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

STATEMENT

on the European Commission's Proposal for a Regulation Laying Down Rules to Prevent and Combat Child Sexual Abuse (COM(2022) 209 final)

Berlin/Cologne/Brussels, 12 September 2022

On 11 May 2022, the EU Commission published its proposal for a Regulation laying down rules to prevent and combat child sexual abuse[1] (hereinafter referred to as the CSAM Regulation). In essence, the proposal includes the introduction of new obligations for providers of online services as well as the designation of so-called "Coordinating Authorities" in the Member States and the establishment of a European Centre to prevent and combat child sexual abuse (''the EU Centre'').

The proposed provisions for providers of online services include a variety of new obligations. The EU Commission's draft contains obligations for:

- risk assessment by hosting service providers, interpersonal communication service providers and app stores;
- a proactive detection of online child sexual abuse by hosting service providers and interpersonal communication service providers (by order);
- reporting of online child sexual abuse by hosting service providers and interpersonal communication service providers;
- removal of depictions of child sexual abuse by hosting service providers (by order);
- the implementation of blocking by Internet access providers of non-removed URLs containing depictions of child sexual abuse (by order).

These obligations are also to apply to non-European providers, as long as they (also) offer their services in Europe.

According to the proposed Regulation, the EU Centre's tasks are to include supporting the providers of online services in fulfilling the new obligations. To this end, the planned EU Centre is to provide, among other aspects, indicators or technologies for the mandatory proactive detection to identify sexual abuse of children (irrespective of the particular legal situation or the particular legal understanding of this term in the Member States; in the context of the Regulation, this is to be understood as concerning persons under 18 years of age) as well as receiving and verifying reports from providers on online child sexual abuse.

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

In this statement, eco – Association of the Internet Industry (eco) would like to provide stimuli for the follow-on legislative process and the associated debates and also to highlight fundamental concerns.

Combating the sexual abuse of children is a key concern and a task for society as a whole. eco and the member companies we represent are conscious of their socio-political responsibility and support the EU Commission in its endeavour to combat the sexual exploitation of children and the dissemination of depictions of sexual abuse via the Internet. The collaboration and cooperation of the companies with the law enforcement agencies and national hotlines, as well as their integration into the international hotline network (INHOPE), already make a significant contribution to combating depictions of child sexual abuse and contribute to the successful investigation and prosecution of the perpetrators.

For more than 25 years, eco has operated a hotline entitled the "eco Complaints Office" – initiated and supported by its member companies – to receive reports on illegal Internet content. One of the main activities of the eco Complaints Office is the effective handling of reports on depictions of sexual abuse and sexual exploitation of children and minors. In addition, eco is a founding member of INHOPE[2], the international umbrella organisation of hotlines that combat depictions of abuse on the Internet and cooperate worldwide for this purpose.

Based on its experience as a contact partner for the Internet industry and as a hotline operator, eco considers a large number of the provisions contained in the proposed Regulation to be in need of clarification or to be fundamentally problematic. For a legally secure and practicable further development of measures to combat sexual abuse of children and minors on the Internet – involving synergies and the simultaneous incorporation of elementary security functions – eco considers adjustments to the proposed content and text of the Regulation to be imperative.

[2] https://www.inhope.org

I. Planned obligations for online service providers

Risk assessment and risk mitigation obligations

In eco's view, the obligations for risk assessment and risk mitigation proposed in the CSAM Regulation are in need of clarification, are unworkable in parts, and also strongly encroach on the privacy of users.

Stipulations for hosting providers and providers of interpersonal communication services

For each service they offer, hosting providers and providers of interpersonal communication services (hereinafter referred to as service providers) are required in future to assess the risk of its use in the context of online child sexual abuse (in terms of the Regulation, the dissemination of depictions of sexual abuse of persons under 18 years of age as well as grooming activities in the digital space). If a potential risk is affirmed, effective, targeted and appropriate measures are to be taken to minimise the risk. In addition, the service providers are to submit a report on the process of preparing, the result of the risk assessment and the planned mitigation measures to the Coordinating Authority of their place of establishment.

The proposed decisive factors for the risk assessment include whether cases of online child sexual abuse have previously been identified in connection with the use of the service, what response strategies and processes exist for dealing with it, what use of the service is intended or possible by the users, and to what extent children use the service. In the case of use by children, the age group and the corresponding degree of risk must be assessed; functions of the service with a potential grooming risk (sharing of pictures/videos, searching for other users, direct communication and contact options, etc.) must be taken into account; requiring age verifications may mitigate a degree of risk.

These stipulations raise a multitude of issues. The associated obscurities and legal uncertainties for the obligated service providers need to be resolved in the course of the follow-on legislative process.

Firstly, it should be noted that the proposed Regulation does not distinguish between the different types of hosting services and the services of interpersonal communications in either the area of risk assessment or in the area of other obligations.

In relation to hosting providers, for example, it is unclear to what degree a subdivision of the hosting services provided needs to be made for the assessment. This could be by a virtual or physical server for classic hosting providers, or by a customer or product and its provision to business or private customers.

In addition to the classic hosting providers and cloud-based IT infrastructure services, the storage of content in social networks and on other platforms (for example, image/file hosting) also comes under the provision of hosting services.

Each one of the diverse set of hosting providers that can be classified as hosting services according to the broad definition of the proposed Regulation has a

different scope for action and control capabilities. Due to the lack of differentiation in the Regulation's text, it is unclear who is to fulfil the obligations in individual cases, i.e. who is the addressee of the stipulations.

By the nature of the services, classic hosting providers and cloud infrastructure service providers regularly have no knowledge of which applications, services and content the users (including corporate customers) store on the server or for what purpose. It is therefore doubtful that classic hosters and cloud infrastructure service providers in particular will be able in practice to conduct and implement the risk assessment obligation proposed in the draft Regulation.

The varied and restricted access options of the classic hosters and cloud infrastructure service providers are therefore of particularly high relevance when it comes to risk mitigation measures. The draft Regulation's proposed adjustments to functions and usage options can generally only be made by the customers. In this context, the options for action of the classic hosters and cloud infrastructure service providers are very limited or non-existent. Moreover, requiring these services to scan, filter or monitor their customers' data is a disproportionate measure with regard to the integrity and confidentiality of customer data.

Furthermore, the Commission's proposal does not differentiate between number-based and number-independent interpersonal communications services as defined in the European Electronic Communications Code. The Regulation therefore is also to cover number-based services such as SMS and voice calls. However, providers of such services cannot technically implement the obligations contained in the proposed Regulation. The operators of these services do not have access to the exchanges for voice calls and SMS and cannot retain them for analysis.

The use of comprehensive age verification measures to minimise the risks of grooming, as proposed in the draft Regulation, comes across as extremely questionable. These measures are not compatible with the principles of data protection, data minimisation and privacy. This concerns both adults and children.

In the course of the follow-on legislative process, the text of the Regulation should be differentiated with regard to the stipulations for providers of hosting services, limited to number-independent interpersonal communications services and clarified with regard to the obligations of non-European providers. It is important to ensure that any obligations are directed at the correct service. First and foremost, obligations should be applied to "data controllers" (for example, customers of a cloud service) and not to "data processors" who do not have the same level of control over the content. In addition, eco recommends the adaptation of the sample list of potential risk mitigation measures.

App store providers

App store providers shall make reasonable efforts to assess (where possible, together with the providers of software applications) the grooming risk of the available apps. If a significant grooming risk is identified, the app store providers are to prevent users under the age of 17 from accessing apps with a corresponding risk.

In this respect, measures for age verification and assessment are to be implemented.

The proposed measures appear problematic in several respects.

App store providers will regularly not be in a position to check and evaluate all the apps developed and provided by third parties in accordance with the specifications. This particularly affects SMEs, free offerings or community projects that offer or operate app stores. An implementation of the obligation could at best be conceivable through an assessment and information about the grooming risk by the respective app providers.

Furthermore, an age-related control or restriction appears questionable in practice. There is no uniform (international or EU-wide) definition of grooming. For example, according to German law, the initiation of contact between adults and minors aged 14 to 17 is permissible and thus does not fall under the offence of grooming in the sense of the Criminal Code. However, according to the Regulation, for users under 17, apps would have to be "blocked" due to a grooming risk.

In addition, a mitigatory "blocking" of all applications and services that offer the possibility of communication in the broader sense, aimed at users under the age of 17, would be unrealistic and difficult to reconcile with the important concept of participation in the modern approach to youth media protection. A general obligation to verify the age of all users (i.e. adults and minors) would be questionable from a data protection law perspective.

Proactive search for child sexual abuse on the Internet / search obligation

The proposed Regulation provides for the obligation to proactively search for online child sexual abuse content – on the grounds of so-called "detection orders". These detection orders shall be issued for a limited period of time at the level of the Member States after going through a multi-stage procedure directed towards service providers. When a corresponding order is issued, the provider concerned is expected in future to proactively search for known and/or new depictions of abuse of children and/or cases of grooming.

The procedure for issuing a detection order is to include the participation of the data protection authorities and a weighing up of all of the affected fundamental rights. The material prerequisite for the issuing of the order is a "significant risk of the service being used for the purpose of online child sexual abuse".

If the services/products are new, it is to be sufficient if comparable products from other providers were affected in the past.

With regard to the obligation to search for new content or for cases of grooming, the prerequisites for an order are supplemented by further stipulations that are also low-threshold. In this respect, it is important to emphasise that a detection order in relation to grooming is only to cover interpersonal communication with users under the age of 17.

For the implementation of a mandatory search obligation, no concrete specification is given to the service providers for the technology to be used. However, it is set out that it must be effective, reliable, state-of-the-art and as non-intrusive as possible. For this purpose, companies can use their own technological solutions or use a technology yet to be provided by the EU Centre. For the indicators to be used for the search, on the other hand, it is stipulated that these must be provided by the EU Centre.

On the proposed Regulation, eco takes a very critical stance on the search obligation for detecting online child sexual abuse and has serious reservations in this respect.

First of all, it should be observed that the vaguely formulated material prerequisites for the issuance of the detection order are likely to lead to legal uncertainty in practice. Furthermore, in the issuing of this detection order, a low-threshold approach is to be expected.

There is a lack of clear and measurable/scalable stipulations and definitions. It is therefore unclear how the respective competent authorities of the individual Member States will interpret and apply in practice the non-defined material prerequisites for determining a high risk of services being used for the purpose of child sexual abuse. This applies in particular to the question of determining whether a significant use of the service for the purpose of online child sexual abuse exists in relation to the prior 12-month assessment period. For example, are ten, 50 or 100 cases per year considered to be sufficient for this, and is a percentage of the total hosting or total offering taken into account? Similar questions arise in estimating whether a considerable use of the service for the purpose of online child sexual abuse can be assumed for the future, despite any risk mitigation measures.

In the context of the publication of the proposed Regulation as well as in response to queries, the EU Commission has emphasised and underlined several times that voluntary detection is not sufficient in the future due to a lack of participation. To what extent a voluntary search by providers of interpersonal communications will still be desired and possible in the future is unclear. The temporary ePrivacy Derogation as a legal basis for corresponding detection measures – for example, in messengers – will expire on 3 August 2024. Voluntary proactive detection measures are not explicitly provided for in the draft CSAM Regulation. Consequently, it must be assumed that the EU Commission intends to create a low-threshold entry barrier for the detection order and thus to open up the possibility for a proactive permanent search obligation.

Drawing conclusions from already existing offerings and connecting these to future new offerings or services is also critical. This, too, suggests that the EU Commission has conceived the stipulations for issuing an order in a low-threshold context. However, the existence of comparable core functions of different services does not necessarily mean that the services are equally susceptible for online child sexual abuse.

The fundamental concerns about a comprehensive search obligation are not diminished by the proposed procedure. A multi-stage procedure cannot rectify the factual outcome. Rather, due to the expiry of the temporary ePrivacy Derogation for providers of interpersonal communications services and the interplay of the CSAM Regulation and the Digital Services Act, a comprehensive and general search obligation, possibly with a "stay down" obligation, is what can be expected.

Even beyond the material stipulations for the detection order, eco's concerns are manifold.

The inclusion of encrypted communication in the search obligation threatens to lead to a general weakening of encryption technologies and would pose massive security risks. This has considerable implications for the confidentiality and integrity of digital communication between businesses and citizens, which would go far beyond the problem of online child sexual abuse. In the area of encryption, there is currently no technology that enables a search while maintaining the level of protection for encryption.[3] This also applies to so-called "encryption backdoors" and "client side scanning". End-to-end encryption means that data can only be seen and read by the two "endpoints" of a conversation: the sender and the intended recipient. For this reason, backdoors that give law enforcement or the provider access to decrypted messages violate the most fundamental principle of end-to-end encryption. At the same time, they create a technical vulnerability that can, for example, be exploited by criminals and other hostile actors and endanger all Internet users. The same applies to client side scanning technologies. A weakening of encryption technologies is therefore strongly opposed by eco.

The approach of using only validated indicators for the implementation of the search order is understandable, but would mean that internationally active companies would have to use separate hash sets for Europe. This raises the question of both practicability and feasibility for companies.

The inclusion of grooming in the search obligation also raises considerable legal and technical concerns. As already mentioned, there is no harmonised legal framework at the European level. From a technical perspective, the unreliable and erroneous search for grooming by AI is a significant factor. Furthermore, there must be acknowledgement that the inclusion of grooming in the search obligation would result in mass surveillance of private and specially protected individual communications. The restriction of the measures stipulated in the Regulation regarding communication with minors under the age of 17 is questionable in terms of technical and practical implementation and would be associated with considerable data protection implications for users of all ages (for example, through identification or age verification).

The Regulation sets out the possibility to use technology provided by the EU Centre for the implementation of a search obligation. However, the integration of a designated technology poses major challenges for companies. It must be compatible with the individual technical infrastructure and must be adapted and

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

integrated at great expense in terms of time, personnel and finances. The security and integrity of the providers' existing technical infrastructure must not be jeopardised by the technology provided. These challenges have not been sufficiently taken into account in the proposal, but should be given strong consideration in the future.

If the provider cannot make use of the EU Centre's technologies due to a lack of compatibility, it will have to ensure the availability of search technologies in the short term with its own resources and efforts. This development is likely to take some time and may take longer than the period of time allowed for companies to implement search measures after the issuance of the detection order (three to 12 months).

In principle, eco would like to point out that any search obligations may pose a particular challenge for SMEs. Taking the situation of SMEs into account is, however, essential in the European economic area. It seems doubtful whether the special situation of SMEs is sufficiently taken into account via the procedural question of "financial and technological capabilities".

eco therefore advocates for a fundamental revision of the provisions on proactive search to track down online child sexual abuse.

In light of these existing concerns, eco is of the opinion that the search obligation should be withdrawn. If the search obligation is retained in the course of the follow-on legislative process, it must be revised with regard to the topics of "practicability and feasibility" and with regard to the voiced technological concerns. The fundamental rights implications for all parties involved must also be given greater consideration. Any further development in this area would have to take greater account of the different possibilities for action of the various types of providers and services, in addition to the role of SMEs.

Ultimately, clear provisions are needed to ensure the required legal compliance. Clarifications are therefore imperative.

Reporting of potential child abuse content

The proposed provisions on mandatory reporting of potential online child sexual abuse raise concerns from a constitutional perspective. They are also questionable from the practicability standpoint.

The proposed Regulation stipulates that service providers who become aware of potential online child sexual abuse must report the relevant content, including further data, to the EU Centre.

In addition, service providers must provide and operate a function for users to report potential child abuse content to the provider.

eco takes a very critical stance on this proposal.

The proposed direct transmission of IP addresses and user data within the framework of the reporting obligation is – without a prior state review, assessment and an order – questionable in terms of the rule of law. Since this involves a sensitive topic and person-specific information, and the underlying suspicion is capable of causing stigmatisation, in advance of the data transmission, by means of state verification, it should be ensured that data is only transmitted in the case of sufficiently confirmed suspicion.

IP addresses and other user data should only be transmitted by a service provider on the basis of a state order (for example, a court order or a decision by a competent authority) in order to comply with the principles of the rule of law. This is the only way to ensure that the transfer of data is justified and legally secure.

Especially in the instance where a report by the service provider is activated on the basis of a user notification, there is also the risk of a legal misjudgement by the service provider. The disclosure of the user's IP address and other data in the event of a misjudgement would have significant negative consequences for the service provider, including in terms of liability vis-à-vis the user and under the GDPR. Such a transfer of responsibility to the service provider or the bearing of risk must not occur.

Technically, it is imperative for the release of data that not only secure and reliable interfaces are provided by the EU Centre, but that these are also standardised; for example, preferably in line with ETSI standards.

In addition, the process for the further handling of the transferred information by the EU Centre should be clearly regulated – including clearly defined maximum retention periods. This is currently lacking, as the proposed Regulation focuses solely on the need for the data for the application purpose.

In addition, the coherence of the CSAM Regulation with other European regulations, such as the e-Evidence legislative package, must be borne in mind and safeguarded in the course of the follow-on legislative process.

Furthermore, as eco's experience indicates, the proposed Regulation on the reporting obligation will in practice often lead to duplicate reporting and consequently to significant additional work. The following constellations are of particular relevance:

Constellation 1 – Notification by a US provider

US providers are required by law to notify NCMEC whenever they become aware of child sexual abuse content. If NCMEC establishes a European connection, it forwards the case to European law enforcement agencies.

If, in the future, US providers also have to report online child sexual abuse material to the EU Centre – which would then check the content and, if necessary, forward it to the law enforcement agencies in the respective Member States – this would result in a duplicate report on the part of the provider as well as a subsequent duplicate report to the law enforcement agencies in the respective Member State.

Constellation 2 – A provider is made aware of potential online child sexual abuse material by a hotline

Hotlines work closely with law enforcement agencies and inform them about validated reports as part of their complaint handling. For example, the German hotlines of eco, FSM and jugendschutz.net first inform the German Federal Criminal Police Office (BKA) about validated reports and only inform the provider after an agreed standstill period. If the provider has to inform the EU Centre in the future about reports from the hotlines, which would then inform the BKA, there would be a duplicate notification to the BKA.

In the context of the follow-on legislative process, eco suggests that the proposed Regulation should not include the direct disclosure of IP addresses and user data, and that this should be conditional on the outcome of a prior state review and order. Furthermore, eco recommends adapting the text of the Regulation in order to avoid duplicate reports. In this respect, it would be feasible, for example, to exempt American providers from the reporting obligation while at the same time strengthening the cooperation of NCMEC with the law enforcement agencies of the European Member States. In the event that the provider becomes aware of potential child abuse content through a hotline, eco is also of the opinion that an exemption of the providers concerned from the reporting obligation is feasible and justifiable.

Provision of a reporting function by service providers

The general and undifferentiated obligation to provide and operate a reporting/flagging function must be questioned with regard to its actual practical use, especially with regard to traditional hosting providers. This is because, as a rule, it is not obvious to users which provider hosts a piece of content and to whom a report should be sent. If traditional hosting providers are nevertheless to provide a reporting infrastructure, this must be practicable.

In eco's view, in this constellation it must be sufficient, for example, if the hosting provider makes a reporting option available centrally on its own website. It is not feasible and practicable for the hosting provider to implement and be responsible for a flagging function on every website or for every offering or service of its customers. For flagging functions on individual websites or services, it would make sense to start with the respective customer as the responsible party, as their options for action can be compared with those of platform providers.

eco suggests that this be clarified and adapted in the course of the follow-on legislative process.

In addition, it would make sense to give classic hosting providers (especially SMEs) the option to cooperate with central neutral contact points (for example, the established hotlines) to receive notifications/reports in order to implement the obligation. For example, such cooperation could involve a link to the reporting

forms of the hotlines instead of the providers having to maintain and operate their own reporting infrastructure.

Strict guidelines for the removal of depictions of child sexual abuse

The EU Commission's proposed regulation places an obligation on hosting service providers to remove depictions of child sexual abuse within 24 hours of being ordered to do so, or to disable access to such content within the EU. For this so-called "removal order", content must have been assessed by the Coordinating Authority, a court or another independent administrative authority designated by the Member State as depicting child sexual abuse. If this is the case, the Coordinating Authority may apply for the order to the competent judicial or administrative authority.

Independently of this formal procedure for the removal order to be established, informal notifications of hosting service providers should continue to be possible in the future, in which the provider removes depictions of child sexual abuse on the basis of indications and notifications; for example, by users or hotlines.

With regard to the specified 24-hour period for implementing the removal order, eco points out that this strict time limit may not be feasible in practice in individual cases. This concerns SMEs in particular. Fewer personnel, technical and financial resources should be taken into account in this context. eco suggests corresponding adjustments to the proposed regulation.

Due to the well-functioning existing reporting channels via hotlines, eco is of the opinion that the planned obligation should at best be understood as an escalation stage and, in practice, a meaningful addition to the existing regime in only a few cases. This is because, in the vast majority of cases, hosting service providers will take down reported content within a very short time without a corresponding order, i.e. voluntarily. Insofar as a report is first received by an authority, it must be ensured and guaranteed that their procedures are carried out swiftly in the interest of preventing further re-victimisation.

Access blocking / blocking of Internet content

The planned obligation for Internet access service providers provides for the blocking of URL-based content containing known depictions of online child sexual abuse not hosted in the EU by means of (temporary) orders, where take-down cannot be obtained from the hosting service provider.

Procedurally, one of the prerequisites is that the service must have been used to a considerable extent in the preceding twelve months for (attempted) access by users to URL addresses that lead to depictions of sexual child abuse.

A URL list that is created and provided by the EU Centre is mandatory for blocking. When a blocking order is issued by a judicial or administrative authority, it is to be

ensured that the list to be used is up-to-date, that its content consists exclusively of depictions of child sexual abuse, and that the implementation of the provider's online blocking is effective and targeted.

For fundamental reasons, eco takes a very critical view of access blocking. Access blocking is neither effective nor sustainable. Apart from this, the procedure proposed in the draft has a large number of problematic aspects and issues.

In the opinion of eco, investigations and the prosecution of the perpetrators as well as the effective and sustainable take-down of the content must have top priority. Accordingly, it is essential to apply the focus on the fight against online child sexual abuse on international cooperation and collaboration in prosecution and take-down. With functioning processes and cooperation, URL-based content with depictions of child sexual abuse can also be reliably and quickly taken down internationally.[4]

The experience of the eco Complaints Office with the cross-border cases of depictions of child sexual abuse shows that take-down can be achieved more quickly internationally if the legal situation in the hosting country with regard to such depictions is also identical in detail to that of the reporting country. eco therefore considers it essential to expand or strengthen international cooperation in any problem cases. From eco's point of view, it is essential to become active on the political level and to advocate for further legal harmonisation on depictions of sexual child abuse. This is especially true in view of the fact that depictions of sexual child abuse are, in principle, internationally prohibited and subject to criminal prosecution. There are nevertheless different standards internationally – and even in the EU – in the detailed definition of depictions of abuse as soon as one leaves the area of the so-called "baseline cases" (i.e. depictions of abuse on prepubescent minors).

In contrast to the take-down of CSAM at the host level, access blocking only creates more difficult access, which can, however, be circumvented relatively easily – especially by those who deliberately access corresponding content.

Determining whether Internet access providers have been used to access child sexual abuse depictions to a considerable extent in the prior 12 months would require access providers to monitor user behaviour and thus the accessed "content". This would be highly precarious from the point of view of data protection, the prohibition of the general surveillance obligations, and the secrecy of telecommunications. Moreover, any surveillance measures should always be ordered by the authorities or the courts.

Irrespective of this, there are no technical opportunities to scan 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). As soon as a

[4] For instance, in 2021, 98.09 % of the URLs with depictions of sexual abuse of children (up to and including 13 years of age) that were reported by the eco Complaints Office were taken down within an average of 5.3 days (including weekends and public holidays). Source: Annual Report of the eco Complaints Office 2021

user applies encrypted VPN connections to use online services, a third-party provider acts as a gateway to the Internet. In this case, the Internet access provider only sees a “tunnel”. Technically, it is also not clear from the outset to which individual addressee a data packet is sent.

Aside from this, it is important from eco’s point of view to have clear and uniform guidelines on the definition of URLs that cannot be taken down and with regard to the currency of the URL blocking list. The risk of overblocking legal and non-objectionable content must be excluded/limited as far as possible. Therefore, the EU Centre must regularly update and check the URLs contained in the database/list for depictions of child sexual abuse. From eco’s point of view, the regular check of these URLs must also include changes of the hosting provider. If a change in hosting is identified in the course of the review, a new “notice and take-down” procedure must be initiated immediately with regard to the relevant URL. This must be done in order to use the new contact and to take into account the priority of taking down depictions of child sexual abuse, as well as to counteract the further re-victimisation of victims by taking down the content.

Updates to the URL list must be provided to Internet access providers affected by blocking orders at least daily.

The proposed regulations strongly interfere with the fundamental rights of the providers concerned and all users. They entail a considerable risk of surveillance and, in addition to serious legal concerns, also raise massive issues from a feasibility perspective. For the further legislative debate, eco therefore advocates the fundamental reconsideration of the inclusion of mandatory blocking of Internet content and a retraction of the current proposed regulations.

II. Implementation / enforcement of the regulation

The proposals for the implementation and enforcement of the CSAM Regulation lack a sustainable involvement of existing actors and proven structures and processes. The use of synergies is called into question.

Designation of competent authorities or Coordinating Authorities in the Member States

For the implementation or enforcement of the Regulation, “competent authorities” or “Coordinating Authorities” are to be established in the Member States, thus creating a neutral body in each Member State. To this end, the proposed Regulation provides criteria for the Coordinating Authority or the other competent authorities, which are to establish new structures as a consequence (for example, legal and functional independence from other authorities or the prohibition to be entrusted with other tasks connected to the prevention or combating of sexual abuse of children beyond the tasks of this Regulation).

The proposal implies that existing structures and established actors cannot be drawn upon and that existing cooperation and synergies are not to be used,

expanded and intensified. For example, the current proposed guidelines do not involve existing actors such as hotlines and law enforcement agencies.

In this regard, eco urgently suggests adapting the stipulations and enabling a strong sustainable involvement of the established structures as well as the cooperation of the different actors and their expertise at the level of the Member States. In eco's view, the EU Commission's wish for neutrality, objectivity and transparency would not be jeopardised by this.

Establishment of a dedicated EU Centre

An EU Centre is to function as a separate, independent agency of the European Union. Its task should be, in particular, to support the various actors in the implementation of the Regulation and the fulfilment of the new obligations (for example, in the area of carrying out risk assessments, detection obligations and blocking obligations). The EU Centre is to provide so-called "indicators" for the implementation of detection and blocking obligations (hash and URL lists), and is also to receive and evaluate reports from providers on potential online child sexual abuse.

The establishment of a separate EU Centre will lead to a coexistence of the EU's own institution and the established hotline network INHOPE (as an umbrella organisation and the individual hotlines as respective INHOPE members), with the EU Centre and the INHOPE network having the common goal of combating online child sexual abuse. Therefore, eco suggests the explicit involvement of existing structures and cooperations and building on their activities and experiences.

The INHOPE network with its hotlines has been active for more than 20 years in many fields, which, according to the draft regulation, the EU Centre will in the future also be responsible for (including the assessment of reported content, cooperation with law enforcement agencies and host providers).

From eco's point of view, it is important to ensure that previous effective measures to combat online child sexual abuse continue to be maintained and, consequently, that the INHOPE network continues to be included as an integral part of the fight against CSAM in the future. For this purpose, a corresponding clarification in the proposed text of the Regulation, outside of the recitals, is urgently required.

Sanctions

The proposal allows Member States to set sanctions at a maximum of six per cent of annual global turnover.

Although the range of fines is based on recent planned legislation, eco is of the opinion that it is still too high. Especially with regard to the large diversity of the companies concerned and the inclusion of SMEs with fewer resources, eco suggests a reduction of the range of fines.

III. Conclusion

eco supports the fight against child sexual abuse on the Internet, but has serious concerns about the provisions proposed in the CSAM Regulation and sees a considerable need for amendments.

The fact that the various service providers have differing capabilities for action and that not all measures can be implemented by all providers must be addressed more effectively. The concrete existing stipulations must be clarified for the different service providers. This applies, for example, not only to the stipulations in the area of risk assessment and risk mitigation, but also to the detection measures and reporting functions.

The proposed Regulation and the new obligations it contains do not differentiate between large and small and medium-sized enterprises. In the follow-on legislative process, the distinctive situation and restricted capacities of SMEs must be taken into account on a stronger and more explicit level.

Furthermore, when it comes to the proposed reporting obligations, the duplication of processes and reporting must be avoided – both at the level of the providers concerned and at the level of the law enforcement agencies. The transmission of IP addresses and other user data should be subject to a prior review and an order by state authorities.

The regulations on proactive search measures and access blocking should be completely reconsidered and revised. Search obligations and mandatory access blocking should be abolished.

eco also advocates that, in the course of the follow-on legislative process (including the subsequent translation of the Regulation's text), inconsistencies with the existing legal situation or with the standard legal and conceptual concepts (cf. the definition of minors, children or "child user" and "child") in the Member States should be eliminated.
