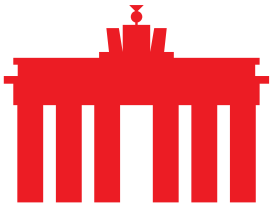

WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

Background Paper on the Proposal for a Regulation Laying Down Rules to Prevent and Combat Child Sexual Abuse (CSAM Regulation)

On 11 May 2022, the EU Commission adopted and published the proposal for a regulation laying down rules to prevent and combat child sexual abuse. After an initial analysis, eco would like to draw particular attention to the following points.

I. Planned obligations for online service providers

- **Risk assessment and risk mitigation**

Stipulations for hosting providers and providers of interpersonal communication services

Hosting providers and providers of interpersonal communication services are to assess the potential risk of "online child sexual abuse" (in terms of the regulation, the dissemination of depictions of sexual abuse of minors and online grooming activities) on their service for each "product" on a provider-specific and service-specific basis. If a potential risk is affirmed, effective, targeted and proportionate "mitigation measures" are to be taken to minimise the risk. In addition, the service providers are to submit a report on the process and result of the risk assessment as well as on the planned mitigation measures to the so-called "Coordinating Authority" of their place of establishment.

Decisive factors for the risk assessment are proposed to include whether "online child sexual abuse" has become known in the past in relation to the product or service to be assessed, what rules exist for dealing with it, what processes have been established, what use is intended or possible by the users and to what extent minors use the service. With regard to minors, the age group and the corresponding degree of risk must be assessed; requiring age verifications may mitigate a degree of risk. Functions of the service with a potential grooming risk (e.g. sharing of pictures/videos, detection for other users, direct contact options, etc.) must also be taken into account.

Examples of "mitigation measures" are listed: Content moderation, strict terms and conditions, internal processes to deal with "online child sexual abuse", including internal "supervision", adaptation of the "products" with the aim of less risky usage possibilities as well as cooperation with competitors and stakeholders (authorities, civil society, trusted flaggers). In relation to grooming, age verification and age assessment measures are proposed to identify and protect minors.

These stipulations for hosting providers and providers of interpersonal communication services raise a variety of issues.

With regard to hosting service providers, no differentiation is made between the various types and offerings of hosting services. In addition to the "classic hosting

providers", the storage of content in social networks and on other platforms (for example image/file hosting) also falls under the provision of hosting services. The diverse hosting services each have different options for action. As a result of this and the lack of differentiation in the proposed regulation, it is unclear who is to fulfil the obligations in the individual case with regard to the specific hosting services, i.e. who is the addressee of the stipulations. As a rule, the classic hosting provider (in contrast to its customers/users) has no knowledge of which applications, services and content the users store on the server or for what purpose. It is also unclear, for example, as to how far a subdivision of the hosting services provided needs to be made for the assessment. This could be by a virtual or physical server, or by a customer or product. In addition, it is often in the nature of the service to have no way of knowing the application options used or the data stored on the systems. It is, therefore, doubtful whether classic providers of hosting services, in particular, will be able to implement the risk assessment proposed in the draft regulation in practice.

In the case of internationally operating providers, the question also arises as to whether the registered office or the respective server location is decisive for the existence of the obligation.

The extent to which the mitigation measures should/could enable voluntary detection measures also seems questionable. The proposed regulation leaves this open. Representatives of the EU Commission have stated, at least in public meetings on the subject, that voluntary detection would no longer be possible in the future under the CSAM Regulation.

The use of age verification measures to minimise the risks of grooming seems extremely questionable. These measures are not compatible with the principles of data protection, data minimisation and privacy. This concerns both adults and children.

App Store Providers

App store providers are to undertake a risk assessment (together with the app providers if necessary) to evaluate the grooming risk of the available apps and then take mitigation measures to protect so-called "child users" (minors up to 16 years of age in terms of the regulation) from relevant risky apps. In this respect, age verification and age assessment measures, references to risk assessment as well as access restrictions to corresponding apps are named as mitigation measures.

The proposed measures appear problematic in several respects. On the one hand, there is the question of technical feasibility. On the other hand, in all instances, the measures represent a major hurdle for practicability

App store providers will regularly not be in a position to check and evaluate all the apps provided in accordance with the specifications. In particular, SMEs, free offerings or community projects that offer or operate app stores are not in a position to fulfil these stipulations. An implementation of the obligation could at

best be conceivable through an assessment and labelling of the grooming risk by the respective providers of the app.

Furthermore, an age-based control or restriction seems problematic in practice. At the international level, and even within Europe, there is no uniform definition of grooming. A mitigatory "blanking out" of all applications and services that offer the possibility of communication in the broader sense for minors would be difficult to reconcile with the important idea of participation in the modern approach to youth media protection. A general obligation to verify the age of all users (adults and minors) would be questionable from a data protection point of view.

- **Detection of CSAM and online grooming**

The proposed regulation requires hosting providers and providers of interpersonal communication services to actively search for known and/or new CSAM and grooming content upon being served with a temporary order (the so-called "detection order"). This obligation is linked to various more far-reaching stipulations, in particular: transparency towards users, the obligation to report on its activities to the Coordinating Authority of the Member State, and the obligation to report CSAM findings.

The "detection order" is to be issued at the level of the Member States, after going through a multi-stage procedure (including the participation of the data protection authorities) and after weighing up all of the affected fundamental rights. However, the material prerequisites for the issuing of a "detection order" by the competent authorities in the Member States stand at a very low threshold, due to the lack of clearly defined specifications. In principle, a "significant risk of online child sexual abuse" is considered to be sufficient. The "likelihood, despite any mitigation measures" or the prevalence of "online child sexual abuse" on the service concerned in the past 12 months are proposed to suffice. If the service/product is new, it is to be sufficient if comparable products from other providers were affected. With regard to the obligation to detect new content or for cases of grooming, the prerequisites for an order are supplemented by 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 up to the age of 16.

No specific technology is stipulated for implementation; however, 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 detection (hash values, AI, etc.), on the other hand, it is stipulated that these must be provided by the EU Centre.

Due to the expiry of the temporary ePrivacy Derogation for providers of interpersonal communication services and the interplay of the CSAM Regulation

and the Digital Services Act, a comprehensive and general detection obligation, possibly with a “stay down” obligation, is to be expected.

eco takes a very critical view of the proposed detection obligation.

The EU Commission has emphasised several times – in the context of the publication of the proposed regulation as well as in response to queries – that voluntary detection is not sufficient due to a lack of participation. Consequently, it must be assumed that the EU Commission intends to create a low-threshold entry barrier for the detection order and thus open up the possibility for mandatory proactive permanent monitoring.

Another point of concern is the lack of clarity as to whether all material prerequisites for the detection order must always be fulfilled or whether the list of prerequisites are an “or enumeration” which must not all be fulfilled. In any case, the fundamental concerns regarding a comprehensive detection obligation cannot be minimised by the proposed procedure.

eco also has considerable concerns about the inclusion of encrypted communication in the detection obligation. A weakening of encryption technologies poses massive security risks. This has considerable implications for the confidentiality and integrity of digital communication between businesses and citizens, which go far beyond the problems of CSAM. A weakening of encryption technologies is therefore strictly rejected by eco.

To what extent voluntary detection by providers of interpersonal communication will still be desired and possible in the future is unclear. Thus, the temporary derogation as a legal basis for corresponding detection measures, for example in messenging services, is expiring. Voluntary, proactive detection measures are not explicitly provided for in the draft CSAM Regulation.

The approach of using only validated indicators for the implementation of the “detection 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 detection obligation also raises considerable legal and technical concerns. In particular, there is no harmonised legal framework at the European level. Different definitions of grooming and different age groups exist in the Member States. From a technical perspective, the unreliable detection of grooming by AI is a significant factor. Furthermore, there must be acknowledgment that the inclusion of grooming in the detection obligation would result in mass surveillance of private and specially protected individual communications. A restriction on communication with minors up to 16 years of age appears questionable in practice and would be associated with considerable data protection implications for all users (for example, through identification or age verification).

In principle, eco would like to point out that any detection 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 “technological & financial capabilities”.

- **Reporting potential online child sexual abuse content**

The proposed regulation requires hosting providers and providers of interpersonal communication services, upon becoming aware of “potential online child sexual abuse”, to report the relevant content to the EU Centre through a specified communication channel and using specified forms. The user concerned is to be informed of any reports that have been made.

Providers must also provide a function for users to report (flag) “potential online child sexual abuse” to the provider.

eco takes a very critical stance on this proposal.

In practice, the proposed regulation on mandatory reporting would often lead to double reporting and consequently to significant additional work:

- Constellation 1 – Notification by a US provider:

  US providers are required by law to notify NCMEC whenever they become aware of such content. If NCMEC establishes a European connection, it forwards the case to European law enforcement agencies (for example, in the case of a German suspect to Germany, to the German Federal Criminal Police Office – BKA).
  If, in the future, the 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.

- 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 as part of their complaint handling. The German hotlines of eco, FSM and jugendschutz.net, for example, first inform the German Federal Criminal Police Office (BKA) and only inform the provider after an agreed standstill period. If the provider has to inform the EU Centre in the future, which would then inform the BKA, there would be a duplicate notification to the BKA.

Furthermore, in the case of "flagged, unvalidated content", the immediate extraction of IP addresses and user data without prior state examination and evaluation is questionable in terms of the rule of law.

The timing of the information to the affected/reported users also seems unclear. The relationship between Art. 12(2) and (3) may trigger a duplicate information obligation where applicable. Insofar as this is intentional, there is a risk of the perpetrator being alerted. In any case, a corresponding clarification is needed.

The general and undifferentiated obligation to provide a reporting/flagging function must be questioned with regard to its actual practical use, especially with regard to traditional providers of hosting services. This is because, as a rule, it is not obvious to users which provider hosts a piece of content and to whom they should send a tip. If traditional providers of hosting services are nevertheless to maintain a reporting infrastructure, this must be practicable. In eco's view, it must be sufficient in this constellation, for example, if the provider of hosting services makes a reporting option available centrally on its own website. A flagging function to be implemented by the provider of hosting services and for which they are responsible on every website of their customers is not feasible and practicable. For flagging functions on individual websites, it would make sense to start with the provider of the respective service as the responsible party, as their options for action can be compared with those of platform providers.

In addition, it would make sense to give traditional providers of hosting services (especially SMEs) the opportunity to cooperate with central neutral contact points (for example, the established hotlines) to receive notices/reports in order to implement the obligation. For example, with appropriate cooperation, a link to the reporting forms of the hotlines would be conceivable instead of maintaining their own reporting infrastructure.

- **Strict take-down guidelines**

The planned obligation for hosting providers to take down CSAM upon request within 24 hours or to disable access to this content within the EU will be flanked by an obligation to report back to the coordinating authority and the EU Centre on the measures taken. In addition, affected users must be informed about the take-down/blocking and the right to complain after six weeks at the latest (or after 12 weeks if the obligation to maintain confidentiality is extended).

For the order, the content must have been classified as CSAM by the coordinating authority, a court or another "independent administrative authority" designated by the Member State. If this is the case, the coordinating authority can request the order, which is to be issued by the judicial or administrative authority after a subsequent examination.

Independently of this formal procedure for the so called removal order to be established with the present draft of the Commission, informal notifications of the host providers are to continue to be possible in the future, in which the provider

removes CSAM on the basis of indications and notifications, e.g. 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 here. eco suggests corresponding adjustments to the proposed regulation.

With regard to informing the users concerned, eco suggests seeking dialogue with the law enforcement agencies to ensure that investigations are not impaired and, in particular, that there are no unwanted alerts given to offenders.

Due to the well-functioning existing reporting channels via hotlines, eco believes 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. In the vast majority of cases, host providers will remove reported/flagged content within a very short time without a corresponding order, i.e. voluntarily. If a tip-off is received by an authority first, it must be ensured and guaranteed that their procedures are carried out swiftly to prevent further re-victimisation.

- **Access blocking/blocking of Internet content**

The planned obligation for Internet access providers allows for the blocking of CSAM URLs not hosted in the EU by means of (temporary) orders, where the host provider refuses the removal and cannot be forced to take down the content. The blocking is accompanied by information for users about the issued blocking orders.

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 and that the implementation of the provider's network blocking is effective and targeted.

The coordinating authority must review the continued necessity of the blocking order at least annually and adjust or revoke the order if necessary.

eco is critical of blocking online content for fundamental reasons. Access blocking is neither effective nor sustainable. Irrespective of this, the procedure proposed in the draft has a large number of problematic aspects and issues.

In the opinion of eco, the investigation and prosecution of the perpetrators as well as the effective and sustainable of the content must have top priority. Accordingly, it is essential to apply the focus on the fight against CSAM on international cooperation and collaboration in prosecution and erasure. With functioning processes and cooperation, URLs with CSAM can also be reliably and quickly taken down internationally.

The experience of the eco Complaints Office – i.e. the eco hotline – with the cross-border CSAM cases shows that take-down can be achieved more quickly internationally if the legal situation in the hosting country with regard to CSAM is

also identical in detail to that of the reporting country. eco, therefore, considers it essential to expand or strengthen international cooperation in any problematic cases. From eco's point of view, it is essential to become active at the political level and to advocate for further legal harmonisation in regard to CSAM. This is especially true in view of the fact that CSAM is, in principle, internationally prohibited and subject to criminal prosecution. In detail, there are nevertheless different standards internationally – and even in the EU – in the definition of depictions of abuse of children and adolescents as soon as one moves on from the area of the so-called "baseline cases" (i.e. depictions of acts of abuse on prepubescent minors).

From eco's point of view, the matter of determining how the Internet access provider has been used to access CSAM in the prior 12 months seems highly questionable. This would require access providers to monitor user behaviour and thus the "content". This, in turn, would be highly precarious from the point of view of data protection, the prohibition of general surveillance obligations, and the secrecy of telecommunications.

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 on on 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 on CSAM. From eco's point of view, the regular check of these URLs must also include changes of the host provider. If a change in hosting is identified during 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 take into account the priority of taking down CSAM, 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.

II. Implementation/enforcement of the regulation

- **Designation of competent 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 that establish new structures as a consequence.

The proposal implies that it is not possible to fall back on already existing structures and established actors and that already existing cooperations and synergies are not to be used, expanded and intensified. In this regard, eco urgently suggests adapting the stipulations and enabling a strong involvement of the established structures as well as the cooperation of the different actors and their expertise at the level of the

Member States. The EU Commission's wish for neutrality would not be jeopardised by this, in eco's view.

- **Establishment of a dedicated EU Centre**

An EU Centre shall be established as an EU Agency. 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 new 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 CSAM. Therefore, eco suggests explicitly involving existing structures and cooperations and building on their activities and experience.

The INHOPE network (www.inhope.org) with its hotlines has been active for more than 20 years in many areas. According to the draft regulation, the EU Centre will, in the future, also have the responsibility to establish these areas (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 CSAM 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 seems urgently necessary.

- **Technology for the implementation of detection obligations**

The draft regulation states that, in the event of a detection obligation, the company concerned may have recourse to technologies to be provided by the EU Centre.

This option, which at first glance seems supportive, will pose considerable challenges in practice. Ultimately, each provider has its own technical setting. In practice, there is a great diversity in the technologies used. The integration of a provided technology always has the challenge that it must be compatible with the existing technical infrastructure. eco sees the risk that this is not sufficiently taken into account in the provision of technology by the EU Centre.

If the provider cannot use EU Centre technologies due to lack of compatibility, it must ensure in the short term, with its own resources and effort, that detection technologies are available that are effective, reliable, state-of-the-art and as non-intrusive as possible. This development is likely to take some time and may take

longer than the period of time allowed for companies to start detecting after the issuance of the detection order (three to 12 months).

- **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 believes that it is still too high. Especially with regard to the great diversity of the companies concerned and the inclusion of SMEs with fewer resources, eco suggests a reduction of the range of fines.