in the digital realm. Such a standard should codify children's existing rights while showing data protection's potential at its best: a forward-thinking innovative driver for proportionate protections that enhance society's engagement with the digital world.

Coordination is key. Taking different approaches could slow down or even undermine the whole effort. Different standards could create regulatory loopholes that firms might exploit. Further, tech companies who adopt privacy respectful processes deserve a straightforward set of expectations, irrespective of where they or their users may be.

Establishing coherent global regulation will close loopholes and make compliance easy for an industry that will never be constrained by national borders. By setting out the common underlying principles of existing regulations for children's data protection, this paper aims to provide a practical contribution to this goal.

We must act urgently and thoughtfully. Most importantly, it is only by acting together that we will build the digital world young people deserve.

*Baroness Beeban Kidron*
*Founder of 5Rights Foundation*

*Elizabeth Denham*
*Trustee, 5Rights Foundation & Former Information Commissioner UK*

## Introduction

Data drives many norms of the digital world, and the way children's data are collected, processed and shared impacts every aspect of their online experience. The EU General Data Protection Regulation (GDPR)[1] stipulates that "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" (Recital 38), reflecting the vulnerabilities associated with their age and developmental capacities, as well as their established rights. The adoption of the GDPR in 2016 set a new global norm and has influenced regulatory reform and inspired new laws around the world.

The European Data Protection Board (EDPB) has developed a series of Guidelines on specific aspects of GDPR, including as regards the protection of children's data. Guidelines 05/2020 detail conditions for the provision of consent for the processing of children's data to be "lawful".[2] A range of further Guidelines consistently reiterate the need to apply additional safeguards for children, for example, as concerns dark patterns,[3] the targeting of social media users[4] and data protection by design and default.[5] What these additional safeguards should be and how, more broadly, GDPR should be interpreted in light of the established legal rights and needs of children is yet to be specified at the EU level. However, a number of European Data Protection Authorities (DPAs) and other authorities have drafted guidelines for children's data protection, inspiring similar efforts around the world, including in Australia and the United States.

These initiatives come as a broader international policy and regulatory landscape governing children's rights in the digital environment takes shape, providing critical guidance.

This paper aims to provide a practical baseline for any further regulatory work on children's data protection work, notably under GDPR.

It presents an overview of the international policy landscape for children's rights in the digital environment (section I); it then compares and contrasts the leading approaches to children's data protection, looking at GDPR-based initiatives (section II) as well as select initiatives from outside of GDPR's remit (section III). The final section provides a practical overview of the key common underlying principles of current international best practices for children's data protection based on GDPR (section IV).

[1] General Data Protection Regulation, 2016
[2] Guidelines 05/2020 on consent under Regulation 2016/679
[3] Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them
[4] Guidelines 10/2020 on restrictions under Article 23 GDPR; Guidelines 08/2020 on the targeting of social media users
[5] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

# Contents

## Children's rights underpinnings for regulatory policy in the digital environment

Children's rights are established in the 1989 United Nations Convention on the Rights of the Child (UNCRC) and elaborated as regards the digital environment in UNCRC General comment No. 25. The Convention codifies children's rights around four key principles: non-discrimination; the best interests of the child; the right to life, survival and development; and respect for the views of the child.[6] These rights for all under 18s are recognised as underpinning EU law, and the key principles of the UN Convention are reflected also in the EU Charter of Fundamental Rights, which states that: "Children shall have the right to such protection and care as is necessary for their well-being"; and that: "In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration."[7]

### a. UNCRC General comment No. 25 on children's rights in relation to the digital environment[8]

In 2021, the UN Committee on the Rights of the Child adopted General comment No. 25[9] setting out how the Convention applies in the digital environment.

> Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention.
>
> *UNCRC General comment No. 25 (para 69)*

General comment No. 25 calls on State parties to "require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services 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 services" (para 39); as well as to "require the business sector to undertake child rights due diligence, in particular, to carry out child rights impact assessments and disclose them to the public" (para 38).

General comment No. 25 warns against the misuse of children's data, including for commercial exploitation (para 103). It specifies that "any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or

[6] United Nations Convention on the Rights of the Child, 1989
[7] Article 24, EU Charter of Fundamental Rights
[8] UNCRC General comment No. 25 on children's rights in relation to the digital environment, 2021
[9] General comments provide interpretation and analysis of specific articles of the Convention on the Rights of the Child or deal with thematic issues related to the rights of the child. General comments – drafted following consultation with all UN Member States, experts and other stakeholders and adopted by the Committee on the Rights of the Child by Consensus – constitute an authoritative interpretation as to what is expected of States parties as they implement the obligations contained in the Convention.

without the child's knowledge [...] and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose" (para 75).

The General comment also prioritises data protection and privacy-by-design to ensure that commercial interests do not take precedence over the best interests of the child:

> Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritise commercial interests over those of the child.
>
> *UNCRC General comment No. 25 (para 110)*

### b. Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment[10]

The 2018 Council of Europe Guidelines call on States to "ensure that the likely impact of intended data processing on the rights of the child is assessed and that the data processing is designed to prevent or minimise the risk of interference with those rights" (para 31).

> In relation to the processing of children's personal data, States should implement, or require relevant stakeholders to implement, privacy-by-default settings and privacy-by-design measures, taking into account the best interests of the child. Such measures should integrate strong safeguards for the right to privacy and data protection into devices and services.
>
> *Council of Europe Guidelines (para 35)*

The Guidelines equally call for the prohibition by law of the profiling of children, except when in the best interests of the child (para 37).

When "children are considered to be capable of consenting to the processing of personal data, their rights, views, best interests and evolving capacities must be taken into consideration. This should be monitored and evaluated while taking into account children's actual understanding of data collection practices and technological developments" (para 30).

[10] 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, 2018

### c. Report of the UN Special Rapporteur on the right to privacy: Artificial intelligence and privacy, and children's privacy[11]

The 2021 report on children's privacy of the UN Special Rapporteur on the right to privacy reiterates the requirement for high levels of privacy by design and default for children.

The report stresses the limitations of consent – whether by a child or parent – and the principle of the best interests of the child: "Consent [...] neither necessarily expresses a child's autonomy nor protects it, particularly where power imbalances exist. Furthermore, parental consent may not always be in the best interests of the child or aligned to the child's views" (para 120).

It echoes the Council of Europe ban on profiling of children (para 127(b)).

It also expresses concerns regarding parental surveillance and calls for more research on parental monitoring norms and their effects on child development (para 128 (c)).

While recognising the strengths of GDPR, the Rapporteur calls for the EU Regulation to better protect children's data, counselling that:

> [T]he general elements of data protection by design, privacy by default, the right not to be subject to automated individual decision-making (art. 22) and data protection impact assessments are worthy of wider application for protecting the personal data of children.
>
> *Report of the UN Special Rapporteur on the right to privacy (para 121)*

### d. OECD Recommendation on Children in the Digital Environment[12] and Guidelines for Digital Service Providers[13]

In 2012 the OECD adopted a Recommendation on children in the digital environment, which called for the bests interests of the child to be upheld as a primary consideration and for the adoption of measures that provide for age-appropriate child safety by design.

In 2021 additional Guidelines specified that Digital Service Providers should take "a precautionary approach" to ensuring children's rights and safety, "including through taking a safety-by-design approach to addressing risk".

Specifically, regarding children's privacy and data protection, the Guidelines state as follows:

> If providing digital services that are for children, or where it is reasonably foreseeable children will access or use them, and that collect, process, share, and use personal data, Digital Service Providers should:

[11] Report of the Special Rapporteur on the right to privacy, 2021
[12] Recommendation of the Council on Children in the Digital Environment, 2012
[13] OECD Guidelines for Digital Service Providers, 2021

> Provide children, and their parents, guardians, and carers, with information on the way that their personal data is collected, disclosed, made available, or otherwise used in language that is concise, intelligible, easily accessible, and set out in a clear and age-appropriate manner;
>
> Limit the collection of personal data and its subsequent use or disclosure to third parties to the fulfilment of the provision of the service in the child's best interests;
>
> Not use children's data in ways evidence indicates is detrimental to their wellbeing; and
>
> Unless there is a compelling reason to do so and there are appropriate measures in place to protect children from harmful effects, not allow the profiling of children or automated decision- making, including on e-learning platforms.
>
> *OECD Guidelines for Digital Service Providers*

Regarding governance and accountability: "Digital Service Providers should have policies and procedures in place to promote the best interests of all children accessing their services. Digital Service Providers should be able to demonstrate compliance with any domestic policies, regulations, or laws in place to safeguard the rights of children in the digital environment."

### e. Council of Europe Strategy on the Rights of the Child[14]

The 2022 Council of Europe Strategy on the Rights of the Child invites "business and industry to fulfil their responsibilities towards children, including by undertaking child impact assessments, ensuring the participation of children in the assessment stages, as well as involving them in the design of digital services and products" (3.2.1) and notes the relevance of the "4Cs" approach with regard to risks including to children's data protection (3.1.1).[15]

### f. EU Strategy on the rights of the child[16]

The 2022 EU Strategy on the Rights of the Child, for the first time, included a chapter on the digital environment. The Strategy noted that: "On data protection and privacy rules, children advocate for companies to develop understandable privacy policies for digital services and applications and ask to be involved in the design and development of new digital products they will use."

The Strategy calls on ICT companies to:

[14] Council of Europe Strategy on the Rights of the Child, 2022
[15] Sonia Livingstone & Mariya Stoilova, Children Online: Research and Evidence, https://core-evidence.eu/updating-the-4cs-of-online- risk/
[16] EU Strategy on the rights of the child, 2022

Ensure that children's rights, including privacy, personal data protection, and access to age-appropriate content, are included in digital products and services by design and by default, including for children with disabilities;

Equip children and parents with adequate tools to control their screen time and behaviour, and protect them from the effects of overuse of and addiction to online products.

*EU Strategy for the Rights of the Child 2022-2027*

### g. UNICEF Manifesto for Better Governance of Children's Data[17]

Published in 2021, UNICEF's Manifesto is aimed at encouraging governments and businesses to address children's rights in data governance frameworks. It contains ten principles for preventing the misuse of children's data and the violation of their UNCRC rights:

#### 10 Principles of the UNICEF Manifesto

The international community must consider these actions when developing and implementing data governance frameworks.

1. PROTECT children and their rights through child-centred data governance. Such data governance should adhere to internationally agreed standards that minimise the use of surveillance and algorithms for profiling children's behaviour.
2. PRIORITISE children's best interests in all decisions about children's data. Governments and companies should give priority to children's rights in their data collection, and processing and storage practices.
3. CONSIDER children's unique identities, evolving capacities and circumstances in data governance frameworks. Every child is different and children mature as they get older, so data governance regulations must be flexible. Marginalised children must never be left behind.
4. SHIFT responsibility for data protection from children to companies and governments. Extend the protection measures to all children below the age of 18, regardless of the age of consent.
5. COLLABORATE with children and their communities in policy building and management of their data. Through distributed models of data governance, children and their communities should have more say in how data is processed, by whom it can be processed, and with whom it can be shared.
6. REPRESENT children's interests within administrative and judicial processes, as well as redress mechanisms. It is imperative that children's rights are integrated into existing mechanisms, such as the work of data protection authorities.

[17] The Case for Better Governance of Children's Data: A Manifesto, UNICEF, 2021

7. PROVIDE adequate resources to implement child-inclusive data governance frameworks. Data protection authorities and technology companies must employ staff who understand children's rights, and governments should allocate funding for regulatory oversight.
8. USE policy innovation in data governance to solve complex problems and accelerate results for children. Policy innovation can help public authorities to make the most of data, while at the same time safeguarding children's rights.
9. BRIDGE knowledge gaps in the realm of data governance for children. There are some urgent knowledge gaps that need further research to ensure that data governance regulations are evidence-based.
10. STRENGTHEN international collaboration for children's data governance and promote knowledge and policy transfer among countries. This Manifesto calls for greater global coordination on law and policy. Uncoordinated national-level data governance laws can lead to competing assertions of jurisdiction and conflict.

*UNICEF Manifesto for Better Governance of Children's Data*

### h. Global Privacy Assembly Resolution on Children's Digital Rights[18] [19]

Data protection authorities meeting under the aegis of the Global Privacy Assembly in October 2021 unanimously adopted a Resolution submitted by the French CNIL and the Italian Garante, and initially co-sponsored by 21 authorities worldwide. The Resolution reiterates key elements of the UNCRC General Comment No. 25, among others calling on States to:

- Prohibit practices aimed at manipulating children or influencing their behaviors in ways which may be against their best interests.
- Prohibit the use or transmission to third parties of children's data for commercial or advertising purposes and the practice of marketing techniques that may encourage children to provide personal data.

The Resolution states that online services providers should integrate the promotion of the best interests of the child and respect for children's rights into the design of services: tracking must be off by default and, where necessary, must not be systematic or carried out without the knowledge of the child; age assurance mechanisms must be proportionate to risk and privacy-preserving; service providers should refrain from profiling children on the basis of a digital record of their actual or presumed characteristics for commercial purpose.

[18] Global Privacy Assembly Resolution on children's digital rights, 2021

> Online service providers should integrate the promotion of the best interests of the child and respect for children's rights into the design of services: in this sense, they should provide for the use of privacy impact assessments, children's rights impact assessments, data encryption solutions, easy-to-understand and easy-to-use privacy settings and default settings that offer the highest protection of children's personal data, and in particular the deactivation by default of certain options, such as geolocation and profiling; and they should also consult with children, parents, or child advocates during the development of their services.
>
> *Global Privacy Assembly Resolution on Children's Digital Rights*

The Resolution also calls for services to be accessible and understandable to children, for educational resources to boost the exercise by children and guardians of the rights of the child, as well as appropriate complaints and redress mechanisms.

## Legislative and policy initiatives for children's data protection based on GDPR

Since the UK's Information Commissioner's Office began work in 2018 on the Age Appropriate Design Code (AADC), a number of DPAs and other authorities have drafted guidance for children's data protection based on GDPR, generally following extensive consultation also with children. This section reviews the main elements of these initiatives in the order of their publication. With the exception of the AADC, which is a regulatory code, they have the status of policy guidance.

### a. UK Age Appropriate Design Code[20]

The Age Appropriate Design Code (AADC) was signed into law in 2020 and came into force in 2021. The statutory Code, enforced by the Information Commissioner's Office, has three conceptual underpinnings:

- Firstly, children must be afforded protections wherever they are online, not only on services specifically designed for them. Services in scope are those 'likely to be accessed by children – where the presence of a child on that service is 'more probable than not' or could be 'reasonably expected'.
- Secondly, a child is defined as a person under 18, as per Article 1 of the United Nations Convention on the Rights of the Child.[21] The Code is clear that data protection rules should reflect the evolving capacities of children as they develop: protections for a 5-year-old do not need to be the same as those for a 17-year-old. It also acknowledges that children of all ages should be afforded privacy suitable for their age.
- Thirdly, products and services in scope of the AADC must consider the privacy and protection of children by design and default.

**15 Standards of the Age Appropriate Design Code**

1. BEST INTERESTS OF THE CHILD: The best interests of the child should be a primary consideration when designing and developing online services likely to be accessed by a child.
2. DATA PROTECTION IMPACT ASSESSMENTS: Services must undertake a data protection impact assessment to assess and mitigate risks to the rights and freedoms of children which arise from those services' data processing.
3. AGE-APPROPRIATE APPLICATION: Services must take a risk-based approach to recognise the age of individual users. They must either establish age with a level of certainty that is appropriate to the risks or apply the standards to all users.

[20] Age Appropriate Design Code, Information Commissioner's Office, 2020
[21] United Nations Convention on the Rights of the Child, 1989

4. TRANSPARENCY: The privacy information provided to users, and other published terms, policies, and community standards, must be concise, prominent and in clear language suited to the age of the child.
5. DETRIMENTAL USE OF DATA: Services must not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or government advice.
6. POLICIES AND COMMUNITY STANDARDS: Services must uphold their own published terms, policies, and community standards.
7. DEFAULT SETTINGS: Settings must be "high privacy" by default, unless there is a compelling reason for a different default setting, taking account of the best interests of the child.
8. DATA MINIMISATION: Only the minimum amount of personal data needed to provide the elements of a service in which a child is actively and knowingly engaged should be collected and retained.
9. DATA SHARING: Children's data must not be disclosed unless there is a compelling reason to do so, taking account of the best interests of the child.
10. GEOLOCATION: Geolocation options must be switched off by default.
11. PARENTAL CONTROLS: Services must give age-appropriate information to children about parental controls. If the service allows a parent or carer to monitor their child's online activity or track their location, it must provide an obvious sign to the child when they are being monitored.
12. PROFILING: Profiling options must be switched "off" by default. Profiling is only permissible if there are appropriate measures in place to protect the child from any harmful effects.
13. NUDGE TECHNIQUES: Nudge techniques must not be used to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.
14. CONNECTED TOYS AND DEVICES: Connected toys or devices must include effective tools to comply with the Code.
15. ONLINE TOOLS: Services must provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

*Age Appropriate Design Code, Information Commissioner's Office*

### b. Swedish Rights of Children and Young People on Digital Platforms: Stakeholder Guide[22]

In 2020, three Swedish government agencies – the Data Inspectorate, the Children's Ombudsman and the Swedish Media Council – each with special responsibility for the

[22] Rights of Children and Young People on Digital Platforms: Stakeholder Guide. Swedish Data Inspectorate, Children's Ombudsman and Media Council, 2020

protection of children and the promotion of their rights -- produced guidance for designers and developers of digital services where it is "common for children and young people to be". Although this test is significantly weaker than the standard set by the UK, Ireland and others, which cover all online services children are likely to access in practice, the Swedish guidance echoes the provisions set out in those regulations, building on the GDPR, the UNCRC (enshrined in Swedish law in 2020) and centring around the concept of the best interests of the child.

The Swedish guidance calls on services to protect children (anyone under the age of 18) from harmful media exposure, defined broadly as harmful content, harmful communication and harmful design, such as features which may encourage children to make decisions that may be detrimental to them (for example, handing over more personal data than they otherwise would).

### c. Dutch Code for Children's Rights[23]

In March 2021, the Dutch Ministry of the Interior and Kingdom Relations published the Code for Children's Rights to help designers focus on the rights of children in the development of digital products, with regard to the UNCRC and GDPR. It defines a child as any person under the age of 18 and is intended to cover all digital services that children might use, not only those explicitly geared towards them. It stresses that, alongside the need for safeguards, children must be guaranteed sufficient freedom to participate online. Encapsulating the concept of a child's best interests, the Code sets out the responsibility of services to not only prevent harm, but to provide a child with a rich online experience.

Threaded throughout the Code are indicative examples of compliance and good practice.

**Principles of the Dutch Code for Children's Rights**

1. Make the best interests of the child the primary consideration when designing.
2. Involve children and their expectations in the design process.
3. Ensure the legitimate processing of personal data of children.
4. Provide transparency in a way that is understandable and accessible to children.
5. Carry out a privacy impact assessment based on children's rights.
6. Provide a child-friendly privacy design.
7. Prevent the profiling of children.
8. Avoid the economic exploitation of children at all times.
9. Avoid a harmful design for children at all times.

[23] Code for Children's Rights, Netherlands Ministry of the Interior and Kingdom Relations, 2021

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

*Code for Children's Rights, Netherlands Ministry of the Interior and Kingdom Relations*

### d. French Recommendations on the Digital Rights of Children[24]

In August 2021, the Commission nationale de l'informatique et des libertés (CNIL) published eight recommendations for meeting those provisions of the GDPR dedicated to the protection of children, recognising their right to age-appropriate information, their right to be forgotten and their evolving capacity to consent to the processing of their data. The recommendations require particular vigilance from online services with regard to the profiling of children.

The CNIL's guidance places more of a focus on parental controls, which marks a shift from the approach of the UK Code and Irish Fundamentals, but the French recommendations nonetheless recognise the balance between a child's right to autonomy and their need for protection, seeking to respond to their evolving capacity to understand matters that affect them, while calling on services to demonstrate in the design of their products their increased responsibility towards children when processing their personal data.

Like the AADC, the CNIL Recommendations recognise the need for design techniques which can both speak to children in their own language and ensure that the interface is neutral and that children are not nudged towards selecting certain options (i.e. providing consent to data collection and use).

**Digital Rights of Children: Recommendations**

1. REGULATE THE CAPACITY OF CHILDREN TO ACT ONLINE: Children represent one of the largest user groups of social networks. By creating an account and ticking a box to agree to the terms and conditions, they are, in fact, entering into a contract.
2. ENCOURAGE CHILDREN TO EXERCISE THEIR RIGHTS: There are several legal and practical reasons why children should be allowed to exercise their own digital rights.
3. SUPPORT PARENTS WITH DIGITAL EDUCATION: Parents are key when it comes to the digital education of children. But they need to be given ways to help them protect their rights while respecting their best interests.
4. SEEK PARENTAL CONSENT FOR CHILDREN UNDER 15: The law does, to a certain degree, accept a child's consent to the processing of data, accompanied by parental consent when the child is under 15.
5. PROMOTE PARENTAL CONTROLS THAT RESPECT THE CHILD'S PRIVACY AND BEST INTERESTS: Parental controls are a tool for protecting children online.

[24] Digital rights of children, Commission Nationale de l'Informatique et des Libertés, 2021

However, the CNIL calls for vigilance when it comes to certain very intrusive features.

6. STRENGTHEN THE INFORMATION AND RIGHTS OF CHILDREN BY DESIGN: Everyone, even children, must be properly informed about how their data is used. This information should be age-appropriate and accessible.
7. CHECK THE AGE OF THE CHILD AND PARENTAL CONSENT WHILE PROTECTING THE CHILD'S PRIVACY: Checking a child's age and parental permission is a complex but crucial issue: how can we protect children if we cannot identify them or know who has parental authority?
8. PROVIDE SPECIFIC SAFEGUARDS TO PROTECT THE INTERESTS OF THE CHILD: Strengthening the rights of children should also involve specific protection measures by design on the websites, services and apps they are likely to use.

*Digital rights of children, Commission nationale de l'informatique et des libertés*

### e. Irish Fundamentals for Child-Oriented Approach to Data Processing[25]

Ireland's Data Protection Commission (DPC) has produced guidance (the "Fundamentals") setting out the standards that all organisations should follow when collecting and processing children's data. The Fundamentals were published in December 2021, following a 3-month public consultation period on a draft version issued at the end of 2020. The Foreword states, "the Fundamentals are entirely consistent with the UK Code, and in particular it is clear that the best interests of the child principle underpin both." The Fundamentals apply to services "directed at, intended for or likely to be accessed by children."

The Fundamentals recognise a child as anyone under the age of 18 and that children use services beyond those that are directed at them, emphasising that mixed-audience services may choose to establish a high level of data protection for both their adult and child users, negating the need to distinguish between the two. The Fundamentals caution against the idea that parental controls alone are a sufficient response to the risks children face online, instead highlighting the importance of default settings that guard against placing disproportionate responsibility on children and parents to navigate online spaces that might be unsafe by design.

Irish Fundamentals

1. FLOOR OF PROTECTION: Online service providers should provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users so that the protections set out in these Fundamentals are applied to all processing of children's data.
2. CLEAR-CUT CONSENT: When a child has given consent for their data to be processed, that consent must be freely given, specific, informed and unambiguous, made by way of a clear statement or affirmative action.

[25] Fundamentals for Child-Oriented Approach to Data Processing, Data Protection Commission, 2021

3. ZERO INTERFERENCE: Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict with, or negatively impact, at any level, the best interests of the child.
4. KNOW YOUR AUDIENCE: Online service providers should take steps to identify their users and ensure that services directed at/intended for or likely to be accessed by children have child-specific data protection measures in place.
5. INFORMATION IN EVERY INSTANCE: Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data.
6. CHILD-ORIENTED TRANSPARENCY: Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child.
7. LET CHILDREN HAVE THEIR SAY: Online service providers shouldn't forget that children are data subjects in their own right and have rights in relation to their personal data at any age. The DPC considers that a child may exercise these rights at any time, as long as they have the capacity to do so and it is in their best interests.
8. CONSENT DOESN'T CHANGE CHILDHOOD: Consent obtained from children or from the guardians/ parents should not be used as a justification to treat children of all ages as if they were adults.
9. YOUR PLATFORM, YOUR RESPONSIBILITY: Companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/ or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and verification of parental consent are effective.
10. DON'T SHUT OUT CHILD USERS OR DOWNGRADE THEIR EXPERIENCE: If your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience.
11. MINIMUM USER AGES AREN'T AN EXCUSE: Theoretical user age thresholds for accessing services don't displace the obligations of organisations to comply with the controller obligations under the GDPR, and the standards and expectations set out in these Fundamentals where "underage" users are concerned.
12. A PRECAUTIONARY APPROACH TO PROFILING: Online service providers should not profile children and/ or carry out automated decision-making in relation to children or otherwise use their personal data for marketing/ advertising purposes due to their particular vulnerability and susceptibility to behavioural advertising unless they can demonstrate how and why it is in the best interests of the child to do so.
13. DO A DPIA: Online service providers should undertake data protection impact assessments (DPIA) to minimise the data protection risks of their

services and in particular the specific risks to children which arise from the processing of their personal data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests.

14. BAKE IT IN: Online service providers that routinely process children's personal data should, by design and by default, have a consistently high level of data protection which is "baked in" across their services.

*Fundamentals for Child-Oriented Approach to Data Processing, Data Protection Commission*

## Legislative initiatives for children's data protection from outside of Europe

The following are a selection of laws and legislative proposals from around the world which provide enforceable protection for children's data.

### a. California Age Appropriate Design Code[26]

The California Age Appropriate Design Code (AB 2273) was signed into law in September 2022. The California Code relies on definitions from the 2018 California Consumer Privacy Act (CCPA). The CCPA established increased protections for children by creating a right to opt-out of the sale of the consumer's personal information if over 16 years of age and the right to opt in if the consumer is under 16 years of age (exercised by the parent for under 13s).[27]

Reflecting the AADC upon which it is modelled, the California Code incorporates the principle of the best interests of the child, the definition of a child as any person under the age of 18, and covers all services children are likely to access in practice. All of these are particularly significant in the US context, where COPPA[28] has long set the age of digital adulthood at 13 and where legislation typically only covers services "directed at" children.

The provisions of the California Code are largely the same as those in the AADC, with the exception of prohibiting 'dark patterns,' which is arguably broader than the AADC's prohibition on 'nudge techniques'.

### b. Australian Online Privacy Bill[29]

The draft Australian Online Privacy Bill defines a child as anyone who has not yet reached the age of 18 and requires that decisions about children's data should be taken with their best interests as the primary consideration.

### c. Indian Personal Data Protection Bill[30]

Chapter IV of the Indian Personal Data Protection Bill 2019 contains special protections for children, requiring any data collector to comply with their best interests and refrain from profiling, tracking, or targeting advertising to children.

### d. Brazilian General Data Protection Law[31]

Brazil's General Data Protection Law, influenced by the GDPR and in force since August 2020, defines a child as anyone under 18. It only allows for children's data to be processed on the conditions that it is strictly necessary for the provision of the service and carried out in accordance with their best interests and with parental consent. Services must publicise the types of data they collect on children, the uses it is put to and how children can exercise their rights in relation to their personal information.

[26] AB-2273 The California Age Appropriate Design Code Act, California Legislature, 2022
[27] California Consumer Privacy Act, 2018
[28] Children's Online Privacy Protection Rule, 1998
[29] Online Privacy Bill (Exposure Draft), Government of Australia, 2021
[30] Personal Data Protection Bill, Indian Parliament, 2019
[31] General Personal Data Protection Act, Brazilian National Congress, 2018

These terms must be presented in a simple, clear and accessible way, appropriate to the child's level of comprehension.

### e. New Zealand Privacy Act[32]

New Zealand's 2020 Privacy Act grants children the same rights as adults to request access to their data, authorise the collection of their data or complain about its disclosure. Where a child is too young to exercise these rights on their own behalf, services are instructed to take a "common sense" approach, regarding a parent or carer as acting on behalf of the child. Where a child under 16, or their representative, seeks to exercise these rights, services do have grounds to withhold the information if releasing it would be contrary to the child's best interests. Services must take "special care" when collecting personal information on children, ensuring they obtain genuine consent. Data collection must be "fair and reasonable", with this being determined by factors including the purpose for the collection, the degree to which collection intrudes on a child's privacy and the time and place the data were collected.

[32] Privacy Act, New Zealand Parliament, 2020

## Fundamental principles for children's data protection

The above children's data protection regimes differ in their legal status, focus, language and level of detail, but the GDPR-grounded initiatives in particular clearly reflect a set of common fundamental principles, which are grounded in international child rights law and policy and constitute international best practice. The table in Annex provides a comparative overview of key principles and their interpretation across the five GDPR-based initiatives.

### a. Definition of a child

A child is somebody under the age 18, in keeping with the definition of a child under the UN Convention on the Rights of the Child, to which all EU Member States are party, as "a person under the age of 18 years."

> 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.
>
> *Code for Children's Rights (Netherlands)*

> [F]or data protection purposes, a child is somebody under the age 18, in keeping with the definition of a child under the UN Convention on the Rights of the Child (UNCRC) as "a person under the age of 18 years."
>
> *Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

### b. Best interests of the child

In line with the fundaments of the UNCRC and EU Charter, the principle of the primacy of the best interests of the child is the cornerstone of all initiatives for children's data protection, and of interpretation of the principles of lawfulness, fairness and transparency that underpin GDPR.

The best interests of the child must be a primary consideration in all actions impacting children, including as regards the design and development of any digital products or services that process children's data or whose data processing activities impact children. This should also be the key criteria against which outcomes for children should be judged.

> If you consider the best interests of child users in all aspects of your design of online services, then you should be well placed to comply with the '"lawfulness, fairness and transparency" principle [of GDPR], and to take proper account of Recital 38.
>
> *Age Appropriate Design Code (UK)*

If there is a balance between various interests, providers must be required to act giving primary consideration to the best interests of the child, including as regards the child's right to:

- Privacy
- Play and engage in recreational activity
- Non-discrimination
- Freedom of information
- Freedom of opinion and thought
- Freedom of association and identity forming

> Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict with or negatively impact, at any level, the best interests of the child.
>
> *Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

To be "fair" and in line with the best interests of the child, children's personal data should not be used in ways that have been demonstrated to cause them – as set out in GDPR Recital 75 – "physical, material or non-material damage".

Various initiatives specify how this applies to marketing and profiling for commercial purposes.

> If you wish to use the personal data of children and young people for marketing, you must always start from what is deemed to be in the child's best interests.
>
> *Stakeholder Guide (Sweden)*

> Online service providers should not profile children and/or carry out automated decision making in relation to children, or otherwise use their personal data, for marketing/advertising purposes due to their particular vulnerability and susceptibility to behavioural advertising, unless they can clearly demonstrate how and why it is in the best interests of the child to do so.
>
> *Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

The Age Appropriate Design Code introduces the concept of the "detrimental use of data" and bans the use of children's personal data for purposes known to be detrimental to their well-being. The Dutch Code provides a range of examples of data practices with negative consequences for the development, health and well-being of children.

> [Applying the precautionary approach], you should:
>
> - avoid using personal data in such ways that children are encouraged to stay on longer...
> - avoid functions which use personal data to automatically extend use ... (data-steered autoplay functions)
> - introduce mechanisms like pause buttons, through which children can take a break any time...
> - limit the excessive use of notifications or make sure they can be easily switched off
> - prevent incentives for children to add as many as possible (unknown) friends or followers
> - not make profiles of children under a certain age openly visible to other users
>
> *Code for Children's Rights (Netherlands)*

### c. Data protection impact assessments

In order to demonstrate compliance with children's rights and the principle of the best interests of the child, the UK Code, Irish Fundamentals, Swedish Guide, Dutch Code (and California Code) make Data Protection Impact Assessments one of their core provisions, requiring providers to assess and mitigate risks arising from data processing. Providers should undertake data protection impact assessments (DPIAs) to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their personal data (based on the 4Cs framework covering content, contact, conduct and consumer/contract risks). The principle of the best interests of the child must be a key criterion in any DPIA.

> Online service providers should undertake data protection impact assessments to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their personal data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests.
>
> *Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

> DPIAs are a key part of your accountability obligations under the GDPR, and help you adopt a 'data protection by design' approach. A good DPIA is also an effective way to assess and document your compliance with all of your data protection obligations... However, DPIAs are not just a compliance exercise. Your DPIA should consider compliance risks, but also broader risks to the rights and freedoms of children that might arise from your processing, including the potential for any significant material, physical, psychological or social harm.
>
> Age Appropriate Design Code (UK)

> You must always carry out a risk assessment before starting any processing of personal data. [...] The special rights held by children and young people in accordance with UNCRC must also be included in your risk analysis, for example in terms of children being protected from all forms of violence and discrimination, the principle of the child's best interests, and the right of children to express their opinion.
>
> Stakeholder Guide (Sweden)

### d. Age assurance[33]

EDPB Guidelines 05/2020 on consent note that "although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful" (para 133). They also specify that that age assurance measures "should be proportionate to the nature and risks of the processing activities" (para 132).[34]

> A child's age may for example have an impact on whether they are able to consent to personal data processing. Their age can also affect the risk assessment. For this reason, it may sometimes be appropriate or necessary to verify a child's age.
>
> *Stakeholder Guide (Sweden)*

Age assurance is required beyond consent in order to ensure all children are given an appropriate level of protection in line with their rights.

[33] The terminology "age assurance" is here used as an umbrella term for a broad family of methods used to ascertain age, with "age verification" providing the highest level of certainty. The Irish Fundamentals use the term "age verification" as set out in GDPR to cover the full range of methods to establish the age of a child with varying levels of robustness and accuracy.

[34] Guidelines 05/2020 on consent under Regulation 2016/679

> In order to properly apply the special rules geared to children, it is necessary to know which of the users are under 18. And in order to implement those rules in a manner appropriate for the – possible different – ages of underage users, it is important to know what age category a child falls under.
>
> *Code for Children's Rights (Netherlands)*

Providers should be required to take a risk-based approach to recognising the age of individual users and ensuring data protections apply effectively to child users and should either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from their data processing, or apply all data protections standards listed in the regulation to all users.[35]

> Online service providers should provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users so that the protections set out in these Fundamentals are applied to all processing of children's data.
>
> *Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

The California Code requires the California Children's Data Protection Working Group to research and make recommendations to ensure that any age assurance mechanisms a service puts in place are minimally invasive and privacy-protective.

The Irish Fundamentals take a similar approach, requiring online services to take steps to identify their users and ensure that services directed at, intended for or likely to be accessed by children have child-specific data protection measures in place.

Appropriate age verification mechanisms will vary depending on factors such as:

- The service being provided
- The sensitivity of the personal data being processed
- The accessibility of the personal data to others
- Further processing and sharing of personal data

The CNIL's Recommendations include a set of standards for privacy-preserving age-assurance.

> Any age and parental consent verification systems should [...] respect the following rules:
>
> 1. PROPORTIONALITY. When choosing an age verification system, online service providers should consider the proposed purposes of the processing, the target audiences, the data processed, the technologies available and the

[35] Extensive detail regarding age assurance is provided by the ICO: https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf

level of risk associated with the processing. A mechanism using facial recognition would therefore be disproportionate.

2. MINIMISATION. Any system should be designed to limit the collection of personal data to what is strictly necessary for the verification, and not retain the data once the verification has been completed. The data should not be used for other purposes, including commercial uses.
3. ROBUSTNESS. Age verification mechanisms must be robust when they are for practices or processing that involves a risk (e.g. targeted advertising for children). For these cases the use of self-declaration methods alone should be avoided.
4. SIMPLICITY. The use of simple and easy-to-use solutions that combine verification of both age and parental consent could be encouraged.
5. STANDARDISATION. "Industry standards" and a certification programme could be encouraged to ensure compliance with these rules and to promote verification systems suitable for a wide range of websites and apps.
6. THIRD PARTY INTERVENTION. Age verification systems based on the intervention of a trusted third party who can check a data subject's identity and status (attribution of parental authority) could be investigated in order to meet the requirements as described above.

*Recommendations on the Digital Rights of Children (France)*

Guidance should also spell out that obligations on providers cannot be bypassed by blocking children from accessing services they have a right to access, nor should their experience be downgraded. Age assurance must not be used to lock children out of spaces they have a right to access, nor as an excuse to gather more personal information than is strictly necessary, but to deliver age-appropriate experiences with minimum data collection proportionate to the risks posed by a service.

If your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience.

*Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

### e. Privacy and safety design and default

Products and services must be required to consider the privacy and protection of children's data by design and by default. Settings must be "high privacy" by default unless there is a demonstrable and compelling reason to do so, taking account of the best interests of the child.

Process as few personal data as possible and consider privacy aspects and child protection in the planning and design of services and systems.

*Stakeholder Guide (Sweden)*

In the Irish Fundamentals, this concept is in its 'Bake It In' approach, which interprets Article 25(2) of GDPR as follows:

> [D]ata protection measures should be built into the architecture and functioning of a product or service from the very start of the design process (rather than being considered after the development phase) and [...] the strictest privacy settings should automatically apply to a product of service.
>
> *Fundamentals for a Child-Oriented Approach to Data Processing (Ireland)*

> You may not process more personal data than is strictly necessary to achieve the specific goal of your service. In other words, you are obliged to include privacy in the design of your app or game and to align the default settings as privacy friendly as possible. In the best interests of the child, it is advisable to give this obligation shape in a child-friendly manner in the design.
>
> *Code for Children's Rights (Netherlands)*

The AADC, Irish Fundamentals and Dutch Code provide extensive lists of design practices to protect children's data and minimise its collection by design. The Dutch Code for instance includes the following instructions:

- 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.
- Build 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.
- 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 protections.
- Make sure that geolocation, microphone and camera are turned off as default settings. After the end of each session in which geolocation is used, the option must be turned off again. At the time the child makes use of geolocation, this must be clear to the child, at all times.

This is how children can be protected from sharing data inappropriately:

- Set the privacy settings on apps to "do not share" as the standard.
- Create an extra popup window to warn the child of the consequences of a choice they are about to make.
- Design important decisions in several steps with a delay to give the child time to think.
- Include a clear, child-friendly explanation of the increased functionality and its risks when the child activates "sharing mode".

*Stakeholder Guide (Sweden)*

Privacy-by-design, taking into account the best interests of the child, should also protect children's data from third parties, including other users of the service, as per GDPR Article 25(2). Children's data must not be disclosed unless there is a demonstrable and compelling reason to do so, taking account of the best interests of the child.

If it is appropriate for you to offer a privacy setting, then your default position for each individual privacy setting should be "high privacy".

This means that children's personal data is only visible or accessible to other users of the service if the child amends their settings to allow this.

This also means that unless the setting is changed, your own use of the children's personal data is limited to use that is essential to the provision of the service. Any optional uses of personal data, including any uses designed to personalise the service have to be individually selected and activated by the child.

*Age Appropriate Design Code (UK)*

### f. Transparency and enabling of rights

Transparency obligations are set out in Article 12 of the GDPR, which requires information to be provided to the data subject "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child".

Children must be properly informed about how their data is used. This information should be age-appropriate and accessible so that users can effectively understand and take advantage of their rights.

*Recommendations on the Digital Rights of Children (France)*

Privacy information and other published terms, policies and community standards, must be concise, prominent, and in clear language suited to the age of the child. Additional specific "bite-sized" explanations about how services use personal data should be provided at the point that use is activated.

The CNIL Recommendations require that child users be given clear and appropriate information about how their data will be used and of their data protection and privacy rights, to ensure the child understands the agreement they are entering into with the services they use. They also recognise the role of design in providing age-appropriate information, recommending that services avoid the use of misleading interfaces, nudges and dark patterns, and involving children in the design process of the interfaces they encounter.

Prominent and accessible tools to help children exercise their data protection rights and report concerns should also be provided. As the Irish Fundamentals also make clear, services must recognise children as data subjects in their own right and have rights in relation to their personal data at any age. A child must be able to exercise these rights at any time and should not be prevented from doing so as a result of their age, maturity or capacity.

> Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.
>
> *Age Appropriate Design Code (UK)*

These provisions are echoed in CNIL's guidance, which calls on services to take every possible measure to explain in a clear and comprehensible manner the process by which a child may exercise their data rights and the legal remedies available.

### g. Parental controls

Parental controls can be used to support parents in providing a more individualised path to protecting and promoting the best interests of their child, in supplement to a safety- and privacy-by-design approach.

Children should be given age-appropriate information about parental controls and provided an obvious sign when they are being monitored by a parent or carer.

> Make sure that the child receives a clear, striking signal when he or she is being watched (even if a parent is watching).
>
> *Code for Children's Rights (Netherlands)*

The CNIL Recommendations caution that parental controls can undermine trust between parent and child, hinder child empowerment and the privacy of the child.

> Any proposed parental controls must comply with data protection rules, and in particular with:
>
> - the principle of proportionality taking into account the child's interests, age and level of maturity, and avoiding the use of intrusive features such as constant tracking;
> - the principle of transparency towards the child by clearly explaining which parental controls are being used;

- the principle of security of the child's data, in order to ensure that third parties do not have access to information about the child (e.g. the child's geolocation data).

*Recommendations on the Digital Rights of Children (France)*

Tools for parental control may therefore only be used if the child is able to understand that they are being monitored and how.

*Stakeholder Guide (Sweden)*

## Conclusion

The principles and provisions of GDPR interpreted together with established children's rights law, set out strong and unambiguous requirements for the protection of children's personal data. Services must recognise children using or likely to use their services and ensure that any risks to their rights and best interests are assessed and mitigated, by design and default. Children do merit special protections for their personal data, and the above overview of child data protection regimes provides a comprehensive and strongly consensual guidebook to what those protections should be.

# Annex: Table: Principles for children's data protection common to existing initiatives under GDPR[36]

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| **Grounding in GDPR** | [This code] sets out specific protections for children's personal data in compliance with the provisions of the GDPR. [...]<br><br>This code supports compliance with those general principles by setting out specific protections you need to build in when designing online services likely to be accessed by children, in line with Recital 38 of the GDPR. [...]<br><br>In particular, this code sets out practical measures and safeguards to ensure processing under the GDPR can be considered 'fair' in the context of online risks to children, and will help you comply with:<br><br>• Article 5(1)(a): the fairness, lawfulness and transparency principle;<br>• Article 5(1)(b): the purpose limitation principle;<br>• Article 5(1)(c): the data minimisation principle;<br>• Article 5(1)(e): the storage limitation principle; | This guide describes selected parts of the requirements set out in the General Data Protection Regulation (GDPR) for when the personal data of children and young people are being processed. [...]<br><br>GDPR contains a number of fundamental principles which can be said to be the core of the Regulation, and which are important to understand and implement. These principles stipulate for example that those responsible for the processing of data relating to children may only collect personal data for explicitly stated and legitimate purposes.<br><br>• are not to process more personal data than is necessary for those purposes.<br>• are to ensure that the personal data is accurate.<br>• are to erase the personal data when it is no longer needed.<br>• are to protect the personal data, for example so that unauthorised persons | The General Data Protection Regulation (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".<br><br>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.<br><br>Aside from the fact as to whether children are mentioned explicitly in recitals or provisions of the GDPR, | In 2018, the entry into force of the GDPR significantly changed the legal landscape by introducing, for the first time, specific provisions dedicated to children into European data protection law. In particular, they require age-appropriate information, provide for the reinforcement of their right to be forgotten and an ability to consent, under certain conditions, to the processing of their data (only over the age of 15 or with their parents for children under 15). They also call for particular vigilance with regard to the profiling of children.<br><br>The GDPR and the French Data Protection Act allow children over the age of 15 to give their own consent for certain types of the processing that require non-contractual "consent". [...]<br><br>The GDPR requires data subjects to be provided with information about how their personal data will be used and about their rights in an intelligible and easily accessible form, using clear and plain language, especially | [T]he Fundamentals will assist organisations that process children's data, by clarifying the principles, arising from the high-level obligations under the GDPR, to which the DPC expects such organisations to adhere. [...] Children are very much front and centre of the data protection landscape in Europe, with Recital 38 of the GDPR stating that children merit specific protection when it comes to the processing of their personal data because they may be less aware of the risks, consequences and safeguards involved as well as their data protection rights. Where children are aware of the risks associated with the processing of their personal data, their age, maturity and developmental capacity will impact on their ability to be able to mitigate those risks. |

[36] This table quotes the original documents. Any paraphrasing or added information is contained within square brackets.

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | • Article 5(2): the accountability principle;<br>• Article 6: lawfulness of processing;<br>• Articles 12, 13 and 14: the right to be informed;<br>• Articles 15 to 20: the rights of data subjects;<br>• Article 22: profiling and automated decision-making;<br>• Article 25: data protection by design and by default; and<br>• - Article 35: data protection impact assessments (DPIAs). | • are not given access to it and so that it is not lost or destroyed.<br>• are to be able to demonstrate that and how you live up to the General Data Protection Regulation. [...] | 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. | any information specifically intended for a child. [...]<br><br>Article 8.2 GDPR implicitly establishes the need to verify age. [...]<br><br>In addition, the GDPR emphasises that automated decision-making based on profiling should not apply to children. | |
| **Grounding in UNCRC** | [This code] takes account of the standards and principles set out in the UNCRC. | Sweden adopted the UN Convention on the Rights of the Child (UNCRC) already in 1990. As of 1 January 2020, the UNCRC is also incorporated into Swedish national law. This means, that all the rights of the UNCRC can be implemented as Swedish law and that children are seen as rights holders, which gives them a stronger legal standing. [...]<br><br>As a creator and person responsible for a digital environment, it is important to have knowledge of children's rights in order to ensure that children are protected and can develop in the digital environment. | 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). | More generally, the United Nations Convention on the Rights of the Child (UNCRC) recognises a child's right to privacy (art. 16) and to be heard (art. 12). These fundamental rights only have concrete and effective meaning if they give children a certain degree of power to ensure that they are respected, especially because it is sometimes their parents who are responsible for giving out their personal data in the first place. This is the stance taken by the recent UN General Comment on children's rights in relation to the digital environment (§72). | The primary source, at an international level, of legal rights for children is the 1989 UN Convention on the Rights of the Child (UNCRC), which is the most ratified convention in history. Having ratified the UNCRC in 1992, Ireland has an obligation under international law to respect, protect and fulfil the rights of children set out in the UNCRC.<br><br>[The Fundamentals set out in detail the relevant provisions of UNCRC Articles 1, 3, 5, 8, 12, 13, 14, 16, 17, 31 and 32.] |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| **Scope - age of child as rights holders** | "This code applies if children are likely to use your service. A child is defined in the UNCRC and for the purposes of this code as a person under 18. | [The Swedish guidance does not explicitly identify a child as anyone under the age of 18, but its references to the UNCRC - and the Convention's incorporation into Swedish law - suggest that 18 is set as the threshold for digital adulthood.] | In the Code we speak of 'children', whereby we are referring to all persons under the age of 18 (Article 1 UNCRC). | The GDPR and the French Data Protection Act allow children over the age of 15 to give their own consent for certain types of the processing that require non-contractual "consent". [...] On the other hand, at the age of 15 the law does not yet recognise "general digital adulthood". | In Ireland, for data protection purposes, a child is somebody under the age 18, in keeping with the definition of a child under the UN Convention on the Rights of the Child (UNCRC) as "a person under the age of 18 years." |
| **Scope – companies** | This code applies to "information society services likely to be accessed by children" in the UK. This includes many apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. It is not restricted to services specifically directed at children. | With this guide we primarily aim to reach stakeholders who create and operate various digital environments where children and young people regularly spend time. Whether you own or create websites, Swedish-language platforms, or have your own YouTube channel, we hope that you will find this guide useful. | This concerns all digital services that children might use, even if they are not explicitly geared to children. | Strengthening the rights of children should also involve specific protection measures by design on the websites, services and apps they are likely to use. | Online service providers should take steps to identify their users and ensure that services directed at/ intended for or likely to be accessed by children have child-specific data protection measures in place. |
| **Best interests of the child** | The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.<br><br>The UNCRC incorporates provisions aimed at supporting the child's needs for safety, health, wellbeing, family relationships, physical, psychological and emotional development, identity, freedom of expression, privacy and agency to form their own views and have them heard. Put simply, the best interests of the child are whatever is best for that individual child. [...] It also recognises the child's right to privacy and freedom from economic exploitation. The importance of access to information, association with others, and play in supporting | According to UNCRC, every child is entitled to express their opinion in any decisions that concerns them. The child's best interests must be taken into consideration. | The weighing of a child's interests and the implementation of the best interests principle consists of two stages. We call this a child impact assessment [:the assessment stage; and the determination stage.<br><br>At the assessment stage, all factors relevant to the interests of the child are considered.] Relevant factors are, inter alia:<br>• possible impact on the well-being and the development of children<br>• possible impact on the rights of children. This includes the rights to:<br>  • non-discrimination<br>  • freedom of information | Children may exercise their own rights directly in relation to their personal data, provided this can be regarded as a "routine act" and especially if it is in the best interests of the child. [...]<br><br>Parents are key when it comes to the digital education of children. But they need to be given ways to help them protect their rights, while respecting their best interests. [...]<br><br>Promote parental controls that respect the child's privacy and best interests. [...]<br><br>With regard to the specific safeguards that should be put in place to protect the best interests of the child, the CNIL invites those responsible for | The core message of these Fundamentals is that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data. [...] Online service providers processing children's data should ensure that the pursuit of legitimate interests do not interfere with, conflict with or negatively impact, at any level, the best interests of the child.<br><br>The UN Committee on the Rights of the Child24 (the UN Committee) has stated25 that determining what is in the best interests of the child should start with an assessment of the specific circumstances that make the child unique, and that the following |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | the child's development. And the child's right, in line with their evolving capacities, to have a voice in matters that affect them. [...]<br><br>The placing of the best interests of the child as a 'primary consideration' recognises that the best interests of the child have to be balanced against other interests. For example, the best interests of two individual children might be in conflict, or acting solely in the best interests of one child might prejudice the rights of others. It is unlikely however that the commercial interests of an organisation will outweigh a child's right to privacy. [...]<br><br>[Y]ou should not process children's personal data in ways that are obviously, or have been shown to be, detrimental to their health or wellbeing. To do so would not be fair. | | • freedom of opinion and thought<br>• freedom of association and identity forming<br>• play and engage in recreational activities<br>• possible impact on the safety of children, for example:<br>• guaranteeing privacy<br>• protection against all forms of exploitation<br>• protection against social risks<br>• preventing confrontation with harmful information<br>• 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.<br><br>[At the determination stage, services should concretely devise the organisational and technical measures to safeguard the child's interests.] | online platforms and services used by children to:<br>• set up stricter default privacy settings;<br>• deactivate by default any profiling systems for children, especially for the purposes of targeted advertising;<br>• not re-use or pass on to third parties the data of children for commercial or advertising purposes, unless they can demonstrate that they are acting for overriding reasons in the best interests of the child. | elements should be taken into account when assessing the child's best interests:<br>• The child's views<br>• The child's identity<br>• Preservation of the family environment and maintaining relations<br>• Care, protection and safety of the child<br>• A situation of vulnerability<br>• The child's right to health<br>• The child's right to education |
| **Age assurance** | Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead. | A child's age may for example have an impact on whether they are able to consent to personal data processing. Their age can also affect the risk assessment. For this reason, it may sometimes be appropriate or necessary to verify a child's age<br><br>Age checks should be preceded by a risk assessment and must not entail any unreasonable processing of data. | In order to properly apply the special rules geared to children, it is necessary to know which of the users are under 18. And in order to implement those rules in a manner appropriate for the – possible different – ages of underage users, it is important to know what age category a child falls under.<br><br>Age verification does not necessarily call on services to ascertain the exact | Any age and parental consent verification systems should [...] respect the following rules:<br><br>PROPORTIONALITY. When choosing an age verification system, online service providers should consider the proposed purposes of the processing, the target audiences, the data processed, the technologies available and the level of risk associated with the processing. A mechanism using | If your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience.<br><br>The Fundamentals require online services to take steps to identify their users and ensure that services directed at, intended for or likely to |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | The Code is not prescriptive about the methods which should be used to establish age, or the level of certainty different methods provide, but does list some of the methods services may wish to consider, including:<br>• Self-declaration<br>• Artificial intelligence<br>• Third-party age verification services<br>• Account holder confirmation<br>• Technical measures<br>• Hard identifiers | | age of their users, merely whether they are in a particular age range or above or below a certain age threshold. The Dutch Code goes further than its equivalents by indicating where different forms of age verification are Appropriate:<br>• User statement (self-declaration) is appropriate for the processing of low-risk data or can be used in combination with another verification technique. This form of age verification is probably not adequate when processing personal data of children.<br>• Technical measures, such as neutral presentation of age categories and blocking the option of changing the first registered age, are appropriate for digital services which can be harmful for children.<br>• Third parties.<br>• Confirmation via e-mail or text link, for example asking the parent to confirm the child's age by clicking on a link which is provided in an e-mail or a text message. | facial recognition would therefore be disproportionate.<br>MINIMISATION. Any system should be designed to limit the collection of personal data to what is strictly necessary for the verification, and not retain the data once the verification has been completed. The data should not be used for other purposes, including commercial uses.<br>ROBUSTNESS. Age verification mechanisms must be robust when they are for practices or processing that involves a risk (e.g. targeted advertising for children). For these cases the use of self-declaration methods alone should be avoided.<br>SIMPLICITY. The use of simple and easy-to-use solutions that combine verification of both age and parental consent could be encouraged.<br>STANDARDISATION. "Industry standards" and a certification programme could be encouraged to ensure compliance with these rules and to promote verification systems suitable for a wide range of websites and apps.<br>THIRD PARTY INTERVENTION. Age verification systems based on the intervention of a trusted third party who can check a data subject's identity and status (attribution of parental authority) could be investigated in order to meet the requirements as described above. | be accessed by children have child-specific data protection measures in place. There is not a one-size-fits-all solution to the issue of age verification. Appropriate age verification mechanisms will vary depending on factors such as:<br>• The service being provided<br>• The sensitivity of the personal data being processed<br>• The accessibility of the personal data to others<br>• Further processing and sharing of personal data<br>Any such measures should be proportionate and grounded on a risk-based approach. |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| **Profiling** | Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).<br><br>[A privacy setting for behavioural advertising which is used to fund a service, but is not part of the core service the child wishes to access, should always be offered. Limited circumstances where it may not be appropriate to offer a privacy setting over profiling include profiling to meet a legal or regulatory requirement, such as safeguarding or child protection, to prevent child sexual exploitation or abuse, or to conduct age assurance.<br><br>Services should:<br><br>• Differentiate between different types of profiling for different purposes<br>• Ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise)<br>• Provide appropriate interventions at the point at which any profiling is activated<br>• Provide appropriate measures to safeguard the child (in particular | Children and adults are equally entitled not to be affected by decisions that are based solely on automated decision-making in which profiling has been part of the process. | 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 (implicitly) encourages 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. Appropriate measures must be taken in this respect.<br><br>[Where it is in the child's best interests for profiling to occur, services should:]<br><br>• Make clear why profiling is in the best interests of the child<br>• Make clear what type of profiling is used for which purpose [separating privacy settings for every form of profiling]<br>• [Have] 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)<br>• Take appropriate measures to safeguard the child from psychological or physical harm [...] | While the GDPR does not generally prohibit the profiling of children, it does highlight the need for specific protection. Indeed, as the European Data Protection Board (EDPB) guidelines on the targeting of social media users point out, "Targeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development". In addition, the GDPR emphasises that automated decision-making based on profiling should not apply to children. | Organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so. |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | from inappropriate content) where profiling is active] | | • Assess whether profiling has any effects which harm the best interests and rights of the child | | |
| **Data Protection Impact Assessments (DPIAs)** | Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code. [...]<br><br>You should begin a DPIA early in the design of your service, before you start your processing. It should include these steps:<br><br>Step 1: identify the need for a DPIA<br><br>Step 2: describe the processing<br><br>Step 3: consider consultation<br><br>Step 4: assess necessity and proportionality<br><br>Step 5: identify and assess risks arising from your processing<br><br>Step 6: identify measures to mitigate the risks<br><br>Step 7: sign off, record and integrate outcomes | You must always carry out a risk assessment before starting any processing of personal data. This applies regardless of whether you intend to launch a new app, an online service or your own channel. Throughout the personal data processing you are also obligated to assess risks and otherwise protect and handle the data correctly. [...]<br><br>The special rights held by children and young people in accordance with UNCRC must also be included in your risk analysis, for example in terms of children being protected from all forms of violence and discrimination, the principle of the child's best interests, and the right of children to express their opinion [...]<br><br>If the risk assessment indicates that your planned personal data processing will likely entail a high risk of violating the freedoms and rights of individuals, GDPR requires you to carry out an impact assessment [...]<br><br>What this means in practice is clarified in The Swedish Authority for Privacy Protection's list of when to conduct an impact assessment. | 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.<br><br>The expectations of children and parents as interested parties must be included in the PIA. 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. [A PIA can also determine] what steps have to be taken to verify age and parental consent both adequately and in a privacy-friendly manner [and] answer the question of whether restricting 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. | N/A | Online service providers should undertake data protection impact assessments (DPIA) to minimise the data protection risks of their services, and in particular the specific risks to children which arise from the processing of their personal data. The principle of the best interests of the child must be a key criterion in any DPIA and must prevail over the commercial interests of an organisation in the event of a conflict between the two sets of interests. |
| **Privacy and safety 'by design and default'** | Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different | Process as few personal data as possible and consider privacy aspects and child protection in the planning and design of services and systems. | You may not process more personal data than is strictly necessary to achieve the specific goal of your service. In other words, you are obliged to include privacy in the | With regard to the specific safeguards that should be put in place to protect the best interests of the child, the CNIL invites those responsible for | [D]ata protection measures should be built into the architecture and functioning of a product or service from the very start of the design process (rather than being |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | default setting, taking account of the best interests of the child) [...]<br><br>How can we make sure that we meet this standard?<br><br>• Provide 'high privacy' default settings [...]<br>• Consider the need for any further intervention at the point at which any setting is changed [...]<br>• Allow users the option to change settings permanently or just for the current use [...]<br>• Retain user choices or high privacy defaults when software is updated [...]<br>• Allow for different user choices on multi-user devices | [The Swedish guidance calls on services to protect children (anyone under the age of 18) from harmful media exposure, defined broadly as harmful content, harmful communication and harmful design, such as features which may encourage children to make decisions that may be detrimental them (for example, handing over more personal data than they otherwise would).]<br><br>Only collecting the absolutely necessary information requires you to adapt the service or system being used to collect personal data. This is referred to as privacy by default. On an online platform, this can for example mean that default settings for a social media service are set so that no more information<br><br>than necessary is collected, shared or displayed.<br><br>You must take into consideration data minimisation and other privacy protection aspects already when designing an IT system and procedures. This is referred to as privacy by design, and it means that you must integrate data protection in time and incorporate it into your working methods. You must therefore design processing, products and systems in the knowledge that children are considered entitled to special protection, that they must feel safe when using services online, and | design of your app or game and to align the default settings as privacy friendly as possible. In the best interests of the child, it is advisable to give this obligation shape in a child-friendly manner in the design.<br><br>If it is likely that a specific design is potentially harmfully for children, you should apply the precautionary approach [...]<br><br>• avoid using personal data in such ways that children are encouraged to stay on longer [...]<br>• avoid functions which use personal data to automatically extend use [...] (data-steered autoplay functions)<br>• introduce mechanisms like pause buttons, through which children can take a break any time [...]<br>• limit the excessive use of notifications or make sure they can be easily switched off<br>• prevent incentives for children to add as many as possible (unknown) friends or followers [...]<br>• not make profiles of children under a certain age openly visible to other users | online platforms and services used by children to:<br><br>• ensure that any additional features not part of the core service are disabled by default<br>• set up stricter default privacy settings<br>• deactivate by default any profiling systems for children, especially for the purposes of targeted advertising<br>• not re-use or pass on to third parties the data of children for commercial or advertising purposes, unless they can demonstrate that they are acting for overriding reasons in the best interests of the child | considered after the development phase) and [...] the strictest privacy settings should automatically apply to a product of service – Fundamentals for a child-oriented approach to data processing (Ireland)<br><br>The user should not have to deactivate (e.g. switch to off) settings which interfere with a person's privacy such as location tracking, health settings which track the movement of a user on a device or settings which automatically broadcast a person's contact details. These obligations are particularly relevant considerations for organisations whose products or services are directed at/ intended for, or are likely to be accessed by children [...]<br><br>The following is a list of examples of data protection by design and default measures that the DPC considers appropriate in the context of children (and indeed some will equally apply to adult data subjects). This list merely serves as an indicative selection of measures but it is by no means exhaustive nor will all such measures necessarily need to be applied to any given case:<br><br>• Default privacy settings – ensure the strictest privacy settings apply to children. [...]<br>• User choice – ensure that in a mixed-audience setting, children have meaningful, clear and plain choice, control and flexibility as |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | | that their right to privacy must be respected.<br><br>This is how children can be protected from sharing data inappropriately:<br><br>• Set the privacy settings on apps to "do not share" as the standard.<br>• Create an extra popup window to warn the child of the consequences of a choice they are about to make.<br>• Design important decisions in several steps with a delay to give the child time to think.<br>• Include a clear, child-friendly explanation of the increased functionality and its risks when the child activates "sharing mode". | | | to settings and features which pose greater levels of risk to children and which can be disabled (e.g. suggestions for new third-party contacts). [...]<br>• Data minimisation – minimise the amount of data collected from children in the first instance and throughout their interaction with a service. [...]<br>• Sharing and visibility – do not systematically share a child's personal data with third parties without clear parental knowledge, awareness and control; build in parental reminders/ notifications, where appropriate, in relation to subsequent sharing activity. [...]<br>• Geolocation – turn off geolocation by default for child users unless the service being provided is necessarily dependent upon it; if this is the case, make it clear to the child that their location is available to the service or can be seen by other users. Significantly reduce the level of accuracy of geolocation data collection except where necessary. [...]<br>• Profiling – turn off identifiers, techniques or settings which allow any tracking of activity online for advertising purposes. [...]<br>• Nudge techniques – avoid the use of nudge techniques that encourage or incentivise children to provide unnecessary |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | | | | | information or to engage in privacy disrupting actions. An example of this might be presenting a large "Use my contact info" button in a prominent position on an app screen, followed by a smaller "Don't use my contact info" button underneath or in a less obvious position. |
| **Transparency and enabling of rights** | The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent, and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.<br><br>Provide prominent and accessible tools to help children exercise their data protection rights and report concerns. [Tools should be prominent, highlighted during the set-up process and with clear access mechanisms such as easily identifiable icons. They should be age-appropriate (with specific recommendations offered for children in different age groups) and easy to use, and specific to the rights they support, such as:]<br><br>• a 'download all my data' tool to support the right of access, and right to data portability<br>• a 'delete all my data' or 'select data for deletion' tool to support the right to erasure | The principle of accuracy and transparency means that, according to GDPR, the processing of personal data must be clear and understandable to the data subjects and must not be carried out in hidden or manipulated ways. Information about the processing must be easily accessible and be worded in clear, simple language. | Give children the opportunity to exercise their rights in the area of data protection; give this a prominent place in the design<br><br>• Make these tools easy to use and age-relevant [...]<br>• Align tools to the rights they support, such as:<br>  • a 'download all my data' tool to support the right of access and the right to data portability<br>  • a 'delete all my data' or 'select data to be deleted' tool to support the right to be forgotten<br>  • a 'stop the use of my data' tool to support the right to restriction of processing and the right to object to processing<br>  • an 'edit' tool to support the right to rectification<br>• Make it clear how children can make a complaint about the processing of their personal data | Children must be properly informed about how their data is used. This information should be age-appropriate and accessible so that users can effectively understand and take advantage of their rights.<br><br>Design transparent and simple interfaces that can be understood by children and that comply with the specific protection measures proposed by the CNIL.<br><br>Various legal and practical arguments combine to allow children to exercise their rights directly in a number of situations. Indeed, the GDPR itself encourages them to do so. It says that children should be informed of their rights in a manner appropriate to their age and level of maturity [...] This reflects the entire philosophy of the French Data Protection Act. Indeed, Article 1 guarantees the right to informational self-determination, meaning that every person must be able to control their own data. This right is particularly relevant for young people who must learn to become conscious and responsible digital | Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on and even if consent was given by a parent on their behalf to the processing of their personal data [...] Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is comprehensible and suited to the age of the child.<br><br>A child may exercise their own data protection rights at any time, as long as they have the capacity to do so and it is in their best interests. |

| | UK Age Appropriate Design Code | Swedish Rights of Children and Young People on Digital Platforms | Dutch Code for Children's Rights | French Recommendations on the Digital Rights of Children | Irish Fundamentals for a Child-Oriented Approach to Data Processing |
|---|---|---|---|---|---|
| | • a 'stop using my data' tool to support the right to restrict or object to processing<br>• a 'correction' tool to support the right to rectification | | | citizens, which certainly involves finding out about their rights and learning to exercise them. [...] The CNIL therefore believes that children should be able to exercise their own personal data rights. | |
| **Parental controls** | If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.<br><br>If you provide parental controls then you should provide age appropriate information so that the child knows that parental controls are in place.<br><br>If your online service allows parental monitoring or tracking of a child, you should provide age-appropriate resources to explain the service to the child so that they are aware that their activity is being monitored by their parents or their location tracked. You should provide a clear and obvious sign for the child (such as a lit-up icon) which lets them know when monitoring or tracking is active.<br><br>You should also provide parents with information about the child's right to privacy under the UNCRC and resources to support age-appropriate discussion between parent and child. | If you offer tools for parental control, you should give the child age-appropriate information about those tools. This can be done through symbols or icons indicating to the child when the monitoring is happening.<br><br>It is also valuable in this context to provide parents with information regarding the child's right to privacy. Furthermore, you need to adhere to the GDPR provisions on legal basis, security, risk assessment, information, etc. like in any use of services and tools in which personal data are processed. | 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). | Any proposed parental controls must comply with data protection rules, and in particular with:<br><br>• the principle of proportionality taking into account the child's interests, age and level of maturity, and avoiding the use of intrusive features such as constant tracking;<br>• the principle of transparency towards the child by clearly explaining which parental controls are being used;<br>• the principle of security of the child's data, in order to ensure that third parties do not have access to information about the child (e.g. the child's geolocation data). | While a number of the recommended measures above allow for parental control and involvement in their child's online experiences, it is vital that organisations processing children's personal data understand that data protection by design and default does not simply mean unilaterally delegating responsibility to parents/ guardians to turn settings and features off on their child's account in order to reach the higher level of protection for children's data required by the GDPR. |