

A HIGH LEVEL OF PRIVACY, SAFETY & SECURITY FOR MINORS

A best practices baseline for the
implementation of the Digital Services
Act for children

February 2024



**5RIGHTS
FOUNDATION**

Supported by



**CHILD
RIGHTS
INTERGROUP**



Eurochild
Putting children at
the heart of Europe

Forewords

The digital world has transformed childhood, bringing with it incredible new opportunities, but also new risks. One in three internet users is a child and, in Europe, technology shapes almost every aspect of their lives and development. The digital world was however not designed for children and does not recognise them, their rights or their needs. Curating their education, their relationships and their play, experts in attention retention and engagement have taken the place of child development specialists.¹ Parents, teachers, and children themselves feel frustrated, and too often scared. “Online I cannot be a child – only an underage adult”, noted one child 5Rights spoke to. “Help us switch off as well as on. We need some thinking and growing time”, said another. It is high time to give children back their childhoods and ensure the digital world is designed for them – and not just corporate profits – to thrive. In passing the Digital Services Act, the European Union aims to do just that. Implemented thoughtfully and enforced robustly, it will lay the foundations for the development of technology that will serve children and society for generations to come. Ahead of the coming into full force of this historic law on 17 February 2024, this report is 5Rights’ contribution to those foundations, upon which we will build the digital world children and young people deserve.



Leanda Barrington-Leach
Executive Director, 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.

¹ To find out more about how children experience the digital environment and the risks they face, see 5Rights Foundation: [Disrupted Childhood: The Cost of Persuasive Design \(2023\)](#); [Pathways: How Digital Design Puts Children at Risk \(2021\)](#); [Risky-By-Design interactive microsite](#); 5Rights-LSE joint research centre [Digital Futures for Children](#).

The implementation of children's established rights in the digital environment is a priority for the European Parliament, as reflected in numerous positions, which note with consistent concern the risks and harms children are facing online, and the importance of safety by design approaches to corporate due diligence.² The Parliament, notably through the work of the Child Rights Intergroup that we have the honour to preside, substantially enhanced key provisions of the Digital Services Act for children, in particular to ensure a high level of privacy, safety and security for minors across all online platforms. As these provisions come into force, we look forward to seeing them diligently implemented, and will work to support and monitor their enforcement in close cooperation with the European Commission and the Board of national Digital Services Coordinators. To this end, we warmly welcome this report from the 5Rights Foundation, setting out a best practices baseline for the guidelines and other implementing measures that will be critical to ensure the DSA delivers on its promise to children, and to European society as a whole.



*David Lega MEP (EPP, Sweden)
Co-Chair, Child Rights Intergroup*



*Catharina Rinzema MEP (Renew Europe,
Netherlands) Vice-Chair, Child Rights Intergroup*



*Milan Brglez MEP (S&D, Slovenia)
Co-Chair, Child Rights Intergroup*



*Emilio Puccio
Secretary General, Child Rights Intergroup*

About the European Parliament Child Rights Intergroup

The Child Rights Intergroup is a cross-party, cross-national group of more than 85 committed Members of the European Parliament, who work together with child-focused organisations to keep children's rights on top of the EU agenda. The aim of the Intergroup is to promote children's rights and ensure that the best interest of the child is taken into account in EU internal and external action.

² *Inter alia* European Parliament [Resolution](#) of 17 January 2024 on virtual worlds – opportunities, risks and policy implications for the single market (2022/2198(INI)); [Resolution](#) of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI)); [Resolution](#) of 5 October 2023 on the new European strategy for a better internet for kids (BIK+) (2023/2670(RSP)); [Resolution](#) of 18 January 2023 on consumer protection in online video games: a European single market approach (2022/2014(INI)); [Resolution](#) of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI)); [Resolution](#) of 11 March 2021 on children's rights in view of the EU Strategy on the rights of the child (2021/2523(RSP)); [Resolution](#) of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child (2019/2876(INI)).

The digitalisation of our society is imposing new challenges for children. While they benefit from the developmental, social and entertainment opportunities that online environments bring, children are increasingly exposed to evolving risks, with disastrous repercussions on their mental health and general well-being, as reported by Eurochild members³. In fact, children's rights that seem to be consolidated offline, are far from being guaranteed online. The Digital Services Act is a milestone that will certainly advance in digital environments and enable children to exercise their rights online. However, it needs to be operationalised with a child rights approach based on the UN Convention on the Rights of the Child, to ensure it delivers effectively for children. This means that all aspects of children's rights, including privacy, protection, participation, and provision, should be equally considered, with primary consideration for the best interests of the child. As an umbrella organisation of which the 5Rights Foundation is a member, we believe the following set of good practices can prove useful in guiding regulators and online platforms to ensure safer and more age-appropriate online experiences for children by design.



Sabine Saliba
Secretary General, Eurochild

About Eurochild

Eurochild is the leading network of organisations and individuals working with and for children in Europe. With 200 members in 42 countries, we strive for a society where all children and young people grow up happy, healthy, confident and respected as individuals in their own right. We aim to bring about positive changes in the lives of children, in particular those affected by poverty and disadvantage.

³ [Paving the way to realise children's rights online in Europe](#), 2024, sub-report elaborated on the basis of Eurochild 2023 report on children in need across Europe - "Children's Rights: Political will or won't?".

Sometimes I feel like all the responsibility is put on me. We don't need to be wrapped in cotton wool, but there should be a basic level of safety, so we then have the power to take responsibility. That would be fairer than what happens now.

5Rights Young Adviser



Introduction

The Digital Services Act (DSA) aims to ensure “responsible and diligent behaviour by providers of intermediary services” which the EU deems “essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights.” Children’s rights come high on this list, and, recognising that “the protection of minors is an important policy objective of the Union”, the DSA sets out specific measures to this end. Rules for all online platforms – banning manipulative dark patterns (Article 25), requiring diligent and proportionate enforcement of terms and conditions (Article 14), action against illegal activity and content (Articles 9, 16, 18, 22 and 23) and high transparency (Articles 15, 24, 26 and 27) – are notably complemented by a requirement to take children out of the advertising business model by banning their profiling for advertising and a broad obligation for all providers of online platforms to “put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service” (Article 28).

The DSA calls for the upholding of best practices and mandates the European Commission and Board of Digital Services Coordinators to develop Guidelines for the application of Article 28(1). This paper aims to bring together existing law and best practices, providing a baseline for the Guidelines that are critical for the DSA to deliver for children.

Our focus here is on the minimum standards of privacy, safety and security to be upheld by all online platforms – big or small. The largest among them face however additional requirements under the DSA. They must ensure their services assess and mitigate any risks to the full enjoyment of the Rights of the Child – extending well beyond their rights to protection to also encompass the positive rights, e.g. to participation, to education and to play, that are critical for children’s full empowerment in the digital era. As Thierry Breton, European Commissioner for the Internal Market, said: “Our main goal is to empower children and to help them navigate the internet confidently”.⁴ This baseline is therefore just that – a floor, not a ceiling. Rising above it will hopefully be an ambitious EU Code of Conduct on Age Appropriate Design that will inspire a new era of innovation, for the benefit of future generations.

⁴ Opening remarks by Thierry Breton, European Commissioner for Internal Market, Safer Internet Forum 2023, <https://www.youtube.com/watch?v=KrsvTshuAeA>.

“The protection of minors is an important policy objective of the Union. [...]

Providers of online platforms used by minors should take appropriate and proportionate measures to protect minors, for example by designing their online interfaces or parts thereof with the highest level of privacy, safety and security for minors by default where appropriate, or adopting standards for protection of minors, or participating in codes of conduct for protecting minors.

They should consider best practices and available guidance [...].

Providers of online platforms should not present advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.”

Digital Services Act (Recital 69)

Contents

Part I – Legal and policy context	11
International legal and policy framework for children’s rights in the digital environment	11
EU legal and policy framework for children’s rights in the digital environment	12
Part II – Implementing Article 28	15
Is your service accessible to children?	15
Does your service offer a high level of privacy, safety and security?	19
How to ensure a high level of privacy, safety and security for minors on your service?	20
Data Minimisation and Sharing	21
Default settings	21
Authentication mechanisms	21
Terms and Conditions	21
Detrimental use of data	22
Profiling	22
Geolocation, microphone and camera	22
Dark patterns	22
Parental controls	25
Reporting, complaints and redress	25
Conclusions	27
About 5Rights Foundation	3
Acknowledgements	27

“Children shall have the right to such protection and care as is necessary for their well-being. In all actions relating to children, whether taken by public authorities or private institutions, the child’s best interests must be a primary consideration.”

**European Charter of Fundamental Rights
(Article 24)**

Part I – Legal and policy context

The DSA does not exist in a vacuum. It should be interpreted and implemented in line with international law and taking into account established policy, regulation and standards.

International legal and policy framework for children’s rights in the digital environment

The Rights of the Child – to which the DSA refers and which the EU is Treaty-bound to protect and promote – are set out in the 1989 UN Convention of that name (UNCRC), to which all EU Member States are party.⁵ The Convention defines a child as anyone under the age of 18 and establishes that the best interests of the child must be a primary consideration in all actions concerning children. It sets out a host of interdependent rights, including (but not limited to):

- Protection from all forms of physical or mental violence, injury or abuse (Article 19), from economic exploitation (Article 32), from all forms of sexual exploitation (Article 34), and from all other forms of exploitation prejudicial to any aspects of the child's welfare (Article 36)
- The right to development (Article 6) and the enjoyment of the highest attainable standard of health (Article 24)
- The right to privacy (Article 16)
- The right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds (Article 13), to freedom of thought (Article 14), and to be heard (Article 12)
- The right to education (Article 28), to access to information from a diversity of sources, and protection from injurious material (Article 17)
- The right to rest and leisure, to engage in play and recreational activities appropriate to the age of the child (Article 31).

In 2021, the UN Committee on the Rights of the Child adopted its [General comment No.25](#) elaborating how the Convention applies in the digital environment, and building on [General comment No. 16](#) regarding the responsibilities of business providers. Its provisions include:

- Ensuring that in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interest of every child is a primary consideration (Para. 12 -13)
- Requiring digital service providers to offer or make available services to children appropriate to their evolving capacities (Para. 19-21)
- Requiring businesses to undertake child rights due diligence, in particular child rights impact assessments, and holding them accountable for preventing their networks or services from being misused for purposes that threaten children’s safety and well-being (Para. 36-38)
- Requiring that businesses adhere to the highest standards of ethics privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of

⁵ Treaty on the European Union, Article 3(3) and Charter of Fundamental Rights of the European Union, Article 24.

their products and services (Para. 39); and that they comply with relevant guidelines standards and codes and enforce lawful necessary and proportionate content moderation rules (Para. 56)

- Prohibiting by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling (Para. 42)
- Ensuring that automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development (Para. 62)
- Taking legislative and other measures to ensure that children's privacy is respected and protected by all organisations and in all environments that process their data. States should require the integration of privacy-by-design into digital products and services that affect children (Para. 70)
- Regulating against known harms. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children's development and rights (Para. 96)
- Introducing or using data protection, privacy-by-design, safety-by-design and other regulatory measures to ensure that businesses do not target children using techniques designed to prioritise commercial interests over those of the child. Examples of such techniques are opaque or misleading advertising or highly persuasive or gambling-like design features (Para. 110).

The 2018 Council of Europe [Guidelines to respect, protect and fulfil the rights of the child in the digital environment](#), 2020 International Telecommunications Union [Guidelines on Child Online Protection](#), and 2021 OECD [Recommendation on Children in the Digital Environment](#) reinforce this international framework which should inform the implementation of the DSA. The OECD Recommendation called on States to:

- Pay due regard to providing a safe and beneficial digital environment for children through the design, development, deployment and operation of such products and services, including through taking a safety-by-design approach to address risks
- Provide information that is concise, intelligible, easily accessible and formulated in clear, plain, and age-appropriate language
- 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 using children's data in ways evidence indicates is detrimental to their wellbeing
- 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.

EU legal and policy framework for children's rights in the digital environment

In line with its Treaty and international obligations, the EU has worked to prioritise implementing children's rights in the digital environment. The [2021 EU Strategy on the Rights of the Child](#) recognised the UNCRC General comment No. 25 and called on ICT companies to ensure that "children's rights are included in digital products and services by design and by default". Revised in 2022 with due recognition also of the General comment No. 25, the [European Strategy for a Better Internet for Kids](#) aims to ensure that every child is protected, empowered and respected online, with a strong emphasis on age appropriate digital services. In 2023, the [European Declaration on Digital Rights and Principles for the Digital Decade](#) committed the Union to promoting positive experiences for children in an age appropriate and safe digital environment and to protecting all children against illegal tracking, profiling and targeting, in particular for commercial purposes. And in November of that year, the EU co-sponsored [United Nations](#)

[General Assembly Resolution](#) reiterated the commitment of the Union and Member States (as well as the other members of the UN) to the effective implementation of children's rights in the digital environment, as set out in UNCRC General comment No. 25.

An increasingly robust body of EU law aims to implement and enforce the rights of the child in the digital environment. Notably:

- The [General Data Protection Regulation](#) (GDPR) provides for additional protections for children's data (Recitals 38 and 58)
- The [Audio-Visual Media Services Directive](#) prohibits the processing of a minor's personal data for commercial purposes and requires video-sharing platform services to take appropriate measures for the protection of minors (Articles 6a2 and 28b)
- The [General Product Safety Regulation](#) recognises the health risks posed by digital products especially for children (Recital 23)
- The [draft AI Act](#) bans systems that exploit the vulnerabilities of any persons due to their age (Article 5) and requires high risk systems to consider whether they are likely to adversely impact children (Article 9)
- The draft [Regulation laying down rules to prevent and combat child sexual abuse](#) prescribes a strong prevention and safety by design approach.⁶

The European Parliament has issued a number of Reports and Resolutions emphasising the will of the co-legislature to ensure further protections for children's rights in the digital environment. The Parliament notably calls for:

- The recognition of the specific needs, vulnerabilities and rights of children and for the design and operation of online services and products safe for children by design and by default – in its 2024 [Resolution on virtual worlds – opportunities, risks and policy implications for the single market](#)
- The promotion and implementation of policy initiatives and industry standards on safety by design in digital services and products for children, and for the best interests of children to be the primary consideration in their design – in its 2023 [Resolution on addictive design of online services and consumer protection in the EU Single Market](#)
- The highest available standards of safety, security and privacy by design and by default for AI systems that are likely to interact or otherwise affect children – in its 2022 [Resolution on Artificial Intelligence in a digital age](#)
- Online games directed at minors to meet the highest standards by design and by default when it comes to safety, security, privacy – in its 2023 [Resolution on consumer protection in online video games: a European single market approach](#).

Finally, the EU standardisation organisations CEN and CENELEC in 2023 adopted a [Workshop Agreement on age appropriate design of digital services](#), establishing a clear process for digital service providers to follow when designing products and services accessible to children.

⁶ See also European Parliament (2023) [Report on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse](#).

Services should assume that young people are going to be on it because young people are all over the internet. The internet is our oyster.

5Rights Young Adviser



Part II – Implementing Article 28

Taking into account the legal and policy context outlined above, this section provides practical guidance for the implementation of the DSA requirement for providers of online platforms to ensure a high level of privacy, safety and security of minors on their service, based on international best practice.

Is your service accessible to children?

The rights of the child are, according to international law to which all EU member states are subject, universal (meaning they apply to all under 18s), inherent (theirs from birth), inalienable (cannot be taken away), unconditional (without conditions attached) and indivisible (all equally important). Among other things, this means that the rights follow the child and apply wherever they are, whether a field, a home, a classroom or a digital platform. As set out above, the UNCRC General comments No. 25 and No. 16 specify the obligations of all business entities, including providers of digital products and services, to respect the rights of the child.

The DSA seeks to go further than these broad obligations by establishing specific due diligence obligations, with regulatory oversight, for companies judged to pose the highest risk. Thus, while children do not forfeit their rights when visiting the website of a bank or a transport provider for example, and these companies retain their responsibilities to respect the rights of any child they interact with, the DSA introduces a regulatory regime requiring “providers of *online platforms accessible to minors*” to ensure them a high level of privacy, safety, and security (Article 28).

An online platform is a service that stores and disseminates information to the public, so this would include all social media platforms, gaming platforms with streaming or chatrooms, search engines and many education technology products among others.

“An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes.” Digital Services Act (Recital 71)

Online platforms accessible to minors include any that do not in their terms and conditions restrict their usage to over 18s – terms they are bound to diligently enforce as per the DSA Article 14. This covers the vast majority of services children use.⁷

Even when a platform’s terms and conditions restrict usage to over 18s, it is in scope if the service can be considered “directed at” minors. This could be for instance because the nature and content of the service or a feature thereof is known to have particular appeal for children,

⁷ Youtube, WhatsApp, TikTok, Snapchat, Instagram and Facebook are the most commonly used online platforms by children – none restrict their usage to over 18s; see OFCOM (2023) [Children and Parents: Media Use and Attitudes](#).

because it is similar to services known to be used by children, because it is promoted to children (e.g. through a lower age rating in an app store, or through advertisement to children or in spaces with significant proportions of children), or because internal or external market research identified under 18s as a market for the service.⁸

Furthermore, a platform is considered accessible to minors where the provider is aware that “some” users are children. Given that GDPR requires all services to obtain parental consent before processing the data of users under ages ranging from 13 to 16 depending on the Member State, such awareness can in those cases be presumed. For children between the age of consent and majority, some of the ways in which a provider will be aware of child users include through data processing for service personalisation, by means of internal or external research, or through direct notification by a user (e.g. through the individual complaints system required by Article 16).

It is important however to note that there is no obligation to assess age in the DSA. **Service providers can ensure they are compliant by ensuring a high level of privacy, safety and security for all users – certainly a best practice.**

If a provider chooses to offer a service that does not meet this bar and is not appropriate for children, the provider should ensure it is not accessible to them, by means of appropriate and proportionate age assurance measures. While approaches may vary, there are a set of interdependent and interconnected common standards considered best practice, and reflected in technical standards being developed by International Standardisation organization, the European standardisation bodies ETSI and CEN-CENELEC, or other international organisations such as the Institute of Electric and Electronic Engineers (IEEE).

Appropriate and proportionate age assurance measures:⁹

- Adhere to data minimisation in order to be privacy-preserving, only collecting data that is necessary to identify the age, and age only, of a user
- Protect the privacy of users in line with GDPR and other data protection rules and obligations
- Are proportionate to the risk of harm arising from the service, or a feature of the service, and the purpose of the age assurance solution used
- Are easy for children to understand and considerate of their evolving capacities
- Are secure and prevent unauthorised disclosure or safety breaches
- Provide routes to challenge and redress if the age of a user is wrongly identified
- Are accessible and inclusive to all users, particularly those with protected characteristics
- Do not restrict children from services or information that they have a right to access
- Provide sufficient and meaningful information for a user to understand how the age assurance system works, in a format and language they can easily understand – including children
- Are effective in assuring the actual age, or age range, of a user
- Anticipate that users may not tell the truth, and do not rely solely on this information.

⁸ CEN-CENELEC (2023) [Workshop Agreement 18016 Age Appropriate Digital Services Framework](#), Section 5 and 8; UK Information Commissioner’s Office (2020) Age Appropriate Design Code, [Services covered by this Code](#); Federal Trade Commission (accessed 2024) [Complying with COPPA: Websites and Online Services Directed to Children, including mixed audience sites and services](#).

⁹ CEN-CENELEC (2023), Section 8.

Any age and parental consent verification systems should [...] respect the following rules:

- **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 facial recognition would therefore be disproportionate.

- **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.

- **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.

- **SIMPLICITY**

The use of simple and easy-to-use solutions that combine verification of both age and parental consent could be encouraged.

- **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.

- **THIRD PARTY INTERVENTION**

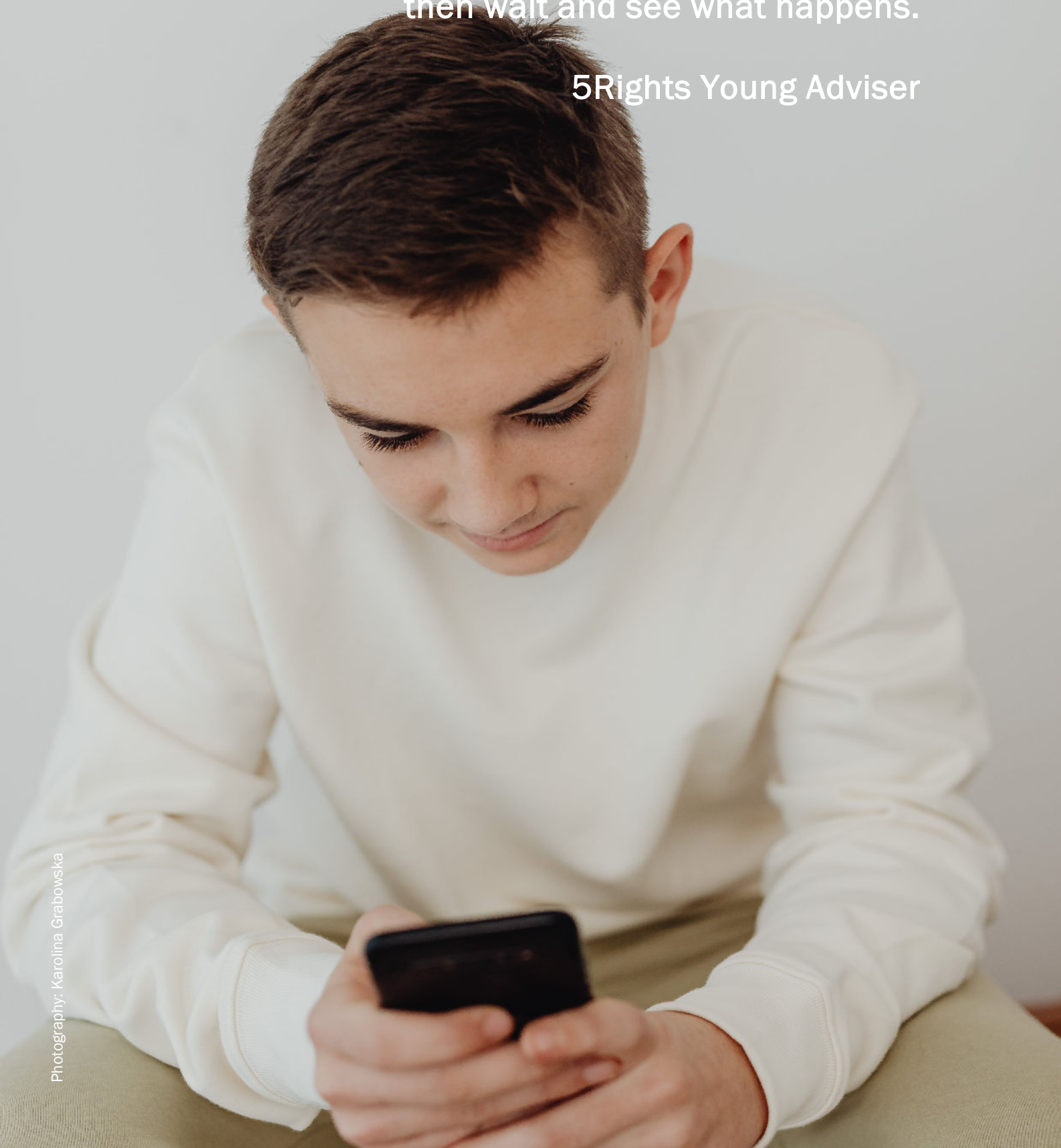
Age verification systems based on the intervention of a trusted third party who can check a data subject’s identity and status (attribution of parental authority) could be investigated in order to meet the requirements as described above.

[CNIL Recommendations on the Digital Rights of Children \(France\)](#)

Services should actually think about the negative effects their features have, even if they don't mean for those effects to happen.

They shouldn't just push out new features and then wait and see what happens.

5Rights Young Adviser



Does your service offer a high level of privacy, safety and security?

Knowing whether measures need to be taken to protect children on a service accessible to them requires some assessment of the privacy, safety and security risks they may face. The data protection impact assessments (DPIAs) required by GDPR, if combined with specific consideration of children’s vulnerabilities, provide a solid basis for this process, and practical tools exist to support companies with this exercise,¹⁰ as do human rights impact assessments (HRIAs) that have long been central business responsibility toolkits.¹¹ The subset of Child Rights Impact Assessments (CRIAs)¹² are frameworks to help companies ask the right questions – ideally as they design their services or any new features but also thereafter and at regular intervals¹³ – with due regard to children’s specific needs and vulnerabilities, so as to know whether they are providing minors with the level of privacy, safety and security required by the law, and address any gaps or weaknesses.¹⁴

In undertaking a CRIA, digital service providers consider how children of varying ages and vulnerabilities (are likely to) interact with their service and the risks their service, individual features or functionalities thereof – alone or in combination, intentionally or not – pose to children.¹⁵ These risks can be broken down into categories known as the “4Cs”, recognising that online risks arise when a child: ¹⁶

- Engages with and/or is exposed to potentially harmful CONTENT
- Experiences and/or is targeted by potentially harmful CONTACT
- Witnesses, participates in and/or is a victim of potentially harmful CONDUCT
- Is party to and/or exploited by a potentially harmful CONTRACT or COMMERCIAL pressure.

A fifth C is that of CROSS-CUTTING risks which cut across all risk categories, such as privacy (interpersonal, institutional and commercial) risks, advanced technology (e.g. AI, Internet of Things, Predictive Analytics and Biometrics) risks, and risks to health and wellbeing.¹⁷

A CRIA can also identify positive contributions, how a service, feature or functionality thereof, can enhance children’s privacy, safety, security or enjoyment of their other rights, and may potentially be further developed or promoted.

A CRIA is a process aiming to ensure the right questions are asked, that the right expertise is sought (including input from children), that evidence of benefits, risks and harms is gathered, rights weighed and options tested, that choices are made that deliver the best outcomes for all – prioritising the best interests of the child – that responsibilities are allocated and follow-up ensured. The CRIA is not prescriptive or interfering with innovation, but, when properly documented, allows the company to demonstrate its due diligence, and the regulator (and researchers) to assess this, in its own right as well as against real world outcomes for children. When made public, a CRIA is also a key transparency tool, contributing to consumer trust.

¹⁰ The UK Information Commissioner’s Office provides specific guidance [on how to undertake a DPIA taking into account the rights of the child](#) as well as specific examples, related to [online retail](#), [mobile gaming apps](#) and [connected toys](#).

¹¹ OHCHR (2011) [Guiding Principles on Business and Human Rights](#), Principle 18.

¹² Digital Future Commission (2021) [Child Right Impact Assessment: A tool to realise children’s rights in the digital environment](#), p.6.

¹³ Idem, p.10; OHCHR (2011) [Guiding Principles on Business and Human Rights](#), Principle 18.

¹⁴ The CRIA as described here is a process focused on identifying and mitigating risks to children’s privacy, safety and security. The CRIA prescribed under Article 34 for Very Large Online Platforms could integrate this work but must go further to consider all risks to the full rights of the child – a much broader spectrum as set out in the UNCRC and its General comments.

¹⁵ UNCRC General comment No. 25, Para. 38; UNCRC General comment No. 16, Para. 78; Council of Europe (2019) [Handbook for policy makers on the rights of the child in the digital environment](#), p.19; also see UNICEF, LEGO, ITU, ENOC etc from Digital Futures Commission (2021), p.6; on their national use see Digital Futures Commission (2021), p.14 and on industry examples see Millicom (2017) [Assessing the Impact of Mobile Network Operators on Children’s Rights: the Millicom experience](#), GSMA (2019) [Enhancing Children’s Lives through Mobile](#), UNICEF (2021) [Model Child Rights Impact Assessment Tool for mobile operators](#).

¹⁶ [The 4Cs: Classifying Online Risk to Children. \(CO:RE Short Report Series on Key Topics\)](#) and the [OECD Typology of Risks. Children in the Digital Environment](#).

¹⁷ Ibid.

Several international standards and best practices detail how to undertake a CRIA, such as the CEN-CENELEC (2023) Workshop Agreement 18086 on '[Age Appropriate Digital Services Frameworks](#)' (point 7.3).

How to ensure a high level of privacy, safety and security for minors on your service?

The Child Rights Impact Assessment (CRIA) process aims to identify risks but also to provide for a mitigation plan to address any risks identified. Undertaken as part of the design process, a CRIA allows a company to design out risks and embed a high level of privacy, safety and security by default.

Privacy, safety and security are highly interconnected. Children's safety – both physical and mental – is too often put at risk due to system design that prioritises the gathering, exploitation and sharing of their data, as well as reach, engagement and content creation for the ultimate aim of monetising attention through advertising. High security – understood as measures, controls and procedures to ensure the integrity, authenticity, availability and confidentiality of data and systems –¹⁸ is essential for both privacy and safety.

GDPR, with its recognition that children merit specific protections for their data,¹⁹ has spurred the development of various codes and enforceable regulatory frameworks for children's privacy and safety in the digital environment, with clear common principles and prescriptions.²⁰ These, adopted by authorities from Sweden²¹ to France,²² from Ireland²³ to the UK,²⁴ all emphasise a precautionary and preventative approach, with the use of Data Protection Impact Assessments (DPIAs) and the embedding of protections for children by design and default.²⁵

These frameworks provide extensive lists of design practices to protect children's privacy and safety, first and foremost though minimising the collection and exploitation of children's data in the first place, and then by setting clear standards for the use of any data collected, building on GDPR and prioritising – as required by the UN Convention – the best interests of the child. Taken together with broader DSA and other EU regulatory requirements and integrating further best practices for children's safety developed by *inter alia* the European Commission, EU national authorities, the Australian e-safety Commissioner,²⁶ and research initiatives such as the Digital Futures for Children centre,²⁷ requirements include (but are not limited to) the following standards.

¹⁸ OECD (2019) [Measuring the Digital Transformation: A Roadmap for the Future](#).

¹⁹ GDPR, Recital 38.

²⁰ 5Rights Foundation (2022), [Approaches to children's data protection: A comparative international mapping](#).

²¹ The Swedish Authority for Privacy Protection, The Ombudsman for Children in Sweden and The Swedish Media Council (Authorities of Sweden) (2021) [Stakeholder Guide: The Rights of Children and young people on digital platforms](#).

²² Ministry of the Interior and Kingdom Relations of the Netherlands (Dutch Ministry of Interior) (2021) [Code for Children's Rights](#); Commission Nationale de l'Informatique et des Libertés (French CNIL) (2021), [8 recommendations to enhance the protection of children online](#).

²³ Data Protection Commission of Ireland (Irish DPC) (2021) [Fundamentals for a Child Oriented Approach to Data Processing](#).

²⁴ UK ICO (2020)

²⁵ European Commission (Accessed 2023) [What does data protection 'by design' and 'by default' mean?](#).

²⁶ Australian eSafety Commissioner (2019) [Safety by Design, Our Vision: Young people](#).

²⁷ 5Rights Foundation & London School of Economics and Political Science, [Digital Futures for Children centre](#).

Data Minimisation and Sharing

Only the minimum amount of personal data needed to provide the elements of the service in which a child is actively and knowingly engaged should be collected and retained.²⁸ Children must have separate choices over which elements they wish to activate. 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.²⁹

Security settings should be high³⁰ and children's data should not be disclosed by the provider unless a compelling reason to do so can be demonstrated, taking into account the best interests of children.³¹ This means for example that children's data should not be reused and shared for commercial or advertising purposes.

Default settings

Settings must be "high privacy" by default unless there is a compelling reason for a different default setting, taking into account the best interests of the child.³² This includes setting children's profiles to private by default.³³

Authentication mechanisms

Authentication mechanisms should be designed in line with a child's capabilities, notably in terms of their ability to retain information long term, their visual acuity and secret keeping.³⁴ Graphical authentication mechanisms can be used as an alternative to password authentication for young children.³⁵

Terms and Conditions

"They should use language that young people actually use and understand. And instead of bombarding us with all the terms right at the start when we sign up, they should give us the information at the time that we need it. For example, when I want to upload a photo, why don't they tell me at that moment what they'll do with it so I can make a better choice? Or they could do it as a pop-up or a video." 5Rights Young Adviser

The terms and conditions that children (or their parents/guardians on their behalf) consent to must be transparent, fair, age appropriate, and duly implemented and enforced (as per the DSA Article 14). All terms, policies and community standards must be easy to find for children, concise, and in both format and language suitable to the age and needs of the child.³⁶ Non-textual messages, such as cartoon, videos, images, icons or gamifications, can be helpful.³⁷ Terms should also be presented in short and timely notifications along the user journey to ensure meaningful engagement, including at the point that specific options are activated.³⁸

²⁸ Importance of data minimisation: UNCRC General comment No. 25, Para. 69.

²⁹ Dutch Ministry of the Interior (2021), Principle 3.

³⁰ OECD (2022) [Recommendation of the Council on the Digital Security of Products and Services](#); John Dempsey et al. (2016) [Child Centred Security](#).

³¹ UK ICO (2020), Principle 9; John Dempsey et al. (2016) [Child Centred Security](#).

³² French CNIL (2021), Recommendation 8; Irish DPC (2021), Fundamental 14; UK ICO (2020), Principle 7; Dutch Ministry of the Interior (2021), Principle 6; Swedish Authorities, (2021), Chapter 2.6.

³³ European Commission (Accessed 2023) [What does data protection 'by design' and 'by default' mean?](#).

³⁴ Karen Renaud et al. (2021) [Principles for Designing Authentication Mechanisms for Young Children: Lessons Learned from KidzPass](#).

³⁵ Ibid.

³⁶ UNCRC General comment No. 25, Para. 39; DSA Article 14(3); UK ICO (2020) Principle 4; Irish DPC (2021) Chapter 3; 5Rights Foundation (2021) [Tick to Agree: Age appropriate presentation of published terms](#).

³⁷ Irish DPC (2021), Chapter 3.2.

³⁸ 5Rights Foundation (2021) [Tick to Agree: Age appropriate presentation of published terms](#).

Detrimental use of data

Digital service providers should 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 official advice,³⁹ for example from the World Health Organisation, European Commission or Member State authorities.

Profiling

“Services need to take off some pressure of pushing stuff on us, including all the ads: they are really annoying, and create pressure to buy stuff in games or things that you think will make you look good or be cool.” 5Rights Young Adviser

Options which use profiling should be off by default (unless the provider can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child).⁴⁰ Profiling should only be implemented if appropriate measures are in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing), and never for the purpose of targeted advertising.⁴¹

Geolocation, microphone and camera

“I really disagree with services that reveal your location. It’s just unsafe.” 5Rights Young Adviser

Location tracking, microphone and camera must be off by default (unless for geolocation the provider can demonstrate a compelling reason for this functionality to be switched on by default, taking account of the best interests of the child) and return to “off” after each use. Whenever a child’s location, sound or video are being recorded or shared, there must be a clear and obvious signal to the child, at all times.⁴²

Dark patterns

“At the moment services are just trying to keep us online for longer, so they can show us more ads and get us to spend more money. And some of the ways they do that are so sneaky, but they’re also so effective that even when I know they’re doing it and it annoys me, I still find it hard to switch off.” 5Rights Young Adviser

“Practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions” or which “can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them” are banned under DSA Article 25.⁴³

³⁹ OECD (2022) Guidelines for Digital Service Providers; UK ICO (2020), Principle 5

⁴⁰ UK ICO (2020), Principle 12; Dutch Ministry of the Interior (2021), Chapter 6; GDPR, Recital 71; Swedish Authorities (2021), Chapter 2.12.

⁴¹ DSA, Article 28(2).

⁴² UNCRC General comment No. 25 (2021), Para. 40; Global Privacy Assembly (2021) [Adopted Resolution on Children’s Digital Rights](#), Point IV; UK ICO (2020), Principle 10; French CNIL (2021), Recommendation 6; Swedish Authorities (2021), Chapter 2.10.

⁴³ DSA, Recital 67 and Article 25.

Such practices, also often known as persuasive design techniques, are highly problematic for children’s privacy and safety.⁴⁴

In designing their products and services, providers must prioritise the best interests of the child over commercial interests. In particular, they should ensure design is not “sticky”, that all functions to extend use or promote reach are turned off by default and that clear and accessible information is provided in a timely manner at the point of access to ensure and promote thought-through, autonomous decisions by the child. Existing rules and guidance instruct providers to:

- Not use nudge techniques to persuade or encourage children to provide unnecessary personal data, activate options which are not in their interests, or weaken or turn off their privacy protections.⁴⁵ Refrain from presenting choices in a non-neutral manner, repeatedly requesting to make a choice where a choice has already been made, making certain choices more difficult or time-consuming than others or default settings difficult to change to a higher privacy setting.⁴⁶ Build in warning measures or positive prompts for when a child tries to lower default security or privacy settings or make potentially sensitive content public.⁴⁷ Design important decisions in several steps with a delay to give the child time to think.⁴⁸
- Not use or activate for children techniques⁴⁹ aiming at maximising a user’s engagement, time spent on the service and/or reach. Examples of such design features are auto-play functions, push notifications, endless scrolls, random-reward features, popularity metrics, incentives to produce and share content, and techniques to apply time pressure or build anticipation.⁵⁰ In addition to avoiding such harmful techniques, positive measures can include making it easy to save and pause (e.g. at any point in a game), encouraging breaks, turning off notifications for children during the night and making it easy to turn them off anytime.
- Turn off recommender systems by default for minors, including for content or friend/follower recommendations, which impact upon children’s right to access a diversity of information, their freedom of thought and action, as well as their safety – both physical and mental. When turned on based on an informed and autonomous decision by the child, s/he should be able to easily modify or influence the main parameters of the recommender systems.⁵¹
- Not expose children to undue or inappropriate commercial pressure, through *inter alia* targeted advertising (banned under Article 28 DSA), influencer placements, in-app or in-game purchases (especially when combined with persuasive design techniques to encourage purchases such as e.g. artificial scarcity in games, or gambling-like features), and advertisements disguised as user/entertainment content or games. The DSA requires all advertisement, both paid for and user generated, to be clearly and consistently labelled.⁵²

⁴⁴ 5Rights (2023) [Disrupted Childhood: The cost of persuasive design](#); 5Rights (2021) [Pathways: How digital design puts children at risk](#); UNCRC General comment No. 25, Para. 110; European Parliament (2023) [Resolution on addictive design of online services and consumer protection in the EU single Market](#).

⁴⁵ UK ICO (2020), Principle 13; Dutch Ministry of the Interior (2021) Principle 6

⁴⁶ Swedish Authorities (2021), Chapter 2.2 - 2.13.

⁴⁷ OECD (2022) [Recommendation of the Council on the Digital Security of Products and Services](#); John Dempsey et al. (2016) [Child Centred Security](#).

⁴⁸ Swedish Authorities (2021), Chapter 2.6.

⁴⁹ DSA Recitals 67, 71 and Article 25.

⁵⁰ 5Rights (2021) [Pathways: How digital design puts children at risk](#).

⁵¹ See DSA, Article 27 on recommender systems.

⁵² DSA, Article 26.

If services know that things are difficult for young people, they should stop doing them.

For example: stop all the scores and streaks, because they encourage people to keep on going to boost their scores even in ways that can be risky or take up time they don't really have; make it easier to sleep or switch off.

5Rights Young Adviser



Parental controls

Parental controls can be an additional tool to support (in particular younger) children, in complement to safety by design and default. They should respect a child's privacy. If parental controls are provided, the child should be given age-appropriate information about the functionality.⁵³ In addition, if they enable the parent or the carer to monitor the child's online activity or track their location, an obvious sign in real time must be provided to the child when they are being monitored.⁵⁴

Reporting, complaints and redress

"I had to make a complaint recently and it was like being stuck in a maze. I kept asking when I would hear back, but they wouldn't give me any info on what was happening to my complaint, who was looking at it and stuff like that. I think they should set out timelines and let us know what the process will be, so we know what to expect and it's not up to us to keep chasing. It's exhausting." 5Rights Young Adviser

Digital service providers must ensure accessible and age-appropriate tools and remedies for children.⁵⁵ Reporting tools, notice and action mechanisms, tools to exercise data protection rights and internal complaint-handling mechanisms should be easily accessible to children and effectively support their privacy, safety and security.⁵⁶ It should be clear to children where they can get support and advice. Reporting tools should be prominent and user-friendly; their use could for instance be highlighted during the sign-up process. Response time should be appropriate to the issue and information should be provided on the actions being taken.⁵⁷ Having a single point of contact and streamlining reporting tools (across providers) would significantly benefit children, who struggle with widely different and complex reporting processes.⁵⁸

⁵³ Swedish Authorities (2021), Chapter 2.11.

⁵⁴ Ibid; UK ICO (2020), Principle 11.

⁵⁵ On the need for remedies for children see: UNCRC General comment No. 25, Para. 36 and Para. 55; Global Privacy Assembly (2021) [Adopted resolution on Children's Digital Rights](#), Point I; UNICEF (2021) [The case for better governance of Children's Data: A Manifesto](#), Principle 6; UK ICO (2020), Principle 15.

⁵⁶ DSA Articles 16 and 20.

⁵⁷ 5Rights Foundation (2021) [Tick to Agree: Age appropriate presentation of published terms](#).

⁵⁸ DSA Article 12; Thorn (2023) [Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking in 2021](#); Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), France (2023) [Combating the dissemination of hate content online: an assessment of the resources implemented by online platforms in 2022 and outlook images](#).

If the business is only
focused on money, the safety
of the platform goes down the
list of things they care about.


5Rights Young Adviser

Conclusions

Thoughtfully implemented, based on existing law and best practice, the DSA has the potential to be transformational for children. To fully deliver on this promise however it also requires robust enforcement. Enforcement requires political will and well-resourced and supported competent authorities. It also requires transparency. Thorough and careful documentation of due diligence measures, combined with meaningful access to data also for researchers, is crucial for regulators to hold companies to account. A high level of transparency – also for users, including children – can build trust and learnings that can spur further positive innovations and best practices. The DSA contains many provisions to this effect. Taken together with a systemic, tech-neutral and outcomes-based approach to children’s privacy and safety as outlined above, they constitute a solid foundation upon which to build the digital world young people deserve.

Acknowledgements

We would like to thank all contributors, and the many experts upon whose work we have built, the network of organisations and individuals who support the rights of children in the digital environment and, most of all, the children and young people whose voices, many cited in this report, underpin our positions and work.



I imagine that the digital world in the 22nd Century will be advanced, brilliant and safe for all children to use effectively and creatively.

5Rights Young Adviser