EuroISPA position paper on the CSAM Regulation

In view of the trilogue negotiations on the proposed regulation issuing rules to prevent and combat child sexual abuse material (CSAM Regulation), EuroISPA would like to share its position.

EuroISPA is deeply committed to the objective of preventing and combatting child sexual abuse and will support efforts to make the digital space safe for all. It is essential, however, that the CSAM Regulation is consistent with processes already established in legislation such as the Digital Services Act (DSA), e-Evidence Regulation, ePrivacy Directive, and the General Data Protection Regulation (GDPR), and that it complies with general principles of cybersecurity and requirements on strong security standards, such as encryption safeguards, as enshrined in the NIS2 Directive.

EuroISPA advocates for strengthening voluntary detection within a clear legal framework that does not impose blanket surveillance nor weaken end-to-end encryption.

1. Encryption, security and surveillance risks

We strongly recommend that the CSAM Regulation avoid any provision which would suggest weakening, circumventing or disabling encryption, privacy or IT security measures at any point in – or prior to – data transmission. The use of encryption technologies, in particular end-to-end encryption, is specifically advised as a key cybersecurity standard by European cybersecurity legislation such as the NIS2 Directive[1]. Therefore, any differing provision in sectoral legislation, such as provisions recommending client-side scanning, would not be compliant with European cybersecurity rules or E2EE principles. Our primary concern is that introducing a system capable of remotely monitoring personal devices – whether smartphones, tablets, or computers – effectively opens a backdoor that could be exploited not only by authorised authorities but also by malicious actors. Such a mechanism risks undermining the security of all users, including those entirely uninvolved in any wrongdoing. Another concern is that the scope of surveillance will not remain confined to social messages but could gradually expand to include any files stored on a device. This raises profound questions about the erosion of privacy protections and other benefits of encryption, and even the constitutional legitimacy of such measures on the basis of the Treaties and the European Charter of Fundamental Rights. Finally, if the system were genuinely secure and trustworthy, it is difficult to justify why certain categories of users are deliberately excluded and shielded from its application. We welcome that the references to potential and mandatory client-side scanning

[1] Recital 98: "In order to safeguard the security of public electronic communications networks and publicly available electronic communications services, the use of encryption technologies, in particular end-to-end encryption as well as data- centric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions, should be promoted. Where necessary, the use of encryption, in particular end-to-end encryption should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services in accordance with the principles of security and privacy by default and by design for the purposes of this Directive".

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

and/or attempts to weaken end-to-end encrypted communication were removed from the Council position. We however recommend adjusting the final text so that in no way – not even as voluntary basis or as part of risk assessment of services – results in weakening or circumventing of encrypted communication or services and/or conflicts with NIS2 Directive rules on cybersecurity.

2. Explicit legal basis for voluntary detection in ICS

To ensure timely and effective responses to child sexual abuse material (CSAM), we recommend that a permanent extension of the ePrivacy derogation for Interpersonal Communication Services (ICS) providers - subject to additional privacy safeguards - be included in the CSAM Regulation. Failing to provide a legal basis for voluntary detection mechanisms would hamper good actors' ability to innovate, improve and develop systems to prevent, disrupt, and remove CSAM. Without the legal certainty to test new technology, tried and true technologies that have served in the fight against CSAM for decades – such as PhotoDNA – would not have been built nor deployed. Introducing a mandatory detection framework would inevitably disincentivise and discourage investment in new and state-of the-art rights preserving innovation central to the safeguarding of children online.

At the same time, we would like to emphasise that voluntary detection measures and potential mitigation measures must not result in any weakening or circumventing of encryption and must respect the various roles service providers play in the digital world, as recognised by the DSA. In particular, they must not undermine the liability safeguards that apply to intermediary service providers.

Finally, we recommend that the CSAM Regulation should not rely on cross-references to the interim Derogation from the ePrivacy[2] and that any relevant concepts from that instrument be directly incorporated into the Regulation itself

3. Cascade approach

We recommend including a clear reference in the CSAM Regulation to a cascade approach which clarifies that, if CSAM is accessible through multiple layers of in-scope electronic communications service providers, only the provider closest to and/or with direct control over such content (the "content controller") should be obligated to take action under the CSAM Regulation. This is rightly reflected in the European Parliament (EP) Report from 2023, see its Amendment 23[3]. This approach is consistent with DSA Recital 27[4], which expressly recognises the different roles and technological capabilities that providers have in the digital economy. This would provide legal clarity, uphold legislative consistency, and deliver an effective solution that enables authorities to address the most appropriate provider in the given situation.

4. Duplicative legislative requirements

The CSAM Regulation should avoid creating duplicative or conflicting legislative requirements in areas that are already regulated by other sectoral or horizontal instruments. Our recommendation is therefore to

[2] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse

[3] As a matter of principle, detection orders should be addressed to the service provider acting as a controller.

[4] Furthermore, where it is necessary to involve electronic communication services, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the specific provider that has the technical and operational ability to act against specific items of illegal content, so as to prevent and minimise any possible negative effects on the availability and accessibility of information that is not illegal content.

remove from the CSAM Regulation any provisions that duplicate or conflict with existing rules in legislation such as the DSA, the e-Evidence Regulation, the Cybersecurity Act, NIS2, the GDPR, or upcoming initiatives such as the data-retention initiative or the Technology Roadmap on Encryption.

5. User notification, transparency and data protection requirements

The CSAM Regulation should not propose requirements for informing affected users on measures taken concerning potential CSAM in Article 12(2)[5] which are substantially different from, or redundant to, the DSA. Given that the DSA is already in effect and will soon be subject to evaluation, adding different obligations for providers in the CSAM Regulation would add unnecessary burden and uncertainty. We recommend deference to and focus on the existing mechanisms in place via the DSA.

User transparency and data protection requirements under the CSAM Regulation should likewise remain aligned with, and not duplicate or conflict with, the existing framework established by the GDPR.

6. Reduce the red tape introduced by risk assessment and risk categorisation provisions

The CSAM Regulation should adhere to the staggered, asymmetric approach established by the DSA for categorising and regulating service providers according to the type of service provided and its level of involvement in disseminating user-generated or third-party content. We oppose provisions requiring every single hosting provider to conduct a thorough and burdensome risk assessment irrespective of the provider's level of control over user content and even when a particular provider is inherently low risk as compared to hosting providers that are data controllers. We suggest following the EP position (Art. 3, 4).

A lengthy process of risk categorisation (and possibly, re-categorisation) would create significant red-tape for service providers, the EU Centre, and the Coordinating Authority (CA). In the spirit of regulatory simplification, we recommend that efforts be undertaken to streamline the risk assessment and categorisation to reduce the duplication of risk assessment (including the child risk review as per the DSA's Article 28 Guidance).

7. Strengthening national reporting services

We would also like to emphasise the importance of national reporting services, such as the Austrian Stopline,which play a crucial role in the fight against CSAM. In this context, the network of hotlines coordinated by INHOPE, together with the network of Safer Internet Centres established under the European Commission's Better Internet for Kids Strategy, plays an important role in facilitating the reporting of suspected CSAM. Within this framework, hotlines operate alongside helplines and can act as trusted flaggers under the Digital Services Act, enabling them to report illegal content efficiently.These services provide an effective channel for users to report suspected material and contribute significantly to the swift removal of illegal content. Strengthening and expanding such initiatives across Europe should be considered an essential part of the broader strategy to combat CSAM. However, a vital part of this is ensuring that these services have adequate resources to integrate with existing reporting infrastructure.

[5] The delayed notification process in Article 12 of the proposed CSAM Regulation conflicts with the DSA's requirement for providers to give customers a detailed statement of reasons with "undue delay" when content is restricted. We consider that the "undue delay" reporting requirement in the DSA is already effective and would be controlling.

This would avoid having multiple reporting systems which create technical overhead, prohibit efficiencies of scale and increase attack surfaces.

8. Competent authorities, Comitology and list of approved technologies

When it comes to competent authorities, we strongly recommend adhering to the EP position and clearly providing for judicial oversight. A pre-approved list of technologies will inevitably fail to keep up with the pace of changing technologies. If such a list is regarded as essential pursuant to Article 10, it should be merely voluntary. We advocate that the European Commission take a more goal-oriented, not method oriented, approach, focusing on directing specific outcomes while refraining from dictating a specific technology or vendor to be used. Prescribing a vendor or technology violates principles of technology neutrality and conflicts with the European Commission's work on the Technology Roadmap for Encryption.

9. Keeping of logs

When it comes to the keeping of logs, we would like to stress that there is a separate initiative ongoing as the European Commission's DG HOME launched a data retention initiative to analyse how to approach law enforcement access to non-content data. The CSAM Regulation should avoid regulating any subject matter which is already being separately evaluated or is already partially addressed in other sectoral legislation, such as e-Evidence Regulation, GDPR, and Free Flow of Non-Content Data in the EU, among others.

10. Age Assurance

While we recognise that age assurance remains one of the many ways in which children can be better protected online, mandating this specific technology for certain services may create legal duplications and fail to meet the intended objective of child protection. A variety of workstreams are also seeking to develop a harmonised EU approach to age verification, notably through the DSA's Article 28 – which take into account its technical overlap with the eIDAS Regulation. We recommend that, in order to avoid conflicting or repetitive rules, the CSAM Regulation should only propose age assurance or age verification as a possible mitigation measure – as opposed to an obligatory provision for high-risk services.

11. Liability of providers and transition period

EuroISPA recommends that any provision addressing the liability of providers in the CSAM Regulation is carefully aligned with DSA requirements, definitions and systems. The CSAM Regulation should further empower providers to continue to exercise voluntary detection and ensure liability protection for providers engaging in their own voluntary mitigation efforts. If the shared goal is minimising child offenses, providers should be supported in their efforts, not face potential liability. No general monitoring obligation should be required (as per the DSA). When it comes to the transition period, we deem it important to avoid introducing too complex and/or new administrative or restrictive requirements. The more complex the respective obligations, rules, reporting requirements, etc. will be, the longer the industry will need to comply with and adjust to this Regulation.

12. Renewed Impact Assessment

As a final comment, it might be useful to provide for a renewed Impact Assessment or executive summary of the expected impacts of the CSAM Regulation, given the substantial changes introduced in the Council and Parliament positions compared to the European Commission proposal in 2022, and the implications these changes may have for providers' GDPR compliance and operational responsibilities.

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