Additional Contribution to the Targeted Public Consultation on the Guidelines for the Protection of Minors under the Digital Services Act (DSA, Article 28)

June 2025

In addition to the answers provided in the online survey, EuroISPA would like to emphasize the following key points as they are of particular importance for providers of online platform:

1. **Guidelines are merely guidance, not obligations**

It must be clearly mentioned that guidelines are non-binding and should not introduce new legal obligations excluded during the DSA legislative process. They serve as supportive best-practice guidance to assist in implementing and enforcing existing rules. It is crucial that companies retain sufficient flexibility in applying recommended measures. Striking a balance between clear guidance and implementation flexibility is essential to effectively mitigate risks. Adopting a technology-neutral approach will enable services to develop tailored, practical solutions suited to their specific products and functionalities.

2. **Keeping flexibility in age assurance tools**

Age verification systems play a valuable role in protecting minors, particularly by restricting access to age-inappropriate content. However, they are just one of several tools needed and cannot alone address all online risks faced by minors. It is important to recognize that various age verification and assurance methods already in use have demonstrated effectiveness, accuracy, and reliability. Online platforms should retain the freedom to continue employing these proven technologies.

We note that age estimation technologies can now achieve high levels of accuracy and reliability and, when sufficiently precise, should be considered acceptable for verifying age for 18+ content. Depending on the nature of the service and its specific risks, there should also be room for age assurance based on self-declaration combined with AI tools that assess behaviour, writing style, and interests typical of the declared age group.

Emerging solutions like age verification apps and digital identity wallets should be regarded as additional options rather than mandatory replacements for existing systems.

Importantly, the deployment of age verification must not extend so far as to restrict the anonymous use of lawful services or infringe on the right to anonymous communication online. Striking the right balance between protection and informational self-determination remains essential.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56

3. Safeguarding the relationship between Article 28 and Article 34 of the DSA

It must be ensured that the guidelines do not disproportionately extend or duplicate the safety measures for minors already established in Article 28 of the DSA and the complementary risk-based obligations in Articles 34 and following. Particular attention should be given to the fact that Articles 34 and 35 impose additional obligations specifically on VLOPs. The broad scope of the proposed measures creates uncertainty about what further actions VLOPs are expected to take.

Moreover, VLOPs require tailored considerations, as general guidelines—while potentially useful—may not be directly applicable due to their wide scope and the diverse nature of search engines.

4. Strengthening minors' rights and parental control frameworks

The guidelines require notification to minors when guardian tools are activated and recommend safeguards against misuse (e.g., real-time signs of monitoring). There is no explicit requirement for platforms to provide minors with recourse if guardian tools are misused (e.g., excessive surveillance, privacy invasion, or restricting access to support resources). Mechanisms for independent review, complaints, or escalation in cases of misuse would better protect minors' rights.

EuroISPA highlights that account-based parental controls offer a more effective approach compared to device-based solutions. These systems provide greater flexibility and precision, enabling parents to manage settings—such as screen time, app permissions, or content filters—remotely and across multiple devices, without needing physical access. This approach reduces the risk of children bypassing restrictions by switching devices. Furthermore, linking controls to an account allows providers to enforce consistent protections across services (e.g., disabling personalised advertising) and supports stronger security measures, including multi-factor authentication and remote password changes. Account-based systems also enable real-time adjustments, such as blocking a newly downloaded app or adapting settings in response to unexpected situations.

EU-Level Parental Control Framework: Establishing a harmonised EU framework for parental control systems is essential to avoid market fragmentation, ensure consistent levels of child protection across Member States, and promote interoperability and innovation. The European Union could explore new initiatives in this area, drawing inspiration from its work on the "mini-wallet" ecosystem for age verification, to encourage the development of effective, privacy-preserving, and user-friendly parental control tools.

About EuroISPA

Established in 1997, EuroISPA is the world's largest association of Internet Services Providers Associations, representing over 3,300 Internet Service Providers (ISPs) across the EU and EFTA countries. EuroISPA is recognised as the voice of the EU ISP industry, reflecting the views of ISPs of all sizes from across its member base.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56