Access restrictions to protect children and their rights in the digital environment

Position Paper | January 2026

Overview

5Rights Foundation welcomes the will of the EU and its Member States to take further and robust action to protect children from unsafe and exploitative practices by technology providers and ensure children's rights are fully respected and upheld in the digital age. In view of national initiatives and the proposal to consider complementing established EU legal and regulatory requirements (notably enshrined in the GDPR, AVMSD, DSA and AI Act) with a 'digital age of majority[1] to access social media', 5Rights calls for a thoughtful approach to access restrictions which respects and upholds children's rights[2] and in no manner dilutes or distracts from corporate responsibility for the privacy, safety and security of all children accessing their services.

This position sets out 4 key points:

1. All under 18s have specific rights to protection and enjoyment of age-appropriate experiences, wherever they are. Older children must not be forgotten, and all services where children are in practice must be safe for them.
2. Access restrictions should be thoughtfully implemented as part of age-appropriate design and in line with existing law:
    - Personalised services - including social media but also many games and AI chatbots - should by default not be accessible to children under 13.[3]
    - Tiered age-appropriate access restrictions should protect all children, including teenagers, from high-risk features.
3. Access restrictions must not be implemented in isolation, but complemented by other measures to protect, support and empower children through age-appropriate design of service.
4. Children should not be banned from accessing the digital world, but companies that exploit them should be banned from accessing them. New burdens must not be put on children or parents; instead, regulators must urgently and robustly enforce market access restrictions against tech companies that fail to comply with the law.

[1] The age of majority is set at 18 by the UN Convention on the Rights of the Child – a definition reflected across many core EU regulations designed to protect children and their rights in the digital environment, that refer to 'minors'. See e.g. European Commission: EU actions on the rights of the child. Under the UNCRC, the rights follow the child, and apply at all times and in all environments. Care should be taken with this terminology: establishing a new age threshold and calling it a 'digital age of majority' could undermine the rights of minors under that threshold. All children deserve protection until they reach the age 18, and providers are accountable for respecting and upholding the rights of younger and older children.

[2] The Convention on the Rights of the Child has been ratified by all EU Member States. Its General comment No. 25 sets out how these rights apply in the digital environment. According to the Convention, any restrictions on children's civil rights and freedoms must be lawful, necessary and proportionate.

[3] Exceptions for personalised services that have proven to deliver benefits to children in line with their rights (e.g. to play or education) must be governed by robust regulatory safeguards and conformity with technical standards.

Access restrictions: benefits and limitations

The digital products and services children use should be age-appropriate: they should be safe and rights-respecting for the child by design and default. Services – or parts thereof – that are not appropriate for children – whether all under 18s or younger groups – should not be accessible to them. The products and services younger children access should in principle be designed specifically for them, catering to their development needs. As children get older, they should be empowered to access and engage with more of the wider digital world, with appropriate safeguards.

A key principle of age-appropriate design is the introduction of default access restrictions to shield children from features, functionalities, content or conduct that expose them to risk.[4] For example: geolocation should be off by default so as not to expose children's live location; children's profiles should be private by default so strangers cannot target them; notifications should be off by default during the night so as not to disturb children's sleep; content filters should be on by default so children are not exposed to hate, porn or extreme violence; tracking, profiling, personalised recommender systems, engagement metrics and reward loops should be off by default to protect children from addiction and manipulation.

Children support such proportionate default protections.[5] In addition, research shows them to be highly effective, as users rarely adjust the pre-defined default settings.[6]

The temptation to extend access restrictions to entire categories of services through blanket-bans is understandable but misguided. In a hybrid and rapidly digitalising world, restricting children's access to large parts of the online environment is neither desirable nor feasible. There is no evidence that blanket bans work to make children's lives better.[7] On the other hand, they could infringe their right to information, play and participation. Targeting only e.g. 'social media' would leave children exposed to – and likely push them toward – other unregulated (and equally problematic) services such as gaming, AI or EdTech platforms.[8] Implemented in isolation, bans risk shifting responsibility away from companies for safety on their services, leaving children above the 'age gate', and those who circumvent restrictions they see as illegitimate,[9] more exposed to risk than ever.

To be effective, access restrictions must be tech-neutral, targeted and proportionate, catering to children's evolving capacities. They must be part of age-appropriate design and not implemented in isolation, with full responsibility for ensuring rights-respecting outcomes for children remaining firmly on providers.

---

[4] As set out in detail in the DSA's Article 28 Guidelines.
[5] 5Rights Youth Ambassadors (2025a). *Youth consultation on age checks* and (2025b). *Youth consultation on the digital age of majority* (carried out by 5Rights Foundation).
[6] See e.g. as cited by the European Commission [C/2025/5519]: Willis, L. E. (2014). *Why not privacy by default?, Berkeley Technology Law Journal, 29*(1), (p.61) ; Cho, H., Roh, S., & Park, B. (2019). *Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings*. *Computers in Human Behavior, 101*, (p.1-13).
[7] See e.g. https://www.sciencemediacentre.org/expert-comments-on-evidence-on-benefits-and-harms-of-social-media-and-social-media-bans-on-young-people/
[8] EU Kids Online, Statement (2025) : Protecting, not excluding : why banning children from social media undermines their rights
[9] Köhler-Dauner, et.al, (2025) Digital Child Protection in social networks : age verification and age tiered regulation in Europe, p.5

Recommendations:

1. Enforce an explicit legal ban on personalised services to under 13s

Personalised services – including social media but also many games and AI chatbots – should by default not be accessible to children under 13, who do not possess the cognitive maturity needed to critically engage with systems designed to shape their perceptions and influence their behaviour.[10]

Data protection law already prohibits the data-processing activities that underpin these services when the subject is under 13, but compliance and enforcement has been lacking.[11] **The EU must urgently strengthen, clarify,[12] and robustly enforce a tech-neutral prohibition on personalised services for under 13s, explicitly including social media, social games and AI chatbots.**

This tech-neutral approach would protect young children from exploitative and risky practices, without shutting them out of the digital world. They could continue to autonomously use non-personalised, age-appropriate digital services, allowing them to access information and play in dedicated, private, and safe environments. Furthermore, default restrictions should not hinder the development of personalised services that are proven to deliver benefits to children in line with their rights (e.g. to play or education); these exceptions must however be governed by robust regulatory safeguards in addition to established requirements for verified parental co-consent.[13]

2. Implement age-tiered access restrictions as part of a wider framework for age-appropriate design

All under 18s have specific rights to protection and enjoyment of age-appropriate experiences, wherever they are. Older children must not be forgotten. The teenage years present critical vulnerabilities in terms of child development.[14] While teenagers should gradually have access to more of the digital world, including personalised services, inbuilt guardrails and support mechanisms are essential for older children who are exposed to a wider range of risks with lower parental supervision.[15]

Tiered age-appropriate access restrictions should protect all children, including teenagers, from features, content and spaces that are high-risk for their age. They should ensure that all children are protected, according to their evolving capacities, as they access the digital world in increased autonomy.

---

[10] See Köhler-Dauner, et.al, (2025) Digital Child Protection in social networks : age verification and age tiered regulation in Europe, p.6

[11] Recital 38 GDPR asserts that children merit specific protection for their personal data. It can also be understood that processing children's data is likely to be high risk to children's rights and freedom and should be thoroughly assessed. Article 8 GDPR mentions that parental consent must be given for the processing of children data under an age fixed by Member States, between 13 and 16.

[12] The law should ensure default restrictions and not rely on parental consent. The age of access should be harmonised across the EU, ideally at 13 years.

[13] See CNIL, (2021), *Rechercher le consentement d'un parent pour les mineurs de moins de 15 ans*

[14] 5Rights Foundation, (2023), *Digital Childhood : Addressing childhood development milestones in the digital environment*.

[15] EU Kids Online (2020), *Survey results from 19 countries*, (pp.109-112)

The EU Digital Services Act Art. 28 Guidelines specifically state that: 'Age assurance tools can be used to underpin the age-appropriate design of the service… to ensure that children only have access to certain content, features or activities that are appropriate for their consumption, taking into account their age and evolving capacities'.

The EU must build on the Guidelines and existing standards to produce statutory guidance on age-tiered access restrictions implementing age-appropriate design. This should be tech-neutral and applicable to all products and services likely to be accessed by children,[16] and be built with child development experts and in consultation with children. It should categorise features and functionalities against recommended default settings and access mechanism,[17] and apply a precautionary approach to the roll-out of new innovations to children. The guidance should also identify other best practices for age-appropriate design beyond access restrictions, including strengthening information and consent mechanisms, warnings, positive nudges, safety filters, as well as reporting and remedy functions.

3. Enforce market access restrictions for non-compliant services

Swift and robust action is needed against services, including social media, that are in blatant non-compliance with EU and international law. The EU must make clear that it will not tolerate the commercial exploitation of children or their exposure to known risks and harms by digital service providers. **Children should not be banned from accessing the digital world, but companies that exploit them should be banned from accessing them.** The EU must immediately enforce market access restrictions against tech companies that provide personalised services to under 13s or demonstrably expose children to risk and harm.[18]

Conclusion

A child-rights respecting approach seeks to empower children's civil rights and freedoms as early as possible, and to protect them as long as possible. Access restrictions can be used to support and protect children, when thoughtfully implemented as part of age-appropriate design and firmly grounded in the Rights of the Child. The EU should send a very clear message that when services – or parts thereof – are not safe for children they should not be accessible to them, and that personalised services (explicitly including social media, personalised games and AI chatbots) are not suitable for younger children and require significant safeguards for teenagers. The EU has the tools at its disposal to do this, through implementation, clarification and enforcement of established law. Access restrictions should not be implemented in isolation but within a broader strategy to build a digital world that is private, safe and secure for children. The EU and its Member States should not be distracted from this critical agenda or be seduced by 'silver bullet' solutions that, instead of reshaping the digital world for good, risk both further exposing children and entrenching systemic exploitation.

---

[16] See e.g. Livingstone, S. & Sylwander, K. R. (2025). Conceptualizing age-appropriate social media to support children's digital futures, *British Journal of Developmental Psychology*.

[17] Additional consent (or co-consent with parent/guardian) processes can also be applied for high-risk elements.

[18] In 2021, following the death of a 10-year-old participating in a TikTok challenge, the Italian Data Protection Authority ordered a provisional suspension of TikTok's data processing for users whose age could not be verified, effectively blocking the company's access to younger children. More such actions should be taken under the GDPR, DSA or AI Act.