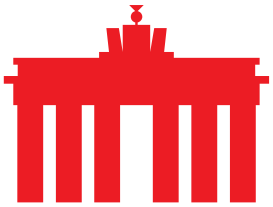


WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

Key Points on the Trilogue of the CSAM Regulation

Berlin/Cologne, 6 January 2026

In May 2022, the European Commission published a proposal for a regulation laying down rules to prevent and combat child sexual abuse[1] (hereinafter referred to as the CSAM Regulation). A wide range of new obligations for online service providers and the establishment of a European Centre to Prevent and Combat Child Sexual Abuse ("EU Centre") form the core of the proposed regulation.

Combating child sexual abuse is a central concern and a task for society as a whole. eco – Association of the Internet Industry (eco) and the member companies we represent are aware of their socio-political responsibility and support the European Commission in its efforts to combat the sexual exploitation of children and the dissemination of child sexual abuse via the Internet. The cooperation and collaboration of companies with law enforcement authorities and national hotlines, as well as their integration into the international network of hotlines (INHOPE), already make a significant contribution today to combating depictions of child sexual abuse.

On the initiative and with the support of its member companies, eco has been operating its hotline, the "eco Complaints Office"[2], for 30 years in order to receive reports of illegal Internet content. A key focus of its activities is the effective handling of reports concerning depictions of child sexual abuse and the sexual exploitation of children. In addition, eco is a founding member of INHOPE[3], the international umbrella organisation of hotlines that take action against abusive content online and cooperate worldwide for this purpose.

The European Parliament and the Council of the European Union have now defined their negotiating mandates for the trilogue negotiations.

With a view to the trilogue negotiations, eco would like once again[4] to contribute to the discourse and address the following points:

- **Proactive Search for Detecting Child Sexual Abuse Online / Search Obligation**

In the trilogue negotiations, regulations on search obligations should be abandoned.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209

[2] https://international.eco.de/topics/policy-law/eco-complaints-office/

[3] https://www.inhope.org/EN

[4] **Previous positions and contributions by eco on the CSAM Regulation are available at:** https://international.eco.de/topics/policy-law/press/downloads/

The European Commission has proposed a far-reaching obligation – based on so-called detection orders – under which affected providers must search for known and/or new depictions of child sexual abuse material and/or cases of grooming.

This proposal has been controversially discussed in the legislative process to date. As a result, the European Parliament and the Council of the European Union have proposed amendments to the European Commission's draft regulation in their respective negotiating mandates. The European Parliament wants to limit the search obligation: a detection order should be considered only as a "last resort" and should be limited/focused on individual users or groups of users where there is reasonable suspicion that they are (directly or indirectly) connected to child sexual abuse online. In addition, end-to-end encrypted communication should be excluded. The Council of the European Union has spoken in favour of removing the search obligation from the CSAM Regulation.

eco rejects the proposed search obligation and advocates refraining from including provisions on the search obligation in the CSAM Regulation in the trilogue.

A mandatory search for the purpose of detecting child sexual abuse raises constitutional and fundamental rights concerns that have not been resolved in the course of the legislative debate to date.

A comprehensive search obligation with low-threshold requirements would contradict the fact that, under the Digital Services Act (DSA), service providers may not be generally obliged to monitor Internet content or search for illegal content.

The inclusion of encrypted communications in the search obligation would also entail a weakening of encryption technologies. This would result in massive security risks that go far beyond the implementation of a search obligation and would have significant impacts on the confidentiality and integrity of digital communications for businesses, politics and citizens.

In the field of encryption, there is currently no technology that allows searching while preserving the level of protection provided by encryption.[5] This also applies to so-called "encryption backdoors" and "client side scanning", which have been repeatedly brought into play in the course of the legislative debate.

End-to-end encryption means that decrypted data can only be seen and read by the "endpoints" in a conversation: the sender and the intended recipient. Therefore, encryption backdoors that grant law enforcement or the provider exceptional access to decrypted messages break end-to-end encryption's most basic principle. At the same time, they create an inherent technical vulnerability that can be exploited by criminals and other hostile state actors, for example, thereby putting all Internet users at risk. The same applies to client-side scanning technologies, where scanning takes place on the device and indicators for the search must be integrated into the device or application. These can then subsequently be easily found and analysed (reverse engineering) by criminals and removed, circumvented or misused. eco therefore firmly rejects any weakening of encryption technologies.

[5] **See, for example:** https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-eu-proposal-to-prevent-and-combat-child-sexual-abuse/

- **Proactive Search for Detecting Child Sexual Abuse Online / Voluntary Measures**

In the trilogue, ways should be found to maintain voluntary, proactive measures for detecting child sexual abuse material.

With the CSAM Regulation, the European Commission wants a system change: a comprehensive search obligation for all providers of hosting services or interpersonal communication is intended to replace voluntary detection measures, as carried out by some providers depending on the specific service offered and the possibilities available. Consequently, the proposed regulation does not contain any provisions on voluntary searches by service providers.

At the same time, the legal basis that currently allows voluntary searches for abuse material will expire on 3 April 2026 (Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communication services for the processing of personal and other data for the purpose of combating online child sexual abuse – hereinafter: temporary ePrivacy derogation).

Both the European Parliament and the Council of the European Union wish to continue allowing voluntary measures to detect child sexual abuse. In this respect, the European Parliament's negotiating mandate provides for so-called voluntary detection orders as a legal basis. Specifically, depending on the outcome of their risk assessment, providers should be able to apply to the competent national authorities for voluntary detection measures within the framework of so-called voluntary detection orders. The Council of the European Union wishes to regulate voluntary searches outside the CSAM Regulation and has advocated for making the temporary ePrivacy derogation permanent as the legal basis for voluntary detection measures.

It therefore depends on the outcome of the trilogue whether and to what extent voluntary searches by providers of interpersonal communication will be permissible in the future.

eco suggests finding ways to maintain voluntary measures for detecting child sexual abuse material. From eco's perspective, regulation of the requirements and specifications to be observed in this regard is conceivable both within the framework of making the ePrivacy derogation permanent and through the inclusion of a corresponding provision in the CSAM Regulation. However, to prevent any confusion or misunderstandings, eco recommends refraining from using the term "**voluntary** detection **order**" and choosing a different terminology.

- **Access Blocking**

In the trilogue, the regulations on access blocking should be fundamentally reconsidered.

The Commission's proposal provides for an obligation on Internet access providers, upon (temporary) order, to block URLs that contain depictions of child sexual abuse online that are not hosted in the EU and are not removed by the hosting service provider. In this regard, no changes are planned in the negotiating mandates of the European Parliament and the Council of the European Union.

eco is fundamentally critical of access blocking. Such access restrictions are neither effective nor sustainable.

In eco's view, the investigation and prosecution of perpetrators, as well as the effective and sustainable deletion of content, must have top priority. Accordingly, it is essential to focus efforts to combat child sexual abuse online on international cooperation and collaboration in law enforcement and on the removal of the content.

The experience of the eco Complaints Office shows that URLs with depictions of child sexual abuse can be removed reliably and quickly, even internationally, with functioning processes and cooperation.[6] The experience of the eco Complaints Office in cross-border cases also shows that URLs can be removed more quickly at international level if the legal situation in the hosting country with regard to depictions of child sexual abuse is identical in detail to that of the reporting country.

eco therefore considers it essential to expand or strengthen international cooperation in the event of any problematic cases. In addition, it is important to take action at the political level and to advocate for further legal harmonisation regarding child sexual abuse material. While such material is in principle, internationally condemned and punishable by law, there are nevertheless country-specific differences in detail in the definition of abuse material once the area of so-called "baseline cases" (i.e., depictions of abuse involving prepubescent minors) is exceeded – even within the EU.

In contrast to the removal of depictions of abuse at the hosting level, access blocking merely creates minor access barriers that can be relatively easily circumvented – especially by those who deliberately seek out such content.

eco therefore recommends that the proposed mandatory access blocking measures should be fundamentally reconsidered in the trilogue negotiations.

If access blocking is retained in the trilogue, fundamental adjustments to the procedure proposed in the Commission's draft will be necessary to at least mitigate existing concerns.

On the one hand, it seems highly questionable how it can/should be determined that the Internet access provider has been used to access abusive content in the last 12 months. This would require access providers to monitor user behaviour and

[6] For example, in 2023, 98.87% of URLs reported to the eco Complaints Office containing child sexual abuse material (involving children up to an including 13 years of age) were removed within an average of 6.17 days (including weekends and holidays). Source: www.eco.de/wp-content/uploads/dlm_uploads/2024/09/jahresbericht-eco-beschwerdestelle_2023_rz_en_web.pdf

thus the “content” accessed. This, in turn, would be highly problematic from the perspective of data protection, the prohibition of general monitoring obligations and telecommunications secrecy.

There are no technical possibilities of scanning content in the transmission process in a content- and context-oriented manner. At most, it would be possible to determine the type of content (video, image, audio). However, as soon as users employ encrypted VPN connections to use online services, a third-party provider acts as a gateway to the Internet. As a result, the Internet access provider only sees a “tunnel”. Furthermore, it is not technically possible to determine in advance to which individual addressee a data packet is being sent.

On the other hand, clear and uniform guidelines are essential for defining non-deletable URLs that cannot be removed, as well as ensuring that the URL blocking list provided is up to date. The risk of over-blocking legal content must be largely excluded or limited as much as possible. Therefore, the URLs contained in the database/list must be regularly reviewed and updated by the EU Centre. The review of these URLs for child sexual abuse material must also include any change of hosting providers.

If a change in hosting is detected during the review, a new “notice and takedown” procedure must be initiated immediately for the relevant URL, to give priority to the removal of child sexual abuse material and to prevent further re-victimisation of the victims. Updates to the URL list must be provided to the Internet access providers affected by blocking orders at least daily.

- **Inclusion of and Cooperation with Existing Structures and Relevant Actors**

In the trilogue, established structures and cooperation between the various actors should be more strongly incorporated into the provisions of the CSAM Regulation.

Implementation and enforcement of the Regulation

According to the Commission’s draft, “competent authorities” or “coordinating authorities” are to be designated as neutral bodies at the Member State level for the implementation and enforcement of the CSAM Regulation. In this context, criteria are provided that consequently establish new structures. At the same time, close cooperation with existing actors is neither required nor explicitly provided for. Consequently, the proposal means that existing structures cannot be relied upon and that already existing cooperation and synergies cannot be used, expanded and intensified. For example, the draft regulation does not include hotlines and law enforcement authorities as relevant actors or authorities at the national level when it comes to detecting and removing abuse material.

At the EU level, a European Centre to Prevent and Combat Child Sexual Abuse (“EU Centre”) is to function as an autonomous and independent agency/institution of the European Union. Its task is intended, in particular, to support the various stakeholders in implementing the regulation and fulfilling the new obligations. The EU Centre is to provide so-called “indicators” for the implementation of search and

blocking obligations (hash and URL lists) and will also receive and evaluate reports from providers regarding potential child sexual abuse online.

The European Parliament has advocated in its negotiating mandate for stronger involvement of hotlines in the provisions of the CSAM Regulation.

eco supports the European Parliament's approach and urgently calls for adapting the Commission's proposal.

The establishment of a specific EU Centre will result in the coexistence of an EU institution and the established INHOPE hotline network. eco therefore calls for existing, established structures and cooperation to be explicitly included and for their activities and experience to be built upon – both at national and European level.

The INHOPE network and its hotlines have been active for over 25 years in many areas that, according to the draft regulation, should also fall within the remit of the EU Centre to be established in the future (including the evaluation of reported content, cooperation with law enforcement authorities and hosting providers).

The same applies to awareness-raising tasks carried out by the EU Centre or the competent authorities, as proposed by some. The so-called awareness nodes/centres in the Member States and their "Insafe Network" have been active for years, including across borders. Hotlines, awareness nodes/centres and the so-called helplines form the Safer Internet Centres in the Member States. Therefore, the EU Centre should have more of a supporting function in this area.

From eco's perspective, it is important that the previously effective measures taken to date to combat child sexual abuse online are maintained and that the existing European networks (e.g., INHOPE) continue to be included as an integral component in combating CSAM in the future. To this end, a corresponding clarification in the regulatory text – outside the recitals – appears urgently necessary in the context of the trilogue: for example, by including an explicit obligation for the EU Centre to cooperate with INHOPE and the hotlines of the INHOPE network.

<u>Reporting obligation</u>

In connection with the inclusion of existing structures and cooperation, it is also relevant that Article 12 of the proposed regulation stipulates that hosting providers and providers of interpersonal communication services must report corresponding content to the EU Centre via a specified communication channel and using prescribed forms upon knowledge of "potential online child sexual abuse". In practice, this will often lead to duplicate reports and consequently to a significant increase in workload:

- Scenario 1 – Report by US providers:

  American providers are legally obligated to inform NCMEC when they become aware of child abuse content. If NCMEC identifies a European

connection, it informs the competent police or authorities in the EU (for example, in the case of a German suspect, the German Federal Criminal Police Office (BKA)).
With the proposed reporting obligation, American providers would in future also have to inform the EU Centre, which would then check the content and, if necessary, forward it to the competent law enforcement authority in the respective Member State.

- Scenario 2 – Provider becomes aware of "child abuse content" through a hotline:

  Hotlines work closely with law enforcement authorities and inform them about child abuse content as part of their complaint handling process. Subsequently, depending on the agreement between the hotlines and the law enforcement authorities, the hotlines then notify the hosting provider that a URL contains child sexual abuse material. If the provider has to inform the EU Centre in future, which then informs the German Federal Criminal Police Office (BKA), this will result in a duplicate report to the BKA.

eco therefore suggests adapting the proposed reporting obligation to provide exceptions in cases involving NCMEC or hotlines, in order to build upon existing structures while simultaneously avoiding duplicate reporting.

- **Requirement for Coherent Regulations**

The trilogue should ensure that the provisions of the CSAM Regulation are coherent with other existing or planned legal regulations.

The combating of abusive content is part of combating prohibited online content, for which there are already a number of regulations, primarily in and with the DSA, which has a special status as a binding, EU-wide applicable and fully harmonising legal framework. It is essential that the provisions of the CSAM Regulation fit coherently into the existing legal landscape in order to provide all actors with the necessary legal certainty. In this context, eco would like to explicitly highlight the following points:

<u>The DSA prohibits an obligation of general monitoring of Internet content</u>

The establishment of a comprehensive search obligation with low-threshold requirements in the CSAM Regulation would contradict the fact that, under the DSA, service providers may not be generally obligated to monitor Internet content or to search for illegal content. Against this background, eco once again urges the trilogue to avoid a comprehensive search obligation on all providers of hosting services or interpersonal communication services.

<u>Definition of regulated entities and differentiation between provider types</u>

The proposed regulation does not distinguish between the different types of hosting services or interpersonal communication services.

In addition to classic hosting and cloud-based IT infrastructure services, the storage of content on social networks and other platforms (e.g., image/file hosters) also falls under the provision of hosting services.

The diverse hosting services included in the draft regulation each have different capabilities for action and control.

It is in the nature of these services that providers of classic hosting and cloud infrastructure services regularly have no knowledge of which services, applications and content users (including corporate customers) store on the server or for what purpose. It is therefore questionable whether they could carry out and implement the proposed risk assessment obligation.

The different and limited access capabilities available to classic hosting providers and cloud infrastructure service providers apply even more so to the implementation of risk mitigation measures. Adjustments to functions or usage options can generally only be made by the customers. The capabilities available to providers of classic hosting or cloud infrastructure services are very limited or non-existent in this regard. To require these services to scan, filter or monitor their customers' data is also disproportionate with regard to the integrity and confidentiality of customer data.

With regard to interpersonal communication, the European Commission's proposal does not differentiate between number-based and number-independent services, as defined in the European Electronic Communications Code. The regulation would therefore also cover number-based services such as SMS and voice calls. However, providers of such services are technically unable to implement the envisaged obligations.

Regarding the parties subject to the obligations, the European Parliament and the Council of the European Union propose some clarifications. The European Parliament wants to limit the scope of the regulation to providers of number-independent interpersonal communication services. Furthermore, primarily "data controllers" should be subject to the obligations. The Council of the European Union also envisages, at least in some areas, a focus on number-independent interpersonal communication services.

eco endorses the efforts of the Parliament and the Council. In this regard, eco appeals to the trilogue participants to align with the Parliament's position. Specifically, the text of the regulation should differentiate between the requirements for hosting service providers and limit the scope to number-independent interpersonal communication services. It must be ensured that any obligations are directed at the correct service. With regard to existing capacities for action, primarily "data controllers" (e.g., customers of a cloud service) and not "data processors" should be obligated.

Age verification/age assessment

The European Commission, the European Parliament and the Council of the European Union have included provisions on age verification and age assessment in

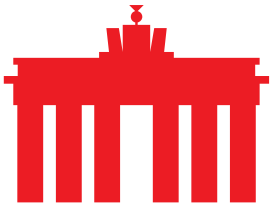
their proposals and negotiating mandates. However, even outside the CSAM Regulation, the topic of age verification/age assessment is currently being widely discussed at the EU and Member States level, with discussions encompassing not only the “if” but also the “how”. In addition, the guidelines on the protection of minors under Article 28 DSA also contain provisions on age assessment and age verification.

From eco’s perspective, it is essential to ensure coherence on this issue in the trilogue and not to create separate requirements if age verification/age assessment requirements are to be retained. It is also important to keep an eye on developments in this area outside the EU, since companies are often also active outside of Europe and international decision-making therefore has particular relevance. Moreover, it remains important that any regulations must be compatible with the principles of data protection, data minimisation and privacy.

Conclusion

eco supports the fight against child sexual abuse online, but advocates for amending or adapting the EU Commission’s proposal at several points within the framework of the trilogue:

- The provisions on proactive searching for the purpose of detecting child sexual abuse online should be fundamentally revised.
- The provisions on access blocking should be fundamentally revised.
- Greater and more explicit involvement of, and cooperation with, existing actors – particularly the INHOPE network and its member hotlines in the Member States – is required.
- The fact that different service providers have different capacities for action and that not all measures can be implemented by all providers must be better taken into account. The specific existing requirements must be clarified for the different types of service providers.
- The special situation and limited capabilities of SMEs must be taken into account more strongly and explicitly.
- In addition, with regard to the proposed reporting obligations, process duplications and duplicate reports must be avoided.
- Legal certainty requires coherent regulations. Against this background, it is necessary to avoid regulations that contradict or could contradict existing or planned laws.



About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. The association focuses on the reliability and strengthening of digital infrastructure, IT security, trust and ethically guided digitalisation. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.