IMPLEMENTING CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT

A NORDIC DECLARATION

PRINS CARL PHILIPS & PRINSESSAN SOFIAS STIFTELSE

5RIGHTS FOUNDATION

BØRNS VILKÅR

MAY 2023

The Nordic countries are fully committed to upholding children's rights in the digital environment, as codified in the United Nations Convention on the Rights of the Child (UNCRC) and its General comment No. 25. We, the undersigned, commit to prioritising children's rights in our implementation of European and domestic law for regulating the digital environment,[1] with the aim to ensure that children can thrive in online spaces that are safe, designed and operated with their best interests in mind. We will work together to develop, enforce and promote a coherent,

[1] Notably the EU Digital Services Act (2022), the General Data Protection Regulation (2016), the upcoming Artificial Intelligence Act and Regulation to prevent and combat Child Sexual Exploitation and Abuse.

proportionate and effective regulatory framework for digital service providers and operators based on the 3 core principles and 15 standards set out hereunder. This Declaration should serve as blueprint to give concrete content and life to children's rights recognised by international, EU and national law. Compliance with all those instruments, as well as other applicable laws and regulations is the foundation on which this Declaration is built. We hope it can also inform the action of national bodies, companies as well as partner countries.

3 CORE PRINCIPLES

1. ALL UNDER 18S HAVE RIGHTS THAT MUST BE PROTECTED AND PROMOTED

A child is anyone under the age of 18 (Article 1, UNCRC) and all children, including teenagers, have the right to special considerations and the prioritisation of their best interests. Children are and must continue to be active and engaged participants of the digital world. We do not seek to protect children from the digital world but within in. Children should be heard, and provided with protections and opportunities appropriate to their age, and diverse needs.

2. CHILDREN'S RIGHTS APPLY WHEREVER CHILDREN ARE IN PRACTICE, NOT ONLY WHERE WE WANT THEM TO BE

Children must be protected wherever they are online, not only on services specifically designed for them, or targeting them. All services that children access or are likely to access must be safe for them, and take their rights into account.[2]

[2] For guidance on how to determine whether a service is likely to be accessed by children, see for example: https://ico.org.uk/for-organisations/childrens-code-hub/likely-to-be-accessed-by-children/

3. SERVICES MUST EMBED PROTECTIONS FOR CHILDREN BY DESIGN AND DEFAULT

Privacy and safety measures for children must be built into each stage of product design and development processes. Organisations must think and act in anticipation of the risks to children, rather than to address harm after it occurs. They should build a high level of privacy, safety and security into the architecture and functioning of their services, and apply these highest levels of protection by default for children.

15 STANDARDS FOR AGE-APPROPRIATE DESIGN

1. BEST INTERESTS OF THE CHILD

The best interests of the child should be a primary consideration when designing and developing digital services likely to be accessed by children. If there is a conflict between various interests (of users or stakeholders, including commercial interests), the service provider must prioritise the best interests of the child.

2. CHILD RIGHTS IMPACT ASSESSMENTS

Providers should undertake a Child Rights Impact Assessment to assess and mitigate risks to the rights and freedoms of children who are likely to access their service(s). They must consider differing ages, capacities, accessibility and development needs, and the full range of risks to children's privacy, safety and security, covering content, contact, conduct, contract and cross-cutting risks.[3]

3. AGE-APPROPRIATE APPLICATION

Providers must take a risk-based and privacy-preserving approach to recognising the age of individual users and ensure they effectively

[3] Framework developed by the EU CO:RE Project, *EU's Children Online: Research and Evidence - A knowledge base on children and youth in the digital world*, under the Horizon 2020 programme, available at https://core-evidence.eu/posts/4-cs-of-online-risk

apply these standards to child users. They can either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children, or apply the standards to all their users. Any age assurance mechanisms in use must be privacy preserving, proportionate, effective, age appropriate, accessible, transparent and secure.[4]

4. TRANSPARENCY

Published terms, policies and community standards as well as privacy information must be concise, prominent and in language and format that is clear and suited to the age of the child. Additional specific 'bite-sized' explanations should be provided at the point of use or feature activation.

5. DETRIMENTAL USE OF DATA

For children's personal data to be processed fairly, in accordance to GDPR and other applicable data protection laws, it should not be used in ways that have been shown to be detrimental to their wellbeing, or that go against internationally recognized standards, industry codes of practice, other regulatory provisions or Government advice. This includes the use of personal data to extend engagement, recommend harmful content or actions, or to unduly influence children's behaviour, notably via automated processes or dark patterns.

6. DATA MINIMIZATION

Only the minimum amount of personal data needed to provide the elements of a service in which a child is actively and knowingly

[4] Any age assurance system must: respect the principle of data minimization and applicable data protection laws; be proportionate to the risks arising from the product or service and to the purpose of the system; be effective in assuring the actual age or age range; be age appropriate, offering functionality appropriate to the capacity and age of children who might use it; be accessible and inclusive to users with protected characteristics; be transparent, providing sufficient and meaningful information in appropriate format and language to understand its operation, and include remedies to challenge or change decisions; be secure, preventing disclosures or breaches; and not unduly restrict access of children to services to which they should reasonably have access. Upcoming ISO and IEEE technical standards will set out these principles in more detail. For further guidance on age assurance see: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

engaged should be processed; child protection needs should not be construed as a reason to process more data.

7. DATA SHARING

Providers and operators of online services or products must not disclose children's data unless they can demonstrate a compelling reason to do so in the best interests of the child. Particular safeguards should be in place for data processed in educational settings.[5]

8. POLICIES AND COMMUNITY STANDARDS

Published terms, policies and community standards (including but not limited to privacy policies, age restrictions, behaviour rules and content policies) must duly reflect applicable legislation and be upheld, including by providing appropriate moderation and support in local languages.

9. DEFAULT SETTINGS

Default settings must respect children's rights and features designed to extend engagement or influence behaviour must be off by default. Settings must ensure the highest level of data protection and privacy by default (unless services can demonstrate a compelling reason for a different default setting in the best interests of the child).

10. LOCATION TRACKING

Geolocation settings, microphone and camera must be off by default (unless with regards to geolocation there is a compelling reason for it to be switched on by default in the best interests of the child). Services must provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session and require children and/or parents give manual consent before they are turned on.

---

[5] Measures to achieve this should include prioritizing public procurement processes that ensure compliance with the highest level of data protection under the GDPR and other applicable laws such as the ePrivacy directive.

11. PARENTAL CONTROLS

If parental controls are provided, children must be given age-appropriate information about this. If an online service allows a parent, carer or educator to monitor their child's online activity or track their location, an obvious sign must be given to the child when they are being monitored.

12. PROFILING

Options which use profiling must be switched 'off' by default (unless there is a compelling reason for profiling to be on by default in the best interests of the child). Profiling is only allowed 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). Profiling for targeted advertising is forbidden.

13. DARK PATTERNS

Practices that are likely to, or effectively distort or impair children's ability to make autonomous and informed choices are prohibited. These include persuasive design strategies, gambling-style features, hidden costs, unfair terms and conditions, as well as techniques 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 be conceived, designed, tested and produced to include effectively ensure a high level of privacy, safety and security for children, by default and by design.

15. ONLINE TOOLS TO EXERCISE RIGHTS

Providers should ensure that prominent, age-appropriate and accessible tools are available to help children exercise their data protection, privacy and other rights as well as report concerns and access redress mechanisms. Such tools should be specific to the rights they support, where appropriate.

***