Attn: Christel Schaldemose, Arba Kokalari, Dita Charanzová, Alexandra Geese, Alessandra Basso, Adam Bielan, Martin Schirdewan, Mikuláš Peksa, Jadwiga Wiśniewska, Henna Virkkunen, Roman Haider, Sabine Verheyen, Geoffroy Didier, Patrick Breyer - DSA Rapporteurs and Shadow Rapporteurs

C/c: Caterina Chinnici, David Lega, Hilde Vautmans– Co-Chairs of the Child Rights Intergroup; Manfred Weber, Iratxe García Pérez, Stéphane Séjourné; Ska Keller, Philippe Lamberts, Raffaele Fitto, Ryszard Legutko – EP Political Group Presidents

Subject: Children's rights in the Digital Services Act

24 March 2022

Honourable MEPs,

The European Parliament two months ago took a historic stand in favour of a better digital world for children, with overwhelming support for provisions requiring services to take into account their rights and best interests (Recital 3), notably by ensuring "a high level of privacy, safety and security by design for minors" (Art 13a.3) and banning targeted ads to minors (Art 24a), based on European standards for age-appropriate services (Art 34.1a).

We – representing more than 2000 children's rights organisations and parents' associations, and speaking on behalf of some 200 million children and parents in the EU – write to you now to urge you to ensure these provisions are not compromised in the final stages of negotiations with the Council.

We understand the French Presidency of the Council has put forward a proposed compromise text, which moves Art 13a.3 to Art 23a and says that "online platforms aimed at or predominantly used by minors" shall ensure a high level of safety, privacy and security by design for minors… These provisions shall "not oblige the provider or online platform to process additional information in order to assess the age of the recipient of the service."

This proposal would empty out the EP's child protection provision in not one but four fundamental ways (set out in more detail in annex to this letter):

- Firstly, by limiting the scope to online platforms which would exclude a whole range of services from most of the gaming industry to search engines to Google Classroom;
- Secondly, by taking almost all the remaining online platforms out of scope by limiting application to those "primarily aimed at minors or predominantly used by them"; thereby excluding the likes of Tiktok and Roblox. The question will be rather what few services remain in scope;
- Thirdly, by undermining system design risk management by including a recital citing examples of relevant targeted measures being – "age verification tools, parental controls, tools aimed at helping minors signal abuse or obtain support" – a list of tools that shift the responsibility back to children and parents; and
- Fourthly, by outlawing age assurance so platforms cannot be required to recognise children on their services and therefore cannot be held accountable for putting them at risk. This would equally render impotent any provision limiting targeted advertising.

Each of these elements is unacceptable and we trust will be firmly rejected by the EP. It is critical that, whatever the final compromise text may be, it fully recognise and take into account the following two principles:

1. **Children's rights apply to all under 18s.** The use of the term "minor" is likely to lead at the national level to conflation with the varying "ages of consent" as established under GDPR. Even when they or their parents/guardian consent to the processing of their data, children do not relinquish their rights. A child of 13 is not an adult, and in many ways older children are at greater risk – since younger children access fewer products and services, have greater adult supervision and spend less time online. All children deserve protection.

2. **Children's rights apply wherever children are in practice.** Children's rights must be upheld irrespective of platform size, of whether a service is specifically designed for children or is predominantly used by them. Most children spend most of their time on services not designed specifically for them, and where – while perhaps present in their millions – they are not the majority of users.

A formulation limiting child protection requirements to services aimed at children or predominantly used by them – especially if "children" are redefined as "minors" – would effectively exempt all but a tiny minority of services used by children from respecting their rights. In this case the DSA would not only fail in practice to deliver a better digital world for children, but would catastrophically set back the fight for the realisation of children's rights in the digital environment.

Children must be recognised online by age assurance mechanisms which are privacy-preserving, and their rights – to access, to age-appropriate services designed with their best-interests in mind and to protection from commercial exploitation – must apply wherever they are. The provision should therefore apply to all "services likely to be accessed by children" [1].

Children and parents, as well as policy-makers around the world, are looking at the EU for leadership. It is imperative that the EU delivers on its values, and fights for all children, and for the full realisation of their rights, in the digital world.

Thanking you for your support, we are sincerely yours,

Baroness Beeban Kidron
Chair, 5Rights Foundation

Victor Petuya
President, European Parents' Association

Guillaume Landry
Executive Director, ECPAT International

Jana Hainsworth,
Secretary General, Eurochild

Aagje Ieven
Secretary General, Missing Children Europe

[1] For a service to be '"likely to be accessed by children", the possibility of this happening needs to be more probable than not. Whether a service is "likely to be accessed by children" will depend upon whether the content and design of the system is likely to appeal to children, and any measures in place to restrict or discourage their access to the service. Alternative language is that of the OECD Recommendation on Children in the Digital Environment and Guidelines for Digital Service Providers, which applies to services "where it is reasonably foreseeable they will be accessed or used by children".

Annex: Analysis of language of French Presidency compromise proposal for Art 23a

1. ONLINE PLATFORMS - Limiting the scope to platforms based on user-generated content (online platforms are defined as "providers of hosting services that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public, again at their request") implies a focus on content and not on the systems and design features of platforms that generate risks to children, and increase the spread and scale of harmful content. It is notably eye-catching that the provision would exclude most gaming services from scope – a massive industry with very substantial impacts on children. Candy Crush, Subway Surfers, The Sims and Homescapes for example are games played by millions of children which include ads, gambling-style features or aggressive promotion of premium features, artificial scarcity and daily rewards. Ed-tech platforms (e.g. Google Classroom) upon which children rely for education would also be out of scope, as would search engines (Google, Alexa…) and any apps that do not have user-to-user functions. It is questionable what aspects of the metaverse or future digital services would be in scope. A narrow definition is already highly problematic based on our current experience, and not future-proof. **Children's rights apply wherever they are and the provision should be applicable to all services "likely to be accessed by children".**

2. AIMED AT OR PREDOMINANTLY USED BY MINORS - The limitation of scope to services that are "primarily aimed at minors or are pre-dominantly used by them" is even more worrying. It would effectively exempt all but a tiny minority of services used by children from respecting their rights. Firstly, most children spend most of their time on services not designed specifically for them, and where – while perhaps present in their millions – they are not the majority of users. This is the case for example with Instagram, Omegle or Clubhouse. **Children's rights apply wherever children are in practice and the rights should follow the child, not any categorisation of service.** Secondly, use of the term "minor" is likely to lead at the national level to conflation with the varying "ages of consent" as established under GDPR. Even when they or their parents/guardian consent to the processing of their data, children do not relinquish their rights. A child of 13 is not an adult, and in many ways older children are at greater risk –since younger children access fewer products and services, have greater adult supervision and spend less time online. Platforms such as TikTok, Roblox, Wink and Among Chat are aimed at and predominantly used by children, but not under 13s. **Children's rights apply to all under 18s.** If this formulation is included, the DSA would not only fail in practice to deliver a better digital world for children, but would catastrophically set back the fight for the realisation of children's rights in the digital environment.

3. NO OBLIGATION TO ASSESS AGE - Saying that tech companies "shall not [be] oblige[d] … to process additional information in order to assess the age of the recipient of the service" is effectively outlawing age assurance. Age assurance that does not rely solely on profiling will always require additional information to establish the age of users. Age assurance is fundamental to ensuring children are delivered age appropriate experiences. This clause will risk giving tech companies a licence to profile children with no limitation. They can on the one hand deny they know age (and claim they have no means to know based on current data) or else use profiling even more extensively on the basis of the data they already have access to in order to deliver services supposedly appropriate for children. Without age assurance tech companies cannot even uphold their own Terms & Conditions setting out minimum ages of access. Age assurance is required by GDPR in order to obtain consent for data processing and in order to provide children with the specific protections for their data that they merit. Such a clause in the DSA would contradict this legal requirement, as well as requirements under e.g. the AVMSD, and other legal requirements regarding e.g. gambling, dangerous substances, access to pornography, etc. All age assurance requires some element of data

processing. Children have a right to age-appropriate services and their presence thus must be established by service providers. **What is important is purpose limitation**, as defined under GDPR so that data collected for the purpose of age assurance is only used for that purpose. **The data processed for age assurance purposes must be the minimum required to meet the purpose, must not be shared, stored or used for any other purpose.**