
# Position Paper on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

## Introduction

EuroISPA is the voice of the European Internet industry, representing over 2.500 Internet services providers from across Europe, all along the Internet value chain. EuroISPA members are at the forefront of the efforts to protect children online and have a longstanding relationship with law enforcement authorities to assist them in the fight against child exploitation.

As such, we are deeply committed to the Commission's objective to prevent and combat child sexual abuse and will support efforts to make the digital space safe for all.

However, EuroISPA members are concerned about the operability and the future of the Regulation given the technical unfeasibility of certain obligations and measures included in the proposal: the different obligations imposed on Internet services providers do not suit the purpose or the technical specificities of the services, hindering achieving the Regulation's goals. In addition, the current text contradicts the core principles of the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the ePrivacy Directive/Regulation, the Network and Information Security Directive (NIS2) and the Open Internet Regulation, which are fundamental laws that ought to be protected.

Furthermore, it is highly important to provide legal certainty once the ePrivacy derogation comes to an end, as well as to ensure that the transition towards the CSAM Regulation does not leave legislative gaps – especially regarding the legal basis for processing of private communications (meta) data. In order to guarantee a smooth functioning of the envisioned scheme, EuroISPA believes it is necessary for the text to provide sufficient choice for the industry to either report to the EU Centre, the assigned local authorities or NCMEC to avoid double reporting and excessive legal liability.

Finally, the new legislation should not create an excessive administrative burden for small and medium-sized enterprises (SMEs).

While the European Parliament and Council discuss the European Commission's proposal, EuroISPA calls on policymakers to consider a series of recommendations that we believe are crucial for the CSAM Regulation to meet its objectives.

Recommendations

**The CSAM Regulation should be aligned with the core principles of the GDPR, the DSA, the ePrivacy Directive/Regulation, the NIS2 and the Open Internet Regulation. End-to-end encryption shall not be broken.**

- Regarding confidentiality of communications portrayed in Article 15(1) of the ePrivacy Directive, the CJEU has made it clear that said article is to be interpreted strictly, meaning that the exception to the principle of confidentiality of communications must remain an exception and must not become the rule. This principle ought to be respected in the CSAM Regulation.
- Encryption tools are part of the framework which allows the Internet and online services to provide safe and secure private communications to their users and ensure ongoing cybersecurity and data protection. By requiring websites to filter and scan for (un)known CSAM and grooming, the proposed legislation allows for client-side scanning of communications and the destruction of end-to-end encryption (E2EE). Breaking E2EE would have a massive impact on the technical Internet infrastructure and impede efforts to create an Internet which enhances trust, user privacy, and freedom of expression since, without impenetrable encryption, no system in the world is secure anymore. Weakening encryption would cause serious issues for the EU regarding sovereignty, fundamental rights of all European citizens, and protection of trade secrets and innovation in Europe, which would have a massive impact on its economy. Given the protection conferred to end-to-end encryption in the ePrivacy Derogation, as well as the strong incentives for encryption provided by the NIS2 Directive, and the recognition of its role to guarantee the security and confidentiality of the communications of children (recital 25), it shall be explicitly protected in the CSAM Regulation as well.
- Furthermore, all 'relevant information society services' under Article 2(f) that are business-to-business (B2B) services should be ruled out of the scope as they are not vectors of the propagation of CSAM, and as weakening the security of these services could put Europe's industrial sovereignty at risk.
- The draft goes further than the GDPR, as the involvement of the national Coordinating Authority is mandatory once a report about suspicious CSAM content has been issued by a company. This is particularly problematic when it comes to grooming, which is more complex to identify and for which current technology is not yet sufficiently developed and accurate. This could therefore translate into giving the national Coordinating Authority access to content that may not be CSAM, grooming nor illegal, compromising the privacy of the individuals involved.
- In addition, the coordination between Data Protection Agencies (DPA) and the Coordinating Authorities is fundamental for the complementarity of the legislations: if a Data Protection Impact Assessment comes to the conclusion that a certain measure is not allowed under GDPR and this is also confirmed by the consulted DPA, the competent authority under the CSAM Regulation should be obliged to follow this result and not oblige a provider to implement a measure that conflicts with data protection obligations.

- The net neutrality principle is jeopardised by the requirement of URL blocking, since it requires the access provider to perform intrusive detailed analyses of each and every data package that is transmitted over their networks (so called deep packet inspection, see also further down), as well as a weakening of the HTTPS protocol, in clear contradiction with current cybersecurity standards. EuroISPA proposes giving the option to service providers to choose the most appropriate blocking method.
- EuroISPA therefore proposes to add an Article 1 (3) "(e) Regulation (EU) 2015/2120" in order to make sure that the net neutrality principle is upheld with regards to the blocking orders. Recital 7 should be amended accordingly.
- Finally, the CSAM proposal should be aligned with the DSA, especially with regards to the illicit character of general monitoring obligations in the frame of detection obligations and orders.

**Number-based interpersonal communication services (NB-ICS) should be excluded from the detection scope as they play little to no role in the proliferation of CSAM and grooming.**

- It is crucial that legislators consider the diversity of the online ecosystem when proposing harmonized rules for all intermediary services. EuroISPA understands that the Commission in its draft tried to include all potentially relevant service providers into the scope. However, the variety and technical possibilities of ISPs should be taken into account. As such, only ISPs that are relevant for the fight against CSAM, and have the technological means to act, should be in the scope of the proposal.
- In the case of traditional number-based interpersonal communication services, this is clearly not the case. These services play little to no role in the proliferation of CSAM and grooming[1] and it would therefore appear disproportionate to subject these companies to the same measures as other service providers. Such was deemed in the EDPB/EDPS Joint Opinion 4/2022, which considered that the scanning of audio communications is particularly intrusive and as such must remain outside the scope of the detection obligations set out in the proposed Regulation, both with respect to voice messages and live communications.
- Furthermore, the application of the obligations to number-based ICS such as SMS and voice calls is, from a technical point of view, unfeasible. Service providers cannot access voice calls and SMS exchanges for analysis, and a general retention obligation for analysis purposes would be disproportionate and contradictory with the ECJ's constant case law[2]. It is not feasible to impose risk reduction solutions on these means of communication.
- The European Commission's justification, whereas such a broad definition is necessary for the Regulation to be "futureproof", is incomprehensible. This would include thousands of non-relevant companies across Europe into the scope to cover only potentially relevant types of services that might come up in the future. Instead, the

[1] IWF-Annual-Report-2021.pdf page 38.

[2] Two landmark judgements *Digital Rights Ireland and Tele 2 / Watson*. The Advocate General's Opinions in several of these cases released in January 2020 indicate the Court does not consider departing from its clear rejection of general and indiscriminate data retention and has provided further clarification of targeted data retention (Opinions C-623/17, C-511/18, C-512/18, C-520/18).

Commission should conduct a regular evaluation of the Regulation in which the scope can be adjusted when new services found to be systematically used to proliferate CSAM content become available.

**The Regulation's 'hosting provider' definition should be narrowed to ensure detection orders are not applied to data processing services deeper in the internet stack.**

- The 'hosting provider' definition includes IT infrastructure providers that can 'store information at the request of a recipient of the service'. Such IT infrastructure players, including cloud infrastructure providers, serve as data processors and sub-processors and are foundational infrastructure, enabling customers to build and run their own cloud-based IT systems which are designed, controlled and managed by the customer. Infrastructure providers, such as cloud infrastructure, are unable to control what content is user for, who has access to it, or any information pertaining to the identity of a specific user. They thus cannot access content in a way that would allow for the adoption of a detection order that does not go beyond what is strictly necessary to effectively address a CSAM risk in a privacy preserving way.
- It is their customers, acting as data controllers, who have general access to and control over end-user content and who are therefore better and more suited to comply with detection orders.
- We thus advise that the Regulation delineates the definition of hosting providers to consider the technical differences between providers that act as 'data processors' and 'data controllers' mirroring the E-Evidence Regulation's Article 5 (6). Detection orders should only be aimed at providers acting as data controllers with direct control over data as opposed to those that provide data processing or sub-processing services, such as IT infrastructure services.

**The legal basis for voluntary measures should be accommodated within the text.**

- Several EuroISPA members have mechanisms and tools in place for the voluntary scanning and detection of CSAM within their services and systems. For online messenger services this is only possible due to the provisions included in the ePrivacy derogation, which is intended to end in August 2024.
- The current CSAM proposal does not include any provision that would provide sufficient legal basis to the providers willing to continue with voluntary measures to do so. Providers of interpersonal communication services are further concerned that the transition from the current ePrivacy derogation to the CSAM Regulation can create a gap in the safety of children online.
- In addition, there are questions regarding the measures that could be undertaken during the waiting period spanning between the assessment of risk mitigation measures undertaken and the issuing of a detection order. It has been confirmed by institution officials that the issuing of the orders is a lengthy procedure of checks and balances, which could lead to a period of inaction and a lack of protection of the minors online.
- Detection orders – due to their severe consequences and the necessary procedural steps – should only be a measure of last resort. Voluntary measures would allow to fill

a potential gap. Current structures, including the hotlines, have proven that notice and take-down measures are effective, low-threshold and quick.

- Given the previous points, and in line with the EDPB/EDPS Joint Opinion 4/2022, it is important to make clear in the text of the proposed Regulation that the voluntary use of technologies for the detection of CSAM and the solicitation of children remains permitted only inasmuch as it is allowed under the ePrivacy Directive and the GDPR, as well as the transition from the current Interim Derogation framework to the proposed system of obligations within the Regulation.

**Error-rate in detecting unknown CSAM and grooming would create privacy issue and over-burden ISPs**

- One of the main concerns towards this proposal is the susceptibility of detection software to errors, which lead to false positives, excessive control and supervision of content that, despite its explicit nature, is not CSAM.
- The European Commission declared its awareness of this problem and has evaluated the accuracy of current grooming detection technology at approximately 90 percent. This estimated error margin of 10 percent is excessive and would lead to a severe number of false positives, as well as an unproportionate burden for ISPs to deal with.
- Regarding unknown CSAM and considering the amount of content that is shared on a daily basis, anything but full accuracy would mean that large numbers of explicit, intimate content being consensually shared in particular between young adults would be flagged by these technologies, stored and shared with third parties.
- Moreover, measures permitting the public authorities to have access on a generalised basis to the content of a communication in order to detect solicitation of children are more likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter of Fundamental Rights.
- Therefore, and in order to enhance the proposal with fundamental rights, EuroISPA considers that, as per the EDPB/EDPS Joint Opinion 4/2022, the relevant provisions related to grooming and unknown CSAM should be removed from the proposal and its detection should be voluntary without any liability to providers.

**EuroISPA calls for a cascade approach to removal orders.**

- Article 5 (6) E-Evidence Regulation clarifies that when data is stored or processed as part of an infrastructure by a 'data processor' on the behalf of a 'data controller', removal orders be addressed first to the data controller, unless there is risk of jeopardizing an investigation or if the data controller cannot be identified by law enforcement.
- This approach is crucial as infrastructure providers do not have direct control over the data they host, and those that do are in a better position to remove content appropriately. In addition, due to the nature and complexity of the technical specifications of IT infrastructure providers, disabling access to content can implicate large portions of a providers' resources, with the ensuing impact of disabling the entirety of a service which could have unintended consequences for other users of the service.

- EuroISPA recognizes the need to expeditiously remove CSAM from services to protect children online. To ensure content is removed as efficiently as possible, however, we urge the co-legislators to introduce a similar 'cascade approach' to the CSAM removal orders, which would clarify that addressing orders to the data processors should be the last resort.

**Blocking orders cannot be considered as the most suitable measure to fight CSAM.**

Blocking measures do not provide a concrete solution to the problem and are easily circumvented.

- EuroISPA would like to emphasize that website blocking is not a suitable measure to combat the dissemination of CSAM. Instead of targeting the content at source, it merely moves it out of sight for parts of the general public – since all blocking technologies can be circumvented. On the hosting side domain names and host servers can easily be changed. On the user side technologies such as virtual private network services and alternative resolvers are easy to use and well-known tools to circumvent blocking measures.
- It has been expressed by institution officials that blocking orders are only to be regarded as the last resort. However, this is not explicitly mentioned in the text of Article 16 and should be clarified. Recital 32 of the Regulation already points in this direction and suggests amongst others that, before issuing a blocking order, it must be determined that it is impossible to have the host provider remove or disable access to the material. As such, the subsidiarity principle should be clearly reinstated in the text.
- Furthermore, it should be specified how the blocking of a website should be coordinated with active investigations, in order not to hinder the work of Law Enforcement.

URL blocking is highly intrusive and detrimental to privacy and security standards.

- As mentioned before, blocking of specific URLs requires the access provider to perform a deep packet inspection. This is similar regarding the obligation to assess whether their users have accessed or attempted to access any of the CSAM indicated by listed URLs during the past 12 months, which are equivalent to creating new data-retention obligations on the content level for ISPs – in clear contradiction with the ECJ's constant case Law. Such intrusive measures have hitherto been considered unlawful both based on net neutrality and privacy arguments. Besides, as most of the data traffic is nowadays encrypted by using HTTPS, a provider would need to decrypt data packages while in transit which would be clearly detrimental to security standards and in conflict with CJEU jurisprudence, in contradiction with the obligations stated in the NIS2, as well as having been deemed as disproportionate by the EDPB and EDPS in their Joint Opinion 4/2022.
- In line with standing jurisprudence of the CJEU, a service provider must be able to choose the most appropriate blocking method. Stipulating a concrete technique, such

as URL blocking, in turn would be an unjustified infringement of the service providers' freedom to conduct a business.[3]

Clarifications are required regarding proportionality and safeguards.

- Article 16 (5)(a) refers to "effective and proportionate limits and safeguards" that are necessary to limit the negative consequences of a blocking order. It is important to establish which limits and safeguards are being referred to.
- Article 16 (7) last sentence requires that "The provisions of this Section shall apply to such requests, mutatis mutandis". This is unclear and should be deleted.
- Article 18 (3) requires Internet access providers to operate complaint mechanisms. Complaints about alleged infringements of Articles 16-18 should, however, be raised to the competent authority and not the access provider for reasons of coherent application.
- EuroISPA would like to see in the text more emphasis on the proportionality of the orders and the mandatory cost reimbursement both for the initial and running costs for blocking measures. In addition, the liability exemption in Article 19 should be extended to web blocking as well.

**The EU Centre will have an important role, yet it might not be suitable for all types of services and the role of hotlines needs to be clarified.**

- The EU Centre shall ensure that the list of indicators that will be gathered to lawfully carry out the obligations imposed on the different providers is aligned and updated with those requirements endorsed by the NCMEC.
- The role of hotlines in the framework of the EU Centre needs to be clarified. For years, hotlines have successfully worked on CSAM being deleted from the Internet. However, the current text does not reflect their importance and future status in the fight against CSAM.
- Policymakers will have to bring clarity or limits on the EU Centre's power to "conduct searches on hosting services" and impose safeguards around such searches.

**Reporting obligations shall give the option to the providers to choose their interlocutor.**

- Given the scope of the different businesses, national or international, and the nature of the child sexual abuse offences that may occur, affecting one single country or multiple, the text should give the option to the ISPs to choose whether to report to the EU Centre or the local authority according to what is the most suitable for them and their business model. Under this scheme, national authorities should have the opportunity to send valid reporting to the Centre, thus also alleviating the burden. Such a scheme would avoid disrupting the well-functioning of already well-established reporting mechanisms for businesses with a national footprint. Furthermore, it would give multinational companies the opportunity to benefit from having a single point of contact.

[3] See C-314/12 UPC Telekabel Recital 52.

- Besides, according to *U.S. Code, Title 18, Part 1, Chapter 110, Section § 2258A - Reporting requirements of providers,* all providers operating on US soil have a duty to report to the CyberTipline of the NCMEC both apparent and imminent violations regarding children exploitation content on their services.
- It shall be clarified in the Regulation how the providers can avoid double reporting to the EU Centre, the NCMEC and to LEA. The cooperation between the cited authorities will be fundamental to maintain the databases updated and prevent the fragmentation of efforts against CSAM.

**Providers need protection against liabilities when it comes to the development and deployment of new technologies to tackle CSAM on their systems.**

- EuroISPA welcomes the initiative to have the EU Centre provide tools free of charge to those that require them. However, it should be taken into consideration that the integration into an existing technical environment is often unfeasible – especially for SMEs – as well as that providers are prevented by law to allow external technology in their infrastructure (see NIS2 requirements). In any case, the roll out of the technologies needed to comply with the obligations stated will regularly require a significant investment and human effort, which a majority of SMEs may not be able to lift.
- EuroISPA considers that a sole focus on error rates is misleading and is likely to constrain industry activities, as well as the ability to innovate. Accuracy will depend on a range of factors, and it is important to clearly distinguish between the tools to detect known CSAM, unknown CSAM and grooming.
- EuroISPA calls for the "Good Samaritan" liability protection to be extended to other types of civil liability and not limiting it to child sexual abuse offences.