

**Proposal for a Regulation laying down rules to prevent and combat
child sexual abuse**

(9068/22)

Contents

AUSTRIA	2
BELGIUM	4
CROATIA	6
DENMARK	7
FRANCE	8
GERMANY	13
GREECE	16
HUNGARY	18
IRELAND	44
ITALY	46
LATVIA	47
LITHUANIA	49
MALTA	50
THE NETHERLANDS	52
PORTUGAL	55
SPAIN	57

AUSTRIA

Austria communicates to you its written comments on Articles 1 to 7 of document ST 9068/22 (CSA proposal) and a question of general nature:

The question of general nature:

Is a direct transmission of suspicious reports from US ISPs via the US National Centre for Missing and Exploited Children (NCMEC) directly to the EU MS then still admissible?

Or will the report have to go through the EU centre in the future?

If this is the case:

- How can it then be ensured that there is no loss of time? This would be particularly fatal in the case of reports of hitherto unknown abuse material - since it can be assumed here that the victim is still in the custody of the perpetrator.

- Can US internet service providers offering their services in the EU continue to scan their content using the indicators available to them and report suspicious activity reports to EU law enforcement authorities?

Or can these now only be communicated to EU authorities if there is a specific detection order?

The comments on Articles 1 to 7:

Chapter I

Article 1:

Austria has a scrutiny reservation. Austria will examine the limits of the scope of application in the context of the discussion of the other chapters of the draft and will submit further comments and proposals for amendments to Article 1 at a later date.

On para. 4:

Recital 9 states that the provisions of the proposal provide for exemptions from the requirements of confidentiality of communications and traffic data under Articles 5 and 6 of the e-Privacy Directive, in accordance with Article 15(1) of the e-Privacy Directive. Recital 9 applies this provision by analogy, as Article 15(1) exclusively empowers Member States to adopt national regulations. The analogous application of Article 15(1) of the e-Privacy Directive appears questionable for the following reasons: Recital 11 of the e-Privacy Directive states with regard to Article 15(1) that the Directive does not apply to areas that are not covered by Community law. The competence of the member states to enact their own regulations in the areas of public security, national defence and state security as well as for the enforcement of criminal law provisions therefore remains unaffected as long as they are designed in conformity with fundamental rights. The aforementioned areas of law fall predominantly, if not exclusively, within the regulatory competence of the Member States. This leads to the conclusion that Article 15(1) of the e-Privacy Directive therefore exclusively "empowers" the Member States to enact such regulations, because only they are competent to enact regulations in these areas. It is therefore fundamentally doubted that Article 15(1) of the e-Privacy Directive can be analogised to the extent that a regulatory competence of the EU can be derived from it, because there is no unintended gap here. Even if Article 15(1) of the e-Privacy Directive could be applied by analogy, the fact that Article 15(1) only mentions measures of internal and external security stands in the way of its use in this specific case. As far as can be seen, it has been assumed so far that the present draft regulation is not intended to deal with law enforcement

measures, but with the harmonisation of the internal market. In this case, the draft would not be a permissible exception to Articles 5 and 6 of the e-Privacy Directive according to Article 15(1) e-Privacy Directive. The Presidency and the EC are therefore requested to clarify whether the present draft is a law enforcement measure within the meaning of Article 15(1) of the e-Privacy Directive.

Furthermore, it is stated that the proposed measures for monitoring and prior checking of the content of users of internet services without concrete grounds for suspicion and without differentiation is not proportionate in the sense of Article 15(1) of the e-Privacy Directive.

Accordingly, there are also massive fundamental rights concerns, in particular with regard to a violation of the right to privacy under Article 7 CFR and the right to data protection under Article 8 CFR. Fundamental rights concerns exist regarding the de facto elimination of all possibilities to use end-to-end encryption of communications in messenger or chat services. The technical implementation of content access to electronic communication is not directly determined by the draft, but in fact content access can only take place through a fundamental breach of secure end-to-end encryption. In addition, the error rate in automatic content recognition is also problematically high. How should this be seen in the context of the required IT security and in relation to secure and confidential communication?

Article 2:

Austria has a scrutiny reservation. Austria will review the definitions during the examination of the other chapters of the draft and will make further remarks and amendment proposals for Article 2 at a later time.

Concerning lit. u:

Is it conceivable that a service provider with its main place of business in a third country has a representative office in several EU countries? What is the procedure then?

What about internet service providers that do not have a branch or representation in the EU? Will they have to actively exclude EU citizens from using their services in the future?

Chapter II

Article 4 line 3:

Communication service providers should provide young users with "options to prevent grooming". What measures should be considered here?

Article 7 line 9:

With this provision, the application period of the detection order is limited to 24 months in case of a risk according to § 207a of the Austrian Criminal Code and to 12 months in case of a risk of grooming.

Is a new risk analysis mandatory thereafter? Is there an accelerated procedure for extending the order in the case of an existing risk?

BELGIUM

At this moment we would like to uphold a general scrutiny reservation. We will study the answers given by the Commission during the last meeting on 5 July, but wanted to confirm some other questions we have:

- We welcome the proposed online seminar in October on the possibilities related to detection technologies and end-to-end encryption. We note in Article 7(4), 1st subparagraph, (b) the condition that *“the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties”*. Elsewhere, in Article 16(4)(d) with blocking orders, we read that those fundamental rights can contain also the provider’s freedom to conduct a business. We noted that the Commission mentioned that “if detection technologies without lowering the privacy level do not exist, detection will not be ordered” but also that those technologies do exist. We hope to gain more insight in the achievable practical end results if a provider is thus arguing that all available solutions provide a lower privacy level than end-to-end encryption (which the study in annex 9 of the impact assessment, especially the table on page 309, clearly confirms), which poses problems for not only the users but also the provider’s legitimate interests and freedoms, and that this thus should preclude an obligation to use those solutions.
- We welcome the announced documents which will shed a light on the comparison with the Digital Services Act and the Terrorist Content Online Regulation. We note that the Commission informed us that Article 8 of the Digital Services Act would not be considered applicable here in the CSA Regulation. However, for example, the minimum requirements related to the notice and action mechanism on the other hand are to be considered applicable. We wonder whether it would not be better to include more concrete references to the DSA in all the relevant Articles. At the very least it seems that it should be mentioned in the text that Article 8 is not applicable as one could easily understand recitals 7 and 8 to imply that this Article 8 concerns an issue that is not or not fully addressed in the CSA Regulation.
- The Commission confirmed that voluntary referral by hotlines to the providers is still possible. Voluntary notifications by the Member States (Article 32) and the EU center (Article 49) are explicitly mentioned in the text. Would it not be advisable to take up a similar reference for the hotlines, for example in the recital 70?
- We understand that Article 2(a) and Article 2(g) refer to the definitions of the DSA. How will this however in practice be streamlined with the slightly different definitions in the TCO Regulation? How will be prevented that different understanding arises concerning which providers are meant and how EU legislation applies to them?
- Would it be advisable to look into the use of the word ‘recipient of the service’ instead of ‘user’ in Article 2(h)? Of course, we would then have to be sure that ‘recipient of the service’ also includes for example a child using the phone of a parent.
- Does Article 6(2) imply that the providers of software application stores would receive the content of the risk assessment of the providers of the apps?

- The reference “*competent judicial authority of the Member State that designated it*” in Article 7(1) seems unduly complicated. Could it be clarified, maintaining the objective to target the competent authority of the member state of establishment? For example “(...) *shall have the power to request the competent judicial authority of its/that Member State* (...)”?
- In relation to Article 7(4) we wonder if elements of proof (that the detection order is thus necessary and the conditions are fulfilled) can also be transmitted by the competent authorities of other Member States. This is not clear to us in the text.
- Based on the phrase “*it is likely, despite any mitigation measures that the provider may have taken or will take, that the service is used, (...)*” in Article 7(5)(a), we would like to know whether a detection order can be issued without first having to resort to sanctioning a lack of mitigating measures. So, if a provider is not complying with its obligation (based on Article 4) to issue mitigating measures, can we immediately issue a detection order or do we first have to issue a sanction in relation to Article 4 before being able to issue a detection order?
- In Article 7(5), (6) and (7) it reads “*the service is used, to an appreciable extent*” for CSAM. This seems to be a very vague notion. On what criteria will this be examined? Could this be specified in the recitals?
- We also would like to understand better the impact of the proposed age of 17 years (or 18 years as was mentioned by several Member States) in relation to grooming. If a Member State would issue a detection order, would/could this then – taking into account its own legal framework – be limited still to the age limit in use in that specific Member State? Or would/should this then be always this standardized 17 years (or 18 years), which would mean that a detection order is issued for something that is not illegal in that jurisdiction – which could create possible difficulties with regard to the derogation of the ePrivacy Directive it seems.

CROATIA

- Child users - the proposal refers to persons under the age of 17 when soliciting sexual activity on the Internet, which is different from the national age limit in the Republic of Croatia.
- The process of creating a risk assessment should be additionally sketched or more precisely explained by the responsibilities that the national coordinating bodies will have. We join the request for an overview of the functioning and tasks of national coordination bodies.

DENMARK

We are reviewing the proposal for the regulation laying down rules to prevent and combat sexual abuse (the CSA) with great interest and we are looking forward to cooperating with you on the file.

We understand that the negotiations are still at an early stage. However, we would like already at this point to raise our concerns relating to Article 28 (1) (c) and in that regard bring a proposal for rephrasing the provision as set out below.

”(c) the power to impose fines, **initiate legal proceedings for the imposition of fines, e.g. by courts, or both, in accordance with national rules and procedures**, in accordance with Article 35 [...]”

The reason for the proposed rephrasing is, that according to the widely accepted interpretation of Section 3(3) of the Danish Constitutional Act, Danish administrative authorities cannot, with binding effect, impose fines or other sanctions characterized as punitive under Danish law. Thus, if Denmark were to introduce the possibility of applying administrative fines, as prescribed in Article 28 (1) (c), as a means of sanctioning breaches of EU law, it is highly likely that Danish courts – ultimately the Supreme Court – would strike down such fines as unconstitutional. As a result, it is not possible for Danish authorities to impose such fines.

At the same time, an administrative authority cannot request directly a judicial authority to impose a fine under Danish national law. The administrative authority must refer the matter to the police and public prosecution service with the purpose of enforcing the law by initiating criminal proceedings before the Danish courts. The reason for this system is that the public prosecution service is subject to a number of important procedural guarantees, which strengthen the position of the accused and the defense.

When the public prosecution service has to assess the issue of prosecution in a criminal case, it does so on the basis of the principle of objectivity, as provided for in the Danish Administration of Justice Act, which is a fundamental principle in Danish criminal justice and is considered one of the most important procedural guarantees of legal certainty. The principle entails that the public prosecution service and the police are obliged to carry out their investigations in an objective manner. This means that the public prosecution service must ensure that criminals are brought to justice, but also that the prosecution of innocents does not take place.

As the current Article does not prescribe for such procedure, we suggest the above stated changes to Article 28 (1) (c), which we believe still protects the purposes of the current article.

We therefore kindly ask you to amend the article as suggested.

FRANCE

General comments

The French authorities would like to begin by welcoming the Commission's proposal and emphasize that they support the general principles set out in it.

However, **the French authorities will be very careful to preserve certain national mechanisms** - in particular the French platform for harmonization, analysis, cross-checking and guidance of alerts (PHAROS) - and not to duplicate tools. They point out that the national mechanisms put in place in some Member States are fully satisfactory and that the balance found must not be undermined in any way.

In addition, the French authorities emphasize the particular complexity of the mechanisms proposed by the regulation and suggest injecting a certain amount of **flexibility** into them. While the French authorities understand and support the need to protect the fundamental rights and privacy of individuals, they believe it is necessary to consider simplifying the proposed tools. For example, the French authorities do not understand, in the context of a takedown order, the **multiplication of actors** before issuing such an order when the very purpose of takedown is to act quickly to **remove** content accessible to all. The French authorities point out that in 2021, the national PHAROS platform requested more than 118,000 removals of child pornography content.

Furthermore, the French authorities believe that **law enforcement authorities** should be more involved in the implementation of injunctions and in the overall architecture of the regulation.

With respect to private communication services and encrypted content in general, the French authorities favor finding **solutions that do not weaken encryption** and they remain vigilant about not imposing particular technologies or means on service providers to comply with the new provisions. Indeed, providers would then be forced to weaken their system to integrate the imposed technology and thus weaken the encryption mechanisms in place.

Finally, the French authorities wish to emphasize that this proposed regulation must be implemented in a manner consistent with existing European legislative instruments such as the **TCO** (Terrorism Content Online) regulation and the "transversal" **DSA** (Digital Services Act) regulation.

Comments by article

- Article 1 (subject matter and scope of the text): to be consistent with the DSA, it would seem appropriate to include search engines in the scope of the actors covered by the regulation. Therefore, Article 1 of the proposed regulation could be completed in this sense. In this context, it should be stressed that the proposed CSA regulation (child sexual abuse) does not provide for an obligation to remove content **from search engines**. The Commission will have to be questioned on this point, underlining that this tool is frequently used by the French authorities to reduce the accessibility of illicit contents to the public.

It is also necessary to **state in the text that the provision does not apply to government communication** systems.

Furthermore, it might be appropriate for article 1 paragraph 3 to make an express reference to the so-called "**TCO**" (terrorism content online) regulation in order to preserve its functioning, as is the case with other texts within this paragraph.

Risk assessment (Chapter 2. Section 1. Articles 3,4,5)

- **section 1 (risk assessment and mitigation obligations):** this section provides for the obligation for hosting companies and interpersonal communication services, regardless of their size, to develop an analysis to assess the risks that their services may be misused for the purpose of sexual abuse of minors and, on the basis of this analysis, to take measures to mitigate the risks. The DSA (Digital Services Act) also provides for such obligations (articles 26 and 27 of the final compromise), but only for very large platforms and search engines. It would therefore be advisable to ensure that the obligations of the DSA and those of the ASM regulation are properly articulated for these very large players, who will be subject to both. In this perspective, it could be useful to add a provision in Chapter II, Section 1 of the ASM Regulation aimed at clarifying this articulation.

- **Article 6** sets out obligations for the application stores. They must, if possible together with the application providers, assess whether a service can be used to solicit children online (the so-called "**grooming**" phenomenon). They must prevent minors from accessing the service if there is a significant risk, but the question of implementation arises. In addition, there are no specific measures to verify age or identity, and in the opposite direction, no measures to verify that an adult would not use children's applications for malicious purposes. However, locking the regulation in too precise technological processes, corresponding to technological innovations, would not allow it to evolve at the pace of technology. It is therefore a question of expediency whether to be precise, which could quickly become outdated, or to take "**reasonable measures**" that would allow an independent authority to adapt to technology in order to prevent and fight against the phenomenon of child solicitation.

- Injonction de détection (article 10 paragraphe 6)

First of all, we should mention a specific service in France, namely the CNAIP (national center for the analysis of child pornography images), which centralizes data of a child pornography nature (photos, videos) and contributes to the detection of illicit content.

- With regard to Article 10(6), the Commission's proposal states that:

"Where a provider detects potential online child sexual abuse through the measures taken to execute the detection order, it shall inform the users concerned without undue delay, after Europol or the national law enforcement authority of a Member State that received the report pursuant to Article 48 has confirmed that the information to the users would not interfere with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences."

However, Article 48 specifies that it is the competent authorities of the Member States - and not Europol - that have to confirm that the information to the user would interfere with an investigation. The Commission should therefore provide more information on this difference in wording, which has serious practical consequences. In any case, the French authorities are **opposed to Europol being able to confirm that a user's information compromises an ongoing investigation**. They point out that Europol is an agency that supports Member States, that it acts only if two or more Member States are affected and that it can in no way commit the competent national authorities.

Moreover, the French authorities welcome the mechanism for challenging an injunction, which offers a highly important guarantee, particularly for users. Indeed, Article 10(5) provides that: "The provider shall inform users in a clear, prominent and comprehensible way of the following: the users' right of judicial redress referred to in Article 9(1) and their rights to submit complaints to the provider through the mechanism *referred to in paragraph 4, point (d) and to the Coordinating Authority in accordance with Article 34* ».

- **Article 9(1)** provides that "providers of hosting services and providers of interpersonal communications services that have received a detection order, as well as users affected by the measures taken to execute it, shall have a right to effective redress.

According to the French authorities, if the possibilities of recourse already existing in domestic law (6-4 LCEN, law for confidence in the digital economy) for the - withdrawal injunctions - do not pose particular problems, this right of recourse such as formulated in the context of the detection injunction does not seem to be sufficiently circumscribed and risks to weaken the current recourse processes. Indeed, each user will be able to exercise a right of appeal if he is affected by the measures taken for the detection order. However, the French authorities raise the question of what the concept of "affected" encompasses, which could, according to them, affect all users of a platform subject to a detection order. However, the French authorities point out that, given the number of users affected by a detection order, the judicial authorities risk becoming overloaded and not being able to study all of the challenges within a respectable period of time and, de facto, risk further undermining the right to a trial within a reasonable period of time (article 6 paragraph 1 ECHR).

During the "Police" group of June 22, 2022 (LEWP-P), the Commission indicated that the use of AI would probably be classified as "high risk" in the sense of the proposed regulation on AI, insofar as the latter detected images and conversations related to "grooming". This classification should not constrain/limit investigations based on the use of AI systems for child sexual abuse or the detection capabilities of online service providers.

Supplier Reporting Requirements (Section 12)

The French authorities welcome this mechanism which allows providers to report to the Center all content potentially related to sexual abuse. They also welcome the creation of a "flag" system for content made available to users.

In this context, the French authorities raise the issue of double reporting that could occur for the same content. They point out that the Member States receive reports directly from public and private actors, in particular from the NC-MEC (national center for missing and exploited children). While the French authorities have taken note of the Commission's explanations on this point, they consider that it would be difficult in practice for the Center to know whether the NCMEC has actually transmitted an alert to the internal security forces. The French authorities are firmly **opposed** to the idea of a deconfliction solution whereby **NCMEC would transmit its alerts exclusively to the Centre**.

In connection with the preceding remarks, the French authorities raise the question of the time frame within which the internal security forces will have access to the alert from the Centre. At present, in France, user alerts provide instant information and enable rapid action to be taken. However, the mechanism provided for in Article 12 involves intermediaries - the Centre - and additional stages - the assessment of the basis for the alert - which risks lengthening the transmission chain.

The French authorities note that the current Article 15a of the compromise text of the DSA provides that when a hosting service provider becomes aware of information giving rise to a suspicion that a criminal offence posing an imminent threat to the life or security of persons has been committed or is about to be committed, it shall immediately inform the authorities responsible for the investigation and prosecution of criminal offences in the Member States concerned. A similar obligation is laid down in Article 14(5) of the TCO Regulation.

The French authorities believe that, at least in situations where ASM content clearly gives rise to a suspicion that a criminal offence posing an imminent threat to the life or safety of persons has been committed or is about to be committed - such as a child rape broadcast via live streaming - prior analysis by the Center seems superfluous. Service providers should be able to automatically remove the content in question and notify the competent authorities in criminal matters.

Finally, the French authorities question the two deadlines proposed in the regulation:

- On the reasons for inserting a period of 3 months within which the competent authorities will have to inform the providers via the Center of their willingness to inform the user or not in order not to harm an ongoing investigation and indicate that they consider this one too short. In this respect, it proposes **to replace the 3-month period with a more general formulation: "within a period set by the law enforcement authorities"**.

- on the relevance of an 18-month period that does not follow any objective criteria. The French delegation recalls that some users may be involved in long and complex investigations and that it would therefore be appropriate to **extend this period**.

Removal order (Article 14)

As a preliminary matter, the French authorities question the term "remove" and ask the Commission to clarify whether this term implies a removal of the content from the servers or simply a public removal of the content.

In addition, the French authorities question the need to call upon an independent judicial/administrative authority to issue a takedown order, at the risk of making the process considerably more cumbersome and when the draft text already provides for the intervention of another independent administrative authority (the "national coordination authority") in the process. They consider that **an administrative authority should be able to issue removal orders** for child pornography content. They may recall that Article 8 of the DSA provides for the possibility for national judicial or administrative authorities to issue such injunctions.

In addition, following the example of what is practiced for online terrorist content and based on the model of the TCO regulation, the French authorities consider that the **competent national authorities should be able to issue, on their own initiative** (and not necessarily on the proposal of the national coordinating authority), **injunctions for the removal** of content relating to online sexual abuse of children to the attention of providers.

Moreover, the French authorities question the possibility for the judicial authority to set the duration of the period of non-information of the user, while the law enforcement authorities can set this period themselves for the other injunctions. Also, the French authorities note that this period of non-information is set by the judicial authority after a "simple consultation" of the "public authorities". The French authorities therefore question this "consultation", which is not binding on the judicial authority. Finally, on this point, the French authorities question the notion of public authority, which seems broader than the concept of "law enforcement authorities".

Furthermore, with regard to the duration of the withdrawal, there is a different time limit between the TCO regulation and the proposed ASM regulation. If the Commission explains this by differences in the nature of the two regulations, would it not nevertheless be appropriate to align the procedures provided for in the ASM and the TCO as much as possible?

Blocking order (Articles 16 to 18)

The implementation of a URL blocking requires a decryption to access the URL. Beyond the impact of decryption on the level of security, administrations have, to date, neither the infrastructure nor the technical capacity to perform this decryption. The French authorities therefore **recommend IP filtering**, either directly or by sinkhole. In addition, the French authorities would like to assure the Commission of their correct interpretation of the **concepts of "remove" and "disable access"**. The choice between "remove" and "disable access" is applicable only to "removal orders" under Article 14. This distinction could allow the host to choose between :

- a removal of the content ("remove") which then becomes inaccessible to all Internet users,
- or a more or less extensive limitation of its access ("disable access"), which would allow, for example, a host to prohibit access to Internet users in the country that has made the request, while allowing Internet users in the rest of the world to access it normally.

With respect to Article 16, the French authorities propose **adding the adjective "adapted"** to the text to specify what is expected of providers: "The Coordinating Authority of establishment shall [...] under the jurisdiction of that Member State to take reasonable and adapted measures to prevent users from accessing known child sexual abuse [...]."

Points to be clarified by the European Commission

At this stage of the analysis, the French authorities have identified two points which, subject to explanation by the Commission, could hinder the proper understanding of certain provisions.

Article 5(1) provides that: "Providers of hosting services and providers of interpersonal communications services shall transmit, by three months from the date referred to in Article 3(4), to the Coordinating Authority of establishment a report specifying the following".

However, Article 3(4) refers to the costs incurred by the Centre in carrying out the analysis of the data samples requested by the providers and does not indicate any date as mentioned in Article 5(1). Thus, it would be appropriate **to modify and replace with the correct reference (Article 3 paragraph 6).**

Furthermore, Article 14(5) on the impossibility of carrying out the withdrawal order, particularly in cases of force majeure, refers to the time limit laid down in paragraph 1 of the same article. However, the French authorities note that **paragraph 1 of Article 14 does not refer to any time limit, but paragraph 2**, which requires the supplier to comply with the order within 24 hours.

GERMANY

General

- Germany welcomes the opportunity to comment on the articles of the first two chapters.
- Given that the Federal Government has not yet completed its examination of the Regulation, we would like to enter a **scrutiny reservation**.

Chapter I:

Regarding Article 1 (Subject matter and scope):

- Paragraph 1 includes the term “uniform rules”.
Are we correct in assuming that the Commission intends to achieve a minimum degree of harmonisation with its proposal?
- We (explicitly) welcome that paragraph 2 focuses on services that are offered in the EU, thus ensuring a level playing field between providers based in and outside the EU.
- Paragraph 3 (b): We would like to ask the Commission once again to clarify the connection between the Regulation and the Digital Services Act: can the Commission confirm that the Regulation should take precedence over the Digital Services Act according to the principles of *lex specialis*? If so, Germany believes that the wording of Article 1 paragraph 3 (b) (“This Regulation shall not affect...”) should be revised.
- As we understand it, the Commission wants the draft Regulation to serve as a legal basis for providers of services for the processing of personal data for the execution of detection orders under Article 6 GDPR and for the envisaged EU Centre as referred to in Regulation (EU) 2018/1725. We therefore ask the Commission to state this more precisely in the draft version.

Article 2 (Definitions):

- Regarding (a) and (b): According to the definitions of the Digital Services Act, “hosting services” include “cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing”. Interpersonal communications services also include number-independent voice calls, all types of emails, messaging services and group chats. We currently believe that the technological measures which the Commission’s proposal applies to the different types of services encroaches upon several fundamental rights, and we therefore expressly enter a scrutiny reservation. Furthermore, we ask the Commission to clarify the proportionality of the envisaged obligations regarding the different services (including cloud services).
- It would be difficult to require providers of cloud services in the dark web to execute detection orders. We therefore ask the Commission to explain how detection orders should be enforced in the dark web.
- To what extent does the Commission’s proposal take into account further alternative action in the dark web?
- Can private activities such as private hosting of email addresses fall within the scope of this Regulation?

- Does the Commission also intend to apply the obligation to providers of data/image hosting services who only store such content to combat the distribution of CSAM? If so, which measures does it intend to take?
- Regarding (l), (o) and (q): To what extent does the Commission's proposal take into account differences in national criminal law? As we see it, such differences also arise with regard to the definitions of Directive 2011/93/EU:

For example, in Germany, child grooming is punishable when it affects children (under the age of 14) but not when it affects adolescents (between the ages of 14 and 18). However, we understand the draft Regulation to mean that attempts to groom adolescents also constitute solicitation of children and thus online child sexual abuse as defined in paragraph (p).

The production and possession of juvenile pornographic material is also not punishable in Germany if it was produced only for personal use and with the consent of the persons depicted. However, we understand the Commission's proposal to mean that youth pornography also constitutes online CSAM as defined in paragraph (p) without exception.

Chapter II

Section 1 "Risk assessment and mitigation obligations":

- In Germany's view, imposing more obligations on providers of certain online services is the right approach for fighting CSA. Requiring more preventive measures can significantly help to make the online environment more child-friendly and to prevent CSA.
- Germany believes that the mandatory risk assessment and risk-mitigation measures which the proposal calls for can help to improve the targeted protection of children and young people against harmful media, as long as private communication remains confidential, and anonymous or pseudonymous use of online services remains possible. However, Germany believes further specification is needed:
 1. We believe binding parameters for risk assessment are necessary in order to significantly increase consistency and legal certainty.
 2. We also believe it is necessary to describe (using examples) which risk-management measures companies are to take. In our view, this could take the form of examples.
- On this point, we also ask the Commission to explain its idea of what constitutes lawful risk management under the Regulation, possibly on the example of particular services. Germany does not believe that it would be sufficient to issue specifications in the planned Guidelines alone (see Article 3 (6) and/or Article 4 (5)).
- Germany is in favour of stricter enforcement of age assurance and age verification measures to mitigate risks and with regard to the obligations of providers of software application stores, as long as the services in question can continue to be used anonymously and pseudonymously. We therefore ask the Commission to describe its support for initiatives for age assurance and verification measures which require a minimum of data (see the BIK+ strategy). What are the specific approaches in this area?

Section 2 “Detection obligations”:

- Germany is in favour of uniform, Europe-wide obligations for certain providers to identify known CSAM.
- In view of the fundamental rights concerned and the possibility of false positive reports (which cannot be ruled out no matter which technology is applied), we are currently conducting an intensive review of the options for identifying new CSAM and grooming and will have more to say about this at a later time.
- We are also carefully reviewing the multi-step procedure proposed by the Commission for issuing detection orders and will comment on it in greater detail later. To aid in visualising the planned processes, we ask the Commission to provide a diagram illustrating the various steps in the planned procedure for issuing detection orders.
- Article 7 (4) states that “evidence of a significant risk” is required before a detection order can be issued. Paragraphs (5), (6) and (7) provide further details as to what constitutes a significant risk. Germany nonetheless believes that additional specification is needed to define “significant risk” with legal certainty and ensure that the CSA Regulation can be applied uniformly. Germany believes that such specification should be included in the text of the Regulation itself, rather than only in the Guidelines.
- According to the proposal, providers of hosting services of publicly disseminated communication can be required to identify online CSA. It is both the responsibility and in the interest of providers to keep their publicly accessible platforms from being used to disseminate online CSA (see for example the statement by Meta at the CSA seminar in Paris on 14–16 June).
- Germany welcomes the Commission’s technology-neutral approach. Providers of interpersonal communication services too are responsible for preventing the dissemination of online CSA via their services; it should therefore be possible to require them to do so. With regard to the technologies to be used, however, we still see an urgent need for clarification, especially concerning the following points:
 - The Regulation must not lead to general interception of private, encrypted communication where there is no suspicion of wrongdoing.
 - Germany is in favour of seamless, secure end-to-end encryption which must not be undermined, neither in technical nor in legal terms. This is one objective of the Coalition Agreement of Germany’s Federal Government, as is the fight against child abuse.
- With this in mind, Germany believes it is necessary to state in the draft proposal, for example in Article 10 (3) (a) (new), that no technologies will be used which disrupt, weaken or modify encryption. The Federal Government is still in the process of reviewing the use of other technologies.
- In view of the fundamental rights concerned, it is necessary in the interest of proportionality to ensure that the technologies to be used are sufficiently sophisticated and fit for purpose, with a minimal error rate.

GREECE

Introduction:

Initially, we would like to provide some general remarks, outlining our afterwards interventions:

The Greek competent authorities for the fight against the online CSAM face the following primary operational deficiencies: 1) Encrypted communications obstruct the success of criminal investigations and seriously harm their effectiveness, 2) Public WI-fi provide a safe internet connection to the perpetrators since the users do not oblige to declare the mac (media access control) address of their device for the access, 3) The availability of the NAT (Network Address Translation) and the VPN (Virtual Private Networks) create significant difficulties for the detection of the IP address and the identification of the perpetrator and 4) The variety of data retention periods even in the EU (e.g., it is one year in Greece and only a few days in an another Member State). Additionally, the perpetrators of this type of crime are moved on the dark web or exploit selected encrypted messaging services based on the denial of their handlers to provide the necessary data.

From the legal perspective, detecting, removing, and blocking CSAM in cyberspace constitutes an interference with the rights of personal life, personal data protection, expression, and confidentiality of communications. Consequently, these actions must be subject to end-to-end safeguards, complying with the principles of necessity and proportionality in all stages of the process.

Regarding the technological domain, we have to pay attention to the current reliability and accuracy of the tailored technologies. Our legislative efforts should be based on independent public assessments and not only on outcomes derived exclusively from private companies.

To conclude, we propose to examine the necessity of the establishment of the Centre at this stage, because the new Centre is referred from the first articles.

Article 2 (definitions):

We will express two modifications and one new suggestion concerning the definitions of article 2.

Par. (m) stipulates that the known CSAM means potential CSAM. We propose to use the word unconfirmed or unverified instead of known because the existence of the words known and potential complicates the meaning of this definition.

In the same spirit of legal clarity on par. (n), we ask for the deletion of the word new and its replacement with the word suspicious.

Furthermore, we suggest inserting a new definition for the indicators, aiming to underline their importance for detecting suspicious CSAM and, simultaneously, to reduce the conception of preventive mass surveillance of online activities, including interpersonal and encrypted communications.

Finally, we support the French proposal to harmonize the age of 18 on par. (i) and (j).

Article 4 (risk mitigation):

One question for the Commission concerning the par. 4 and the last phrase, "*That description shall not include information that may reduce the effectiveness of the mitigation measures.*" Which is the consideration for this provision? Could the Commission mention particular examples?

Article 5 (risk reporting):

A question for the Commission. How is the consistent management of the risk assessments by the various Coordinating Authorities ensured, refraining from different handling?

Article 7 (issuance of detection orders):

For this article, we declare a scrutiny reservation. In principle, we agree with the approach by the Commission, following the relevant case-law of both the Court of Justice and the European Court of Human Rights. For instance, one of the prerequisites is the decision to be issued by a judicial or an independent administrative authority. We are coming back to the structural matter of data retention. How does the Commission consider the implementation of a detection order in a Member State when its data retention period is too limited?

HUNGARY

HU fully supports the objectives of the draft regulation; however, we have some general comments regarding its approach on certain important elements.

The proposed legislation appears to have a complex enforcement structure, with no clear or well-defined competences, even though it builds on the solutions used in the draft Digital Services Regulation (hereinafter "DSA") and in Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on combating the dissemination of terrorist content online (hereinafter "TCO"). According to the TCO Regulation, the coordinating authority and the judicial or independent administrative authority are one and the same, but they are separate authorities in the draft Regulation laying down rules for preventing and combating sexual abuse of minors (hereinafter 'CSA'). A simpler solution is for the competent authority to be able to issue blocking or removal orders itself, rather than having to go to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplications should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

The limitations of URL-based screening in the draft proposal could undermine the effectiveness of the CSA Regulation and it would therefore be appropriate to include digital fingerprint-based screening among the technical options.

In Hungary, the problem of end-to-end encryption, which makes it difficult to detect certain crimes and to access and use electronic evidence in criminal proceedings, poses a significant challenge, and it is therefore essential to create the technical conditions for law enforcement agencies to have access to e-evidence, while ensuring appropriate safeguards. In order to act more effectively, possible solutions in this area need to be explored and the Europol Innovation Lab will increasingly provide priority support in this exploration.

We agree with the delegations that called for Europol to be involved in the negotiations on the draft as soon as possible.

It is not clear from the proposal how the new institutional system will draw on the experience of INHOPE and the Member States' Internet hotlines and incorporate them into the institutional system.

In Article 83(2)(a), the proposal provides for data collection based on "gender"; however, for Hungary only the data collection on the basis of sex would be acceptable.

The role, competences, and location of the EU centre to be established should be deeply discussed.

Chapter I

We agree with the subject matter and scope set out in Article 1 of the draft, with the reference in Article 1(4) to Chapter 2, Section 2 of the Regulation.

The definitions need to be reviewed. In Article 2 of the draft, we propose to include in point (j) of the definitions an age limit of 18 years or a reference to the age of consent of the Member States, 17 years being unacceptable in this form. We suggest to change it in coherence with the previous definition, or refer to the different interpretation within the MSs.

Chapter II

The title of the chapter does not reflect its content. Sections 2 and 4 already deal with the issuance of a detection and removal decision, which concerns the role of the coordinating authority rather than that of the service provider. The wording of the regulation is very far from meeting the requirement of clear, unambiguous and transparent regulation. It would be good if these powers could be merged or restructured.

In Article 3 par 4 (Subsequently, the provider shall update the risk assessment where necessary and at least once every three years from the date at which it last carried out or updated the risk assessment) the timeframe looks a bit too long, this assessment should be a living exercise

The question of whether the condition in Article 7(4)(a) is fulfilled is partly a police matter, while all other tasks could be carried out by a designated authority, as in the TCO Regulation. The wording of Article 7(4) is incorrect, as it seems to completely exclude the discretion of a judicial authority or an independent administrative body, whose decision is formal if the conditions are met. If this is the aim, it also seems more realistic to concentrate powers in the hands of the judicial authority or the independent administrative body.

The language of the orders as defined in sections 2 and 4 should be the official language of the issuer and English, not the language requested by the service provider. Significant additional administrative burden and costs may be induced by translations. We require here a ruling on the official language of the Coordinating Authority and English.

Immediate fulfilment of the information obligation in Section 3 Article 12 (undue delay) may cause problems for law enforcement action and should be suspended, if possible, pending the reaction of EU headquarters. Immediate compliance with the obligation to provide information may cause problems for law enforcement action, which should preferably be suspended pending the reaction of EU Centre.

The provisions on victim protection and support services and their information, as set out in Articles 20, 21, do not reflect the fact that victims are necessarily children. There are no rules on representation, the situation and consequences of the sexual exploitation of children within the family are not addressed, and no reference is made to the relevant EU rules in force. We are talking about children victims here, thus we need a very detailed explanation here on requirements and obstacles. The proposed legislation does not cover rules on representation and protection against criminal parents as legal representatives. In accordance with the first two paragraph of Article 21 we should refer on the applicable EU legislation concerning victim protection and support, and we should channel these activities into the existing mechanisms in this field.

Article 22 requires service providers to keep relevant data. The proposal sets a general retention period of 12 months. However, the draft sets long procedural deadlines in a number of places and, although it is stated that derogations from this general deadline may be made to meet specific needs, it would be preferable to increase this general deadline significantly. We should keep the data until these procedures ends. Deadline mentioned above in this text are much longer in anyway. We suggest to open the possibility for 5 years in this proposal.

Chapter III

Our view is that the coordinating authority's remit should be reviewed. Hungary can cover these competences, but not in one organisation. It would also be unwise to codify such a complex organisation at the level of EU regulation, as this approach would generate conflicts of competence and duplication. The tasks of the authorities and the police are mixed up and do not build on each other in a logical way. We want to build on our existing capacities, with appropriate coordination.

Article 26-30 of the draft expects an independent authority as coordinating authority, on the initiative of which another independent authority will have to take a decision, which seems to be an unnecessary duplication. The competences of the coordinating authority include investigative, analytical and evaluative elements. This cannot be done by an independent administrative authority, and the police service should not be burdened with unnecessary coordination and administrative tasks. The possibility of designating other supporting competent authorities is only mentioned in the draft, and then there are no further references to them, so it is not possible to define their role. The system of complex cooperation at national level should not be interfered with in such a deep way, it is proposed to follow the methodology of the TCO.

In Article 35, the level of fines imposed does not converge with existing EU legislation, we see no clear justification for this. We don't understand why this number was chosen; for the TCO it is 4%, the GDPR also. Is this an area that requires more severe sanctions?

The title of Articles 31 and 38 should be modified, their substantive consequences should be clarified, and the draft should not touch on criminal procedure issues. These monitoring activities in Article 31 are normally channelled also to the law enforcement task. Article 38 cannot be defined as investigation from criminal procedure point of view.

Article 36 par 1 rules that where the Commission has reasons to suspect that a provider of relevant information society services infringed this Regulation in a manner involving at least three Member States, it may recommend that the Coordinating Authority of establishment assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation. We would like to know what is the legal basis and information that allows the COM to come to such a conclusion, and where is the background to this in this draft.

Chapter IV

Article 42 designates The Hague in the Netherlands as the seat of the EU Centre. This was objected by several member states. This solution seems logical in terms of efficient use of capacity and the need for close cooperation with Europol, but it should still be a decision for Member States. We support liaison via liaison officers. We believe that more detailed rules are needed for the relationship with Europol.

Chapter V

Regarding the data collection and transparency reporting more detailed analysis is needed, as it seems to be a bit too detailed. Not just statistics, but detailed activity reports from Member States is required. For coordinating authorities, this detailed data provision will be a significant burden.

As mentioned already at the general remarks, Article 83(2)(a), second indent foresees the collection of data on the basis of "gender", which we do not accept. According to the horizontal Hungarian position, we reject the concept of gender, and for us the collection of data based on "sex" is appropriate. Therefore, Article 83(2)(a), the collection of data based on "gender" should be replaced by the word "sex". For the Hungarian side, we reject the concept of gender as such, in our view there is only sex. Furthermore, in reality, the authorities collect data only on the basis of sex, so the mandate cannot be fulfilled in this way.

We try to be as constructive as possible during the negotiations and we will provide our more detailed position within the framework of the discussions within the LEWP.

of the detection orders issued in accordance with Section 2 of Chapter 2¹ of this Regulation.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

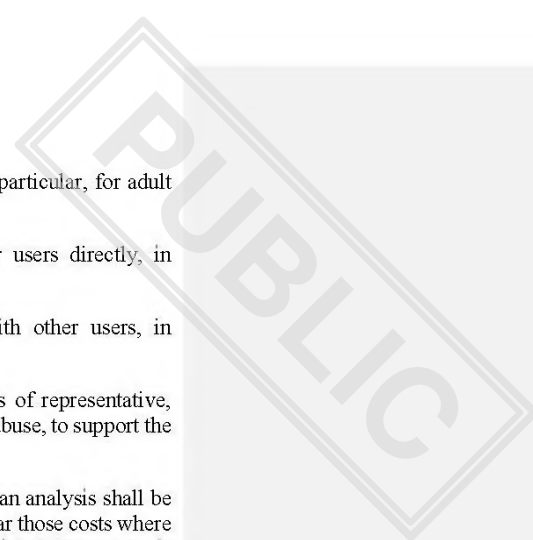
- (a) ‘hosting service’ means an information society service as defined in Article 2, point (f), third indent, of Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC];
- (b) ‘interpersonal communications service’ means a publicly available service as defined in Article 2, point 5, of Directive (EU) 2018/1972, including services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service;
- (c) ‘software application’ means a digital product or service as defined in Article 2, point 13, of Regulation (EU) .../... [on contestable and fair markets in the digital sector (Digital Markets Act)];
- (d) ‘software application store’ means a service as defined in Article 2, point 12, of Regulation (EU) .../... [on contestable and fair markets in the digital sector (Digital Markets Act)];
- (e) ‘internet access service’ means a service as defined in Article 2(2), point 2, of Regulation (EU) 2015/2120 of the European Parliament and of the Council¹;
- (f) ‘relevant information society services’ means all of the following services:
 - (i) a hosting service;
 - (ii) an interpersonal communications service;
 - (iii) a software applications store;
 - (iv) an internet access service.
- (g) ‘to offer services in the Union’ means to offer services in the Union as defined in Article 2, point (d), of Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC];
- (h) ‘user’ means any natural or legal person who uses a relevant information society service;

¹ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

- (i) ‘child’ means any natural person below the age of 18 years;
- (j) ‘child user’ means a natural person who uses a relevant information society service and who is a natural person below the age of 18~~2~~ years;
- (k) ‘micro, small or medium-sized enterprise’ means an enterprise as defined in Commission Recommendation 2003/361 concerning the definition of micro, small and medium-sized enterprises²;
- (l) ‘child sexual abuse material’ means material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU;
- (m) ‘known child sexual abuse material’ means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (a);
- (n) ‘new child sexual abuse material’ means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (b);
- (o) ‘solicitation of children’ means the solicitation of children for sexual purposes as referred to in Article 6 of Directive 2011/93/EU;
- (p) ‘online child sexual abuse’ means the online dissemination of child sexual abuse material and the solicitation of children;
- (q) ‘child sexual abuse offences’ means offences as defined in Articles 3 to 7 of Directive 2011/93/EU;
- (r) ‘recommender system’ means the system as defined in Article 2, point (o), of Regulation (EU) .../... *[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*;
- (s) ‘content data’ means data as defined in Article 2, point 10, of Regulation (EU) ... [on European Production and Preservation Orders for electronic evidence in criminal matters (.../... e-evidence Regulation)];
- (t) ‘content moderation’ means the activities as defined in Article 2, point (p), of Regulation (EU) .../... *[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*;
- (u) ‘Coordinating Authority of establishment’ means the Coordinating Authority for child sexual abuse issues designated in accordance with Article 25 by the Member State where the provider of information society services has its main establishment or, where applicable, where its legal representative resides or is established;

Commented [HU1]: We suggest to change it in coherence with the previous definition, or refer to the different interpretation within the MSS.

² Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36–41).



- enabling users to search for other users and, in particular, for adult users to search for child users;
- enabling users to establish contact with other users directly, in particular through private communications;
- enabling users to share images or videos with other users, in particular through private communications.

3. The provider may request the EU Centre to perform an analysis of representative, anonymized data samples to identify potential online child sexual abuse, to support the risk assessment.

The costs incurred by the EU Centre for the performance of such an analysis shall be borne by the requesting provider. However, the EU Centre shall bear those costs where the provider is a micro, small or medium-sized enterprise, provided the request is reasonably necessary to support the risk assessment.

The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to supplement this Regulation with the necessary detailed rules on the determination and charging of those costs and the application of the exemption for micro, small and medium-sized enterprises.

4. The provider shall carry out the first risk assessment by *[Date of application of this Regulation + 3 months]* or, where the provider did not offer the service in the Union by *[Date of application of this Regulation]*, by three months from the date at which the provider started offering the service in the Union.

Subsequently, the provider shall update the risk assessment where necessary and at least once every three years from the date at which it last carried out or updated the risk assessment. However:

- (a) for a service which is subject to a detection order issued in accordance with Article 7, the provider shall update the risk assessment at the latest two months before the expiry of the period of application of the detection order;
- (b) the Coordinating Authority of establishment may require the provider to update the risk assessment at a reasonable earlier date than the date referred to in the second subparagraph, where there is evidence indicating a possible substantial change in the risk that the service is used for the purpose of online child sexual abuse.

5. The risk assessment shall include an assessment of any potential remaining risk that, after taking the mitigation measures pursuant to Article 4, the service is used for the purpose of online child sexual abuse.

6. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1 to 5, having due regard in particular to relevant technological developments and to the manners in which the services covered by those provisions are offered and used.

Commented [HU2]: This timeframe looks a bit too long
this assessment should be a living exercise

- (a) make reasonable efforts to assess, where possible together with the providers of software applications, whether each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children;
- (b) take reasonable measures to prevent child users from accessing the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children;
- (c) take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b).
2. In assessing the risk referred to in paragraph 1, the provider shall take into account all the available information, including the results of the risk assessment conducted or updated pursuant to Article 3.
3. Providers of software application stores shall make publicly available information describing the process and criteria used to assess the risk and describing the measures referred to in paragraph 1. That description shall not include information that may reduce the effectiveness of the assessment of those measures.
4. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1, 2 and 3, having due regard in particular to relevant technological developments and to the manners in which the services covered by those provisions are offered and used.

Section 2 Detection obligations

Article 7

Issuance of detection orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect online child sexual abuse on a specific service.
2. The Coordinating Authority of establishment shall, before requesting the issuance of a detection order, carry out the investigations and assessments necessary to determine whether the conditions of paragraph 4 have been met.

To that end, it may, where appropriate, require the provider to submit the necessary information, additional to the report and the further information referred to in Article 5(1) and (3), respectively, within a reasonable time period set by that Coordinating Authority, or request the EU Centre, another public authority or relevant experts or entities to provide the necessary additional information.

Commented [HU3]: The proposed regulation seems to have a complex implementation structure, with no clear or well-defined competences, despite the fact that the proposal builds on the solutions used in the DSA and TCO Regulations. In the TCO Regulation the coordinating authority and the judicial or independent administrative authority are one and the same, but in the CSA Regulation they are separate authorities. A simpler solution would be for the competent authority to be able to issue blocking or removal orders itself, rather than having to apply to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplication should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

4. The Coordinating Authority of establishment shall request the issuance of the detection order, and the competent judicial authority or independent administrative authority shall issue the detection order where it considers that the following conditions are met:

Commented [HU4]: better wording is needed, it is understood that the independent authority does not have any discretionary power in deciding whether or not to issue

- (a) there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5, 6 and 7, as applicable;
- (b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties.

When assessing whether the conditions of the first subparagraph have been met, account shall be taken of all relevant facts and circumstances of the case at hand, in particular:

- (a) the risk assessment conducted or updated and any mitigation measures taken by the provider pursuant to Articles 3 and 4, including any mitigation measures introduced, reviewed, discontinued or expanded pursuant to Article 5(4) where applicable;
- (b) any additional information obtained pursuant to paragraph 2 or any other relevant information available to it, in particular regarding the use, design and operation of the service, regarding the provider's financial and technological capabilities and size and regarding the potential consequences of the measures to be taken to execute the detection order for all other parties affected;
- (c) the views and the implementation plan of the provider submitted in accordance with paragraph 3;
- (d) the opinions of the EU Centre and of the data protection authority submitted in accordance with paragraph 3.

As regards the second subparagraph, point (d), where that Coordinating Authority substantially deviates from the opinion of the EU Centre, it shall inform the EU Centre and the Commission thereof, specifying the points at which it deviated and the main reasons for the deviation.

5. As regards detection orders concerning the dissemination of known child sexual abuse material, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met:

- (a) it is likely, despite any mitigation measures that the provider may have taken or will take, that the service is used, to an appreciable extent for the dissemination of known child sexual abuse material;
- (b) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent for the dissemination of known child sexual abuse material.

- (e) whether the detection order issued concerns the dissemination of known or new child sexual abuse material or the solicitation of children;
- (f) the start date and the end date of the detection order;
- (g) a sufficiently detailed statement of reasons explaining why the detection order is issued;
- (h) a reference to this Regulation as the legal basis for the detection order;
- (i) the date, time stamp and electronic signature of the judicial or independent administrative authority issuing the detection order;
- (j) easily understandable information about the redress available to the addressee of the detection order, including information about redress to a court and about the time periods applicable to such redress.
2. The competent judicial authority or independent administrative authority issuing the detection order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.
- The detection order shall be transmitted to the provider's point of contact referred to in Article 23(1), to the Coordinating Authority of establishment and to the EU Centre, through the system established in accordance with Article 39(2).
- The detection order shall be drafted in the language declared by the provider pursuant to Article 23(3).
3. If the provider cannot execute the detection order because it contains manifest errors or does not contain sufficient information for its execution, the provider shall, without undue delay, request the necessary clarification to the Coordinating Authority of establishment, using the template set out in Annex II.
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annexes I and II where necessary to improve the templates in view of relevant technological developments or practical experiences gained.

Article 9

Redress, information, reporting and modification of detection orders

1. Providers of hosting services and providers of interpersonal communications services that have received a detection order, as well as users affected by the measures taken to execute it, shall have a right to effective redress. That right shall include the right to challenge the detection order before the courts of the Member State of the competent judicial authority or independent administrative authority that issued the detection order.
2. When the detection order becomes final, the competent judicial authority or independent administrative authority that issued the detection order shall, without undue delay, transmit a copy thereof to the Coordinating Authority of establishment.

Commented [HU5]: We require here a ruling on the official language of the Coordinating Authority+English

Section 3

Reporting obligations

Article 12

Reporting obligations

1. Where a provider of hosting services or a provider of interpersonal communications services becomes aware in any manner other than through a removal order issued in accordance with this Regulation of any information indicating potential online child sexual abuse on its services, it shall promptly submit a report thereon to the EU Centre in accordance with Article 13. It shall do so through the system established in accordance with Article 39(2).
2. Where the provider submits a report pursuant to paragraph 1, it shall inform the user concerned, providing information on the main content of the report, on the manner in which the provider has become aware of the potential child sexual abuse concerned, on the follow-up given to the report insofar as such information is available to the provider and on the user's possibilities of redress, including on the right to submit complaints to the Coordinating Authority in accordance with Article 34.

The provider shall inform the user concerned without undue delay, either after having received a communication from the EU Centre indicating that it considers the report to be manifestly unfounded as referred to in Article 48(2), or after the expiry of a time period of three months from the date of the report without having received a communication from the EU Centre indicating that the information is not to be provided as referred to in Article 48(6), point (a), whichever occurs first.

Where within the three months' time period referred to in the second subparagraph the provider receives such a communication from the EU Centre indicating that the information is not to be provided, it shall inform the user concerned, without undue delay, after the expiry of the time period set out in that communication.

3. The provider shall establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to flag to the provider potential online child sexual abuse on the service.

Article 13

Specific requirements for reporting

1. Providers of hosting services and providers of interpersonal communications services shall submit the report referred to in Article 12 using the template set out in Annex III. The report shall include:
 - (a) identification details of the provider and, where applicable, its legal representative;
 - (b) the date, time stamp and electronic signature of the provider;
 - (c) all content data, including images, videos and text;

Commented [HU6]: immediate compliance with the obligation to provide information may cause problems for law enforcement action, which should preferably be suspended pending the reaction of EU Centre

- (d) all available data other than content data related to the potential online child sexual abuse;
 - (e) whether the potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material or the solicitation of children;
 - (f) information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address;
 - (g) information concerning the identity of any user involved in the potential online child sexual abuse;
 - (h) whether the provider has also reported, or will also report, the potential online child sexual abuse to a public authority or other entity competent to receive such reports of a third country and if so, which authority or entity;
 - (i) where the potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material, whether the provider has removed or disabled access to the material;
 - (j) whether the provider considers that the report requires urgent action;
 - (k) a reference to this Regulation as the legal basis for reporting.
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annex III to improve the template where necessary in view of relevant technological developments or practical experiences gained.


Section 4 **Removal obligations**

Article 14

Removal orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a removal order requiring a provider of hosting services under the jurisdiction of the Member State that designated that Coordinating Authority to remove or disable access in all Member States of one or more specific items of material that, after a diligent assessment, the Coordinating Authority or the courts or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material.
2. The provider shall execute the removal order as soon as possible and in any event within 24 hours of receipt thereof.
3. The competent judicial authority or the independent administrative authority shall issue a removal order using the template set out in Annex IV. Removal orders shall include:

Commented [HU7]: The proposed regulation seems to have a complex implementation structure, with no clear or well-defined competences, despite the fact that the proposal builds on the solutions used in the DSA and TCO Regulations. In the TCO Regulation the coordinating authority and the judicial or independent administrative authority are one and the same, but in the CSA Regulation they are separate authorities. A simpler solution would be for the competent authority to be able to issue blocking or removal orders itself, rather than having to apply to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplication should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

- 
- (a) identification details of the judicial or independent administrative authority issuing the removal order and authentication of the removal order by that authority;
 - (b) the name of the provider and, where applicable, of its legal representative;
 - (c) the specific service for which the removal order is issued;
 - (d) a sufficiently detailed statement of reasons explaining why the removal order is issued and in particular why the material constitutes child sexual abuse material;
 - (e) an exact uniform resource locator and, where necessary, additional information for the identification of the child sexual abuse material;
 - (f) where applicable, the information about non-disclosure during a specified time period, in accordance with Article 15(4), point (c);
 - (g) a reference to this Regulation as the legal basis for the removal order;
 - (h) the date, time stamp and electronic signature of the judicial or independent administrative authority issuing the removal order;
 - (i) easily understandable information about the redress available to the addressee of the removal order, including information about redress to a court and about the time periods applicable to such redress.

4. The judicial authority or the independent administrative issuing the removal order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

It shall transmit the removal order to the point of contact referred to in Article 23(1) by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order, to the Coordinating Authority of establishment and to the EU Centre, through the system established in accordance with Article 39(2).

It shall draft the removal order in the language declared by the provider pursuant to Article 23(3).

Commented [HU8]: It should be the language of the coordinating authority+English

5. If the provider cannot execute the removal order on grounds of force majeure or de facto impossibility not attributable to it, including for objectively justifiable technical or operational reasons, it shall, without undue delay, inform the Coordinating Authority of establishment of those grounds, using the template set out in Annex V.

The time period set out in paragraph 1 shall start to run as soon as the reasons referred to in the first subparagraph have ceased to exist.

6. If the provider cannot execute the removal order because it contains manifest errors or does not contain sufficient information for its execution, it shall, without undue delay, request the necessary clarification to the Coordinating Authority of establishment, using the template set out in Annex V.

activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

In such a case:

- (a) the judicial authority or independent administrative authority issuing the removal order shall set the time period not longer than necessary and not exceeding six weeks, during which the provider is not to disclose such information;
- (b) the obligations set out in paragraph 3 shall not apply during that time period;
- (c) that judicial authority or independent administrative authority shall inform the provider of its decision, specifying the applicable time period.

That judicial authority or independent administrative authority may decide to extend the time period referred to in the second subparagraph, point (a), by a further time period of maximum six weeks, where and to the extent the non-disclosure continues to be necessary. In that case, that judicial authority or independent administrative authority shall inform the provider of its decision, specifying the applicable time period. Article 14(3) shall apply to that decision.

Section 5 **Blocking obligations**

Article 16

Blocking orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing known child sexual abuse material indicated by all uniform resource locators on the list of uniform resource locators included in the database of indicators, in accordance with Article 44(2), point (b) and provided by the EU Centre.
2. The Coordinating Authority of establishment shall, before requesting the issuance of a blocking order, carry out all investigations and assessments necessary to determine whether the conditions of paragraph 4 have been met.

To that end, it shall, where appropriate:

- (a) verify that, in respect of all or a representative sample of the uniform resource locators on the list referred to in paragraph 1, the conditions of Article 36(1), point (b), are met, including by carrying out checks to verify in cooperation with the EU Centre that the list is complete, accurate and up-to-date;
- (b) require the provider to submit, within a reasonable time period set by that Coordinating Authority, the necessary information, in particular regarding the accessing or attempting to access by users of the child sexual abuse material

Commented [HU9]: The proposed regulation seems to have a complex implementation structure, with no clear or well-defined competences, despite the fact that the proposal builds on the solutions used in the DSA and TCO Regulations. In the TCO Regulation the coordinating authority and the judicial or independent administrative authority are one and the same, but in the CSA Regulation they are separate authorities. A simpler solution would be for the competent authority to be able to issue blocking or removal orders itself, rather than having to apply to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplication should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

Article 20

Victims' right to information

1. Persons residing in the Union shall have the right to receive, upon their request, from the Coordinating Authority designated by the Member State where they reside, information regarding any instances where the dissemination of known child sexual abuse material depicting them is reported to the EU Centre pursuant to Article 12. Persons with disabilities shall have the right to ask and receive such an information in a manner accessible to them.

That Coordinating Authority shall transmit the request to the EU Centre through the system established in accordance with Article 39(2) and shall communicate the results received from the EU Centre to the person making the request.

2. The request referred to in paragraph 1 shall indicate:
 - (a) the relevant item or items of known child sexual abuse material;
 - (b) where applicable, the individual or entity that is to receive the information on behalf of the person making the request;
 - (c) sufficient elements to demonstrate the identity of the person making the request.
3. The information referred to in paragraph 1 shall include:
 - (a) the identification of the provider that submitted the report;
 - (b) the date of the report;
 - (c) whether the EU Centre forwarded the report in accordance with Article 48(3) and, if so, to which authorities;
 - (d) whether the provider reported having removed or disabled access to the material, in accordance with Article 13(1), point (i).

Commented [HU10]: We are talking about children victims here, thus we need a very detailed explanation here on requirements and obstacles. The proposed legislation does not cover rules on representation and protection against criminal parents as legal representatives.

Article 21

Victims' right of assistance and support for removal

1. Providers of hosting services shall provide reasonable assistance, on request, to persons residing in the Union that seek to have one or more specific items of known child sexual abuse material depicting them removed or to have access thereto disabled by the provider.
2. Persons residing in the Union shall have the right to receive, upon their request, from the Coordinating Authority designated by the Member State where the person resides, support from the EU Centre when they seek to have a provider of hosting services remove or disable access to one or more specific items of known child sexual abuse material depicting them. Persons with disabilities shall have the right to ask and receive any information relating to such support in a manner accessible to them.

Commented [HU11]: In accordance with this we should refer on the applicable EU legislation concerning victim protection and support, and we should channel these activities into the existing mechanisms in this field.

As regards the first subparagraph, point (a), the provider may also preserve the information for the purpose of improving the effectiveness and accuracy of the technologies to detect online child sexual abuse for the execution of a detection order issued to it in accordance with Article 7. However, it shall not store any personal data for that purpose.

2. Providers shall preserve the information referred to in paragraph 1 for no longer than necessary for the applicable purpose and, in any event, no longer than 12 months from the date of the reporting or of the removal or disabling of access, whichever occurs first.

They shall, upon request from the competent national authority or court, preserve the information for a further specified period, set by that authority or court where and to the extent necessary for ongoing administrative or judicial redress proceedings, as referred to in paragraph 1, point (d).

Providers shall ensure that the information referred to in paragraph 1 is preserved in a secure manner and that the preservation is subject to appropriate technical and organisational safeguards. Those safeguards shall ensure, in particular, that the information can be accessed and processed only for the purpose for which it is preserved, that a high level of security is achieved and that the information is deleted upon the expiry of the applicable time periods for preservation. Providers shall regularly review those safeguards and adjust them where necessary.

Article 23

Points of contact

1. Providers of relevant information society services shall establish a single point of contact allowing for direct communication, by electronic means, with the Coordinating Authorities, other competent authorities of the Member States, the Commission and the EU Centre, for the application of this Regulation.
2. The providers shall communicate to the EU Centre and make public the information necessary to easily identify and communicate with their single points of contact, including their names, addresses, the electronic mail addresses and telephone numbers.
3. The providers shall specify in the information referred to in paragraph 2 the official language or languages of the Union, which can be used to communicate with their points of contact.

The specified languages shall include at least one of the official languages of the Member State in which the provider has its main establishment or, where applicable, where its legal representative resides or is established.

Article 24

Legal representative

1. Providers of relevant information society services which do not have their main establishment in the Union shall designate, in writing, a natural or legal person as its legal representative in the Union.

Commented [HU12]: We should keep the data until these procedures ends. deadline mentioned above in this text are much longer. In anyway we suggest to open the possibility for 5 years in this proposal.

CHAPTER III

SUPERVISION, ENFORCEMENT AND COOPERATION

Section 1

Coordinating Authorities for child sexual abuse issues

Article 25

Coordinating Authorities for child sexual abuse issues and other competent authorities

1. Member States shall, by [Date - two months from the date of entry into force of this Regulation], designate one or more competent authorities as responsible for the application and enforcement of this Regulation ('competent authorities').
2. Member States shall, by the date referred to in paragraph 1, designate one of the competent authorities as their Coordinating Authority for child sexual abuse issues ('Coordinating Authority').

The Coordinating Authority shall be responsible for all matters related to application and enforcement of this Regulation in the Member State concerned, unless that Member State has assigned certain specific tasks or sectors to other competent authorities.

The Coordinating Authority shall in any event be responsible for ensuring coordination at national level in respect of those matters and for contributing to the effective, efficient and consistent application and enforcement of this Regulation throughout the Union.

3. Where a Member State designates more than one competent authority in addition to the Coordinating Authority, it shall ensure that the respective tasks of those authorities and of the Coordinating Authority are clearly defined and that they cooperate closely and effectively when performing their tasks. The Member State concerned shall communicate the name of the other competent authorities as well as their respective tasks to the EU Centre and the Commission.
4. Within one week after the designation of the Coordinating Authorities and any other competent authorities pursuant to paragraph 1, Member States shall make publicly available, and communicate to the Commission and the EU Centre, the name of their Coordinating Authority. They shall keep that information updated.
5. Each Member State shall ensure that a contact point is designated or established within the Coordinating Authority's office to handle requests for clarification, feedback and other communications in relation to all matters related to the application and enforcement of this Regulation in that Member State. Member States shall make the information on the contact point publicly available and communicate it to the EU Centre. They shall keep that information updated.
6. Within two weeks after the designation of the Coordinating Authorities pursuant to paragraph 2, the EU Centre shall set up an online register listing the Coordinating

Commented [HU13]: Our view is that the coordinating authority's remit should be reviewed. Hungary can cover these competences, but it would not be advisable to codify such a complex organisation into one organisation, nor at the level of EU regulation, as this approach would create conflicts of competence and duplication. The tasks of the judicial, administrative authorities and the police are mixed up and do not build on each other in a logical way, and we would like to build on our existing capacities, with proper coordination.

- Authorities and their contact points. The EU Centre shall regularly publish any modification thereto.
7. Coordinating Authorities may, where necessary for the performance of their tasks under this Regulation, request the assistance of the EU Centre in carrying out those tasks, in particular by requesting the EU Centre to:
 - (a) provide certain information or technical expertise on matters covered by this Regulation;
 - (b) assist in assessing, in accordance with Article 5(2), the risk assessment conducted or updated or the mitigation measures taken by a provider of hosting or interpersonal communication services under the jurisdiction of the Member State that designated the requesting Coordinating Authority;
 - (c) verify the possible need to request competent national authorities to issue a detection order, a removal order or a blocking order in respect of a service under the jurisdiction of the Member State that designated that Coordinating Authority;
 - (d) verify the effectiveness of a detection order or a removal order issued upon the request of the requesting Coordinating Authority.
 8. The EU Centre shall provide such assistance free of charge and in accordance with its tasks and obligations under this Regulation and insofar as its resources and priorities allow.
 9. The requirements applicable to Coordinating Authorities set out in Articles 26, 27, 28, 29 and 30 shall also apply to any other competent authorities that the Member States designate pursuant to paragraph 1.

Article 26

Requirements for Coordinating Authorities

1. Member States shall ensure that the Coordinating Authorities that they designated perform their tasks under this Regulation in an objective, impartial, transparent and timely manner, while fully respecting the fundamental rights of all parties affected. Member States shall ensure that their Coordinating Authorities have adequate technical, financial and human resources to carry out their tasks.
2. When carrying out their tasks and exercising their powers in accordance with this Regulation, the Coordinating Authorities shall act with complete independence. To that aim, Member States shall ensure, in particular, that they:
 - (a) are legally and functionally independent from any other public authority;
 - (b) have a status enabling them to act objectively and impartially when carrying out their tasks under this Regulation;
 - (c) are free from any external influence, whether direct or indirect;

Commented [HU14]: Article 26-30 of the draft expects an independent authority as coordinating authority, on the initiative of which another independent authority will have to take a decision, which seems to be an unnecessary duplication. The competences of the coordinating authority include investigative, analytical and evaluative elements, which an independent administrative authority cannot perform, and the police service should not be burdened with unnecessary coordination and administrative tasks. The possibility of designating other supporting competent authorities is only mentioned in the draft, and then there are no further references to them, so it is not possible to define their role. The system of complex cooperation at national level should not be interfered with in such a deep way, it is proposed to follow the methodology of the TCO.

without unduly restricting access to lawful information by users of the service concerned.

The temporary restriction shall apply for a period of four weeks, subject to the possibility for the competent judicial authority, in its order, to allow the Coordinating Authority to extend that period for further periods of the same lengths, subject to a maximum number of extensions set by that judicial authority.

The Coordinating Authority shall only extend the period where it considers, having regard to the rights and legitimate interests of all parties affected by the restriction and all relevant facts and circumstances, including any information that the provider, the addressee or addressees and any other third party that demonstrated a legitimate interest may provide to it, that both of the following conditions have been met:

- (a) the provider has failed to take the necessary measures to terminate the infringement;
- (b) the temporary restriction does not unduly restrict access to lawful information by users of the service, having regard to the number of users affected and whether any adequate and readily accessible alternatives exist.

Where the Coordinating Authority considers that those two conditions have been met but it cannot further extend the period pursuant to the second subparagraph, it shall submit a new request to the competent judicial authority, as referred to in paragraph 2, point (b).

Article 30

Common provisions on investigatory and enforcement powers

1. The measures taken by the Coordinating Authorities in the exercise of their investigatory and enforcement powers referred to in Articles 27, 28 and 29 shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement of this Regulation or suspected infringement to which those measures relate, as well as the economic, technical and operational capacity of the provider of relevant information society services concerned, where applicable.
2. Member States shall ensure that any exercise of the investigatory and enforcement powers referred to in Articles 27, 28 and 29 is subject to adequate safeguards laid down in the applicable national law to respect the fundamental rights of all parties affected. In particular, those measures shall only be taken in accordance with the right to respect for private life and the rights of defence, including the rights to be heard and of access to the file, and subject to the right to an effective judicial remedy of all parties affected.

Article 31

Searches to verify compliance

Coordinating Authorities shall have the power to carry out searches on publicly accessible material on hosting services to detect the dissemination of known or new child sexual abuse material, using the indicators contained in the databases referred to in Article 44(1), points (a)

and (b)), where necessary to verify whether the providers of hosting services under the jurisdiction of the Member State that designated the Coordinating Authorities comply with their obligations under this Regulation.

Commented [HU15]: This monitoring activities are normally channelled also to the LAE task.

Article 32

Notification of known child sexual abuse material

Coordinating Authorities shall have the power to notify providers of hosting services under the jurisdiction of the Member State that designated them of the presence on their service of one or more specific items of known child sexual abuse material and to request them to remove or disable access to that item or those items, for the providers' voluntary consideration.

The request shall clearly set out the identification details of the Coordinating Authority making the request and information on its contact point referred to in Article 25(5), the necessary information for the identification of the item or items of known child sexual abuse material concerned, as well as the reasons for the request. The request shall also clearly state that it is for the provider's voluntary consideration.

Section 3

Other provisions on enforcement

Article 33

Jurisdiction

1. The Member State in which the main establishment of the provider of relevant information society services is located shall have jurisdiction for the purposes of this Regulation.
2. A provider of relevant information society services which does not have an establishment in the Union shall be deemed to be under the jurisdiction of the Member State where its legal representative resides or is established.

Where a provider failed to appoint a legal representative in accordance with Article 24, all Member States shall have jurisdiction. Where a Member State decides to exercise jurisdiction under this subparagraph, it shall inform all other Member States and ensure that the principle of *ne bis in idem* is respected.

Article 34

Right of users of the service to lodge a complaint

1. Users shall have the right to lodge a complaint alleging an infringement of this Regulation affecting them against providers of relevant information society services with the Coordinating Authority designated by the Member State where the user resides or is established.
2. Coordinating Authorities shall provide child-friendly mechanisms to submit a complaint under this Article and adopt a child-sensitive approach when handling

complaints submitted by children, taking due account of the child's age, maturity, views, needs and concerns.

3. The Coordinating Authority receiving the complaint shall assess the complaint and, where appropriate, transmit it to the Coordinating Authority of establishment.

Where the complaint falls under the responsibility of another competent authority of the Member State that designated the Coordinating Authority receiving the complaint, that Coordinating Authority shall transmit it to that other competent authority.

Article 35

Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of the obligations pursuant to Chapters II and V of this Regulation by providers of relevant information society services under their jurisdiction and shall take all the necessary measures to ensure that they are implemented.

The penalties shall be effective, proportionate and dissuasive. Member States shall, by [Date of application of this Regulation], notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendments affecting them.

2. Member States shall ensure that the maximum amount of penalties imposed for an infringement of this Regulation shall not exceed 6 % of the annual income or global turnover of the preceding business year of the provider.
3. Penalties for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information or to submit to an on-site inspection shall not exceed 1% of the annual income or global turnover of the preceding business year of the provider or the other person referred to in Article 27.
4. Member States shall ensure that the maximum amount of a periodic penalty payment shall not exceed 5 % of the average daily global turnover of the provider or the other person referred to in Article 27 in the preceding financial year per day, calculated from the date specified in the decision concerned.
5. Member States shall ensure that, when deciding whether to impose a penalty and when determining the type and level of penalty, account is taken of all relevant circumstances, including:
 - (a) the nature, gravity and duration of the infringement;
 - (b) whether the infringement was intentional or negligent;
 - (c) any previous infringements by the provider or the other person;
 - (d) the financial strength of the provider or the other person;
 - (e) the level of cooperation of the provider or the other person;

Commented [HU16]: we can live with this regulation, we just don't understand why this number was chosen; for the TCO 4%, the GDPR also, this is an area that requires more severe sanctions?

or conversation is identified as constituting child sexual abuse material or as the solicitation of children, the Coordinating Authority submits the material to the EU Centre, in accordance with that paragraph, within one month from the date of reception of the report or, where the assessment is particularly complex, two months from that date.

4. They shall also ensure that, where the diligent assessment indicates that the material does not constitute child sexual abuse material or the solicitation of children, the Coordinating Authority is informed of that outcome and subsequently informs the EU Centre thereof, within the time periods specified in the first subparagraph.

Article 37

Cross-border cooperation among Coordinating Authorities

1. Where a Coordinating Authority that is not the Coordinating Authority of establishment has reasons to suspect that a provider of relevant information society services infringed this Regulation, it shall request the Coordinating Authority of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

Where the Commission has reasons to suspect that a provider of relevant information society services infringed this Regulation in a manner involving at least three Member States, it may recommend that the Coordinating Authority of establishment assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

Commented [HU17]: What is the legal basis and information that allows the COM to come to such a conclusion, and where is the background to this in this draft?

2. The request or recommendation referred to in paragraph 1 shall at least indicate:
 - (a) the point of contact of the provider as set out in Article 23;
 - (b) a description of the relevant facts, the provisions of this Regulation concerned and the reasons why the Coordinating Authority that sent the request, or the Commission suspects, that the provider infringed this Regulation;
 - (c) any other information that the Coordinating Authority that sent the request, or the Commission, considers relevant, including, where appropriate, information gathered on its own initiative and suggestions for specific investigatory or enforcement measures to be taken.
3. The Coordinating Authority of establishment shall assess the suspected infringement, taking into utmost account the request or recommendation referred to in paragraph 1.

Where it considers that it has insufficient information to assess the suspected infringement or to act upon the request or recommendation and has reasons to consider that the Coordinating Authority that sent the request, or the Commission, could provide additional information, it may request such information. The time period laid down in paragraph 4 shall be suspended until that additional information is provided.
4. The Coordinating Authority of establishment shall, without undue delay and in any event not later than two months following receipt of the request or recommendation referred to in paragraph 1, communicate to the Coordinating Authority that sent the

request, or the Commission, the outcome of its assessment of the suspected infringement, or that of any other competent authority pursuant to national law where relevant, and, where applicable, an explanation of the investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation.

Article 38

Joint investigations

Coordinating Authorities may participate in joint investigations, which may be coordinated with the support of the EU Centre, of matters covered by this Regulation, concerning providers of relevant information society services that offer their services in several Member States.

Such joint investigations are without prejudice to the tasks and powers of the participating Coordinating Authorities and the requirements applicable to the performance of those tasks and exercise of those powers provided for in this Regulation.

2. The participating Coordinating Authorities shall make the results of the joint investigations available to other Coordinating Authorities, the Commission and the EU Centre, through the system established in accordance with Article 39(2), for the fulfilment of their respective tasks under this Regulation.

Article 39

General cooperation and information-sharing system

1. Coordinating Authorities shall cooperate with each other, any other competent authorities of the Member State that designated the Coordinating Authority, the Commission, the EU Centre and other relevant Union agencies, including Europol, to facilitate the performance of their respective tasks under this Regulation and ensure its effective, efficient and consistent application and enforcement.
2. The EU Centre shall establish and maintain one or more reliable and secure information sharing systems supporting communications between Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services.
3. The Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services shall use the information-sharing systems referred to in paragraph 2 for all relevant communications pursuant to this Regulation.
4. The Commission shall adopt implementing acts laying down the practical and operational arrangements for the functioning of the information-sharing systems referred to in paragraph 2 and their interoperability with other relevant systems. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 87.

Commented [HU18]: this cannot be defined as investigation from CP point of view.

CHAPTER IV

EU CENTRE TO PREVENT AND COMBAT CHILD SEXUAL ABUSE

Section 1

Principles

Article 40

Establishment and scope of action of the EU Centre

1. A European Union Agency to prevent and combat child sexual abuse, the EU Centre on Child Sexual Abuse, is established.
2. The EU Centre shall contribute to the achievement of the objective of this Regulation by supporting and facilitating the implementation of its provisions concerning the detection, reporting, removal or disabling of access to, and blocking of online child sexual abuse and gather and share information and expertise and facilitate cooperation between relevant public and private parties in connection to the prevention and combating of child sexual abuse, in particular online.

Article 41

Legal status

1. The EU Centre shall be a body of the Union with legal personality.
2. In each of the Member States the EU Centre shall enjoy the most extensive legal capacity accorded to legal persons under their laws. It may, in particular, acquire and dispose of movable and immovable property and be party to legal proceedings.
3. The EU Centre shall be represented by its Executive Director.

Article 42

Seat

The seat of the EU Centre shall be The Hague, The Netherlands.

Section 2

Tasks

Article 43

Tasks of the EU Centre

The EU Centre shall:

Commented [HU19]: This solution seems logical in terms of efficient use of capacity and the need for close cooperation with Europol, but it should still be a decision for Member States.

Article 53

Cooperation with Europol

Commented [H20]: More detailed rules are needed on the relationship with Europol.

1. Where necessary for the performance of its tasks under this Regulation, within their respective mandates, the EU Centre shall cooperate with Europol.
2. Europol and the EU Centre shall provide each other with the fullest possible access to relevant information and information systems, where necessary for the performance of their respective tasks and in accordance with the acts of Union law regulating such access.

Without prejudice to the responsibilities of the Executive Director, the EU Centre shall maximise efficiency by sharing administrative functions with Europol, including functions relating to personnel management, information technology (IT) and budget implementation.

3. The terms of cooperation and working arrangements shall be laid down in a memorandum of understanding.

Article 54

Cooperation with partner organisations

1. Where necessary for the performance of its tasks under this Regulation, the EU Centre may cooperate with organisations and networks with information and expertise on matters related to the prevention and combating of online child sexual abuse, including civil society organisations and semi-public organisations.
2. The EU Centre may conclude memoranda of understanding with organisations referred to in paragraph 1, laying down the terms of cooperation.

Section 5

Organisation

Article 55

Administrative and management structure

The administrative and management structure of the EU Centre shall comprise:

- (a) a Management Board, which shall exercise the functions set out in Article 57;
- (b) an Executive Board which shall perform the tasks set out in Article 62;
- (c) an Executive Director of the EU Centre, who shall exercise the responsibilities set out in Article 64;
- (d) a Technology Committee as an advisory group, which shall exercise the tasks set out in Article 66.

- whether the report led to the launch of a criminal investigation, contributed to an ongoing investigation, led to taking any other action or led to no action;
 - where the report led to the launch of a criminal investigation or contributed to an ongoing investigation, the state of play or outcome of the investigation, including whether the case was closed at pre-trial stage, whether the case led to the imposition of penalties, whether victims were identified and rescued and if so their numbers differentiating by gender and age, and whether any suspects were arrested and any perpetrators were convicted and if so their numbers;
 - where the report led to any other action, the type of action, the state of play or outcome of that action and the reasons for taking it;
 - where no action was taken, the reasons for not taking any action;
- (b) the most important and recurrent risks of online child sexual abuse, as reported by providers of hosting services and providers of interpersonal communications services in accordance with Article 3 or identified through other information available to the Coordinating Authority;
 - (c) a list of the providers of hosting services and providers of interpersonal communications services to which the Coordinating Authority addressed a detection order in accordance with Article 7;
 - (d) the number of detection orders issued in accordance with Article 7, broken down by provider and by type of online child sexual abuse, and the number of instances in which the provider invoked Article 8(3);
 - (e) a list of providers of hosting services to which the Coordinating Authority issued a removal order in accordance with Article 14;
 - (f) the number of removal orders issued in accordance with Article 14, broken down by provider, the time needed to remove or disable access to the item or items of child sexual abuse material concerned, and the number of instances in which the provider invoked Article 14(5) and (6);
 - (g) the number of blocking orders issued in accordance with Article 16, broken down by provider, and the number of instances in which the provider invoked Article 17(5);
 - (h) a list of relevant information society services to which the Coordinating Authority addressed a decision taken pursuant to Articles 27, 28 or 29, the type of decision taken, and the reasons for taking it;
 - (i) the instances in which the opinion of the EU Centre pursuant to Article 7(4)(d) substantially deviated from the opinion of the Coordinating Authority, specifying the points at which it deviated and the main reasons for the deviation.

Commented [TZZ1]: As mentioned already at the general remarks, Article 83(2)(a), second indent foresees the collection of data on the basis of "gender", which we do not accept. According to the horizontal Hungarian position, we reject the concept of gender, and for us the collection of data based on "sex" is appropriate. Therefore, Article 83(2)(a), the collection of data based on "gender" should be replaced by the word "sex". For the Hungarian side, we reject the concept of gender as such, in our view there is only sex. Furthermore, in reality, the authorities collect data only on the basis of sex, so the mandate cannot be fulfilled in this way.

IRELAND

Ireland is strongly in favour of the Regulation as a whole and is keen to ensure that the measures it introduces are both effective and efficient.

Ireland repeats this general comment made at the Working Party, which broadly relates to a number of articles: we have concerns in relation to the range and complexity of the responsibilities placed on the national Coordinating Authorities and we continue to scrutinise all references to national authorities. In order to assist Member States' understanding on this aspect of the proposal, we repeat our suggestion, made in earlier written comments, for flow charts setting out the Commission's understanding of how the national coordinating authorities will interact with each other and other bodies. It might also be helpful if the Commission could enumerate all the tasks it foresees the Coordinating Authorities undertaking.

We have similar concerns around efficiency and complexity in relation to the responsibilities given to the "judicial authority or independent administrative authority". It is our understanding that the Regulation requires that Member States make provision for the role of this second national competent authority in addition to the Coordinating Authority. We note that the Presidency paper accompanying the upcoming discussion at the informal COSI states "Member States may appoint one or more national competent authorities". Does this mean one or more, in addition to the "judicial authority or independent administrative authority"?

In Ireland the Courts are our "judicial authorities" – is it intended that we should go to the Courts for approval for the issuance of every detection, removal or blocking order? Alternatively, if we go down the path of an "independent administrative authority" this raises the question of why we are creating two separate new independent national authorities to deal with the same matters? Although we are very aware of the need for safeguards and accountability, we have reservations with the level of complexity involved.

We also have some comments that were not made at the Working Party. Again, we are supportive of the principles underlying the process laid out in the Regulation whereby detection order follows risk mitigation follows risk assessment, but we are trying to understand the practical implications.

One issue that has been raised with us by a prominent online service provider (and no doubt raised also with the Presidency and Commission) is that the Regulation will stop companies from continuing to use techniques which prevent harm from happening online in the first place. The company claims that the proposal does not provide a legal basis for companies to process communications metadata to tackle child sexual abuse in the absence of receiving a detection order from a member state authority. There are prevention techniques which are currently deployed which would no longer be allowed under these proposals.

Ireland regards prevention as very important and would be concerned that there could be a lengthy period in which the legal basis for voluntary detection was removed but before any DO had been issued. The risk is greater when we consider the possibility that we cannot know how long it will take for the first DOs to be issued, or even be sure that will be issued at all. By this we mean we are creating a process in which Coordinating Authorities, which are required to be completely independent, and independent judicial or administrative authorities, all have to decide that a DO is justified, and any challenges to these decisions must be overcome. So in addition to taking some time, the outcome of the process cannot be certain. Is there any way of introducing the process envisaged by the Regulation but also ensuring that the preventative measures currently being employed, which have been shown to be effective, can continue?

Ireland expects to have further comments to make in relation to Article 7 specifically, and the ways in which national authorities, other bodies and the EU Centre interact in general. We will share these in due course.

From a drafting point of view we would point out the below errors:

- Article 4.2.d has a reference to 3.4 that should read 3.6.
- Art 5.1 chapeau has the same mistake.
- Art 5.1.a refers to 3.5 when it should read 3.7.

ITALY

With regards to the discussion on the 5th July regarding CSA Proposal we would like to recall our previous comments on articles from 1 to 7.

We really appreciated the CION replies and the opportunity granted to share a work flow scheme to better understand the roles, powers and prerogative of the different actors involved in the Regulation (PP, CA, EU Centre). This would be disseminate at national level in order to facilitate a deeper evaluation on the impact on national legal and operational framework.

Please consider also that since national assessment on the proposal is still pending, we have a general scrutiny reservation on the text.

LATVIA

GENERAL PRELIMINARY COMMENTS

LV agrees that work on prevention and combating of child sexual abuse (CSA) **has to be intensified**.

LV also agrees that **voluntary measures** by providers to detect and report CSA **have proven insufficient**.

LV continues assessing the proposed CSA Regulation. Thus, LV maintains **general scrutiny reservation**.

DETAILED PRELIMINARY COMMENTS

Article 3 “Risk assessment”

LV finds it important that almost all hosting service providers and interpersonal communications service providers have **at least 6 months** to carry out the first risk assessment. LV understands that in accordance with Article 3(4) the first risk assessment has to be carried **by 3 months after the date of application of the proposed CSA Regulation** (it shall apply from six months after its entry into force that is on the twentieth day following that of its publication in the Official Journal of the European Union). Thus, in practice, the relevant providers already offering their services in the Union will have **9 months** from the entry into force of the proposed CSA Regulation to prepare the first risk assessment, that, in LV view, is sufficient. In view of this, LV considers that **at least 6 months** should also be granted to those providers that did not offer the service in the Union by the date of application of the proposed CSA Regulation (currently 3 months).

Article 5 “Risk reporting”

LV believes that in the second sentence of Article 5(3) **a reference to Article 5(2)**, not to the first subparagraph should be (LV considers that this provision refers to the suspension of the 3 months’ period related to the assessment and determination of the Coordinating Authority of the establishment referred to in paragraph 2 of this Article).

Chapter II “Obligations of providers of relevant information society services to prevent and combat online child sexual abuse”

General comment: LV would like to clarify, whether after the entry into application of the proposed CSA Regulation (when the Interim Regulation (Regulation (EU) 2021/1232) ceases to apply), relevant service providers will be able to continue the **voluntary detection of the CSA** on the basis of the proposed CSA Regulation (as COM previously pointed out the issuance of the first detection order could take **approximately 1 year**). If the answer is affirmative, LV would like to draw attention to the fact that in such case certain service providers (who will not be issued a detection order, but who will nevertheless continue voluntary detection of CSA) will continue making their own decisions regarding fundamental rights, as well as there will not be harmonized guaranties (so far COM mentioned that one of the aims for the mandatory detection of CSA by relevant providers was to eliminate such situations).

Article 7 “Issuance of detection orders”

LV notes that in accordance with Article 3(4)(a) a hosting service provider or interpersonal communications service provider whose service is subject to a detection order issued in accordance with Article 7 has to update the risk assessment at the latest two months before the expiry of the period of application of the detection order. In view of this, LV considers that Article 9(3) should set not only a maximum period of application of a detection order, but also **an adequate minimum one (for example, 6 months)**.

LV would like to understand whether the application period of the issued detection order can be extended, as well as the procedure for the issuance of a new detection order, namely, whether in practice there can be a situation where a hosting service provider or an interpersonal communications service provider is not required to make a mandatory detection of CSA in a particular service for a certain period of time despite the high risk of dissemination of CSA there.

LITHUANIA

Please be informed, Lithuania strongly supports the new EU Commission's initiative regarding Regulation on combating child sexual abuse. Unprecedented growth of numbers of child sexual abuse all over the world on the Internet calls EU member states to be united to tackle it. We would like to highlight, that it is appropriate to assess the proposed regulation not only in the context of proportionality with human rights but also in the context of the personal data protection. We support **measures that clearly describe the obligations for digital service providers to respond, to assess and to remove immediately the illegal content online.**

However, **we are reserved about the establishment of a separate EU centre.** We do understand that the envisaged functions of the centre are crucial and necessary in addressing child sexual exploitation, but the nature of the functions is specific and covers a rather narrow field.

Additionally, it is questionable whether with the establishment of a/m centre will not provoke the delays in the process of the information exchange with law enforcement and deletion of the illegal content online, as it will be an extra chain in the whole process.

Lastly, we would like to take a **scrutiny reservation to the whole proposal itself** as the internal discussions with relevant partners in the capital have just started and due to the complexity and volume of above mentioned Regulation, we need more time to dig deeper in the details and address this proposal respectively.

MALTA

– General considerations

In principle, the Maltese government supports this proposal. At this stage, Malta joins other Member States in entering a general scrutiny reservation. It is important to set out clear aims and objectives and how these are going to be implemented by both the private sector and public authorities. To this end, the legislative proposal should not present a complex approach which would decrease the effectiveness of its aims and objectives.

Malta welcomes the references to hotlines used to report online child sexual abuse to be afforded the necessary recognition in this legislative proposal. With the current text, it is felt that an emphasis of the involvement of the hotline organisations in child sexual abuse material and notice takedown is not adequately reflected in the recitals and operative text. It is therefore imperative to articulate this involvement better for such hotline organisations to continue receiving reports and issuing notice takedowns.

- Article 1

The wording used is reflective of the balance that needs to be found between preventing and combatting child sexual abuse while safeguarding the rights and interests of users of the targeted information society services, in particular to protect the integrity and importance of end-to-end encryption. To this end, Malta looks forward to the opinion of the European Data Protection Supervisor on this legislative proposal.

Another important point is that because of the fact that this *lex specialis* is far-reaching, the specific nature of the judicial and administrative organs and their cooperation with the proposed coordinating authority need to be clear.

In terms of paragraph 2 of Article 1, should this be understood as the scope of the proposed Regulation applying for both intra-EU cross-border information society services as well as those outside the EU which do not have a main establishment? This may require clarification.

In addition, the legislative proposal is similar to Regulation (EU) 2021/784 in some aspects. Again, with reference to paragraph 2 of Article 1, should it be therefore understood that in the intra-EU case, the competent authority of one Member State can issue detection/removal/blocking orders to a relevant information society service established in another Member State or are these orders to be issued to a provider of services by the Coordinating Authority under which that relevant information society service is established? The latter seems to be the case on reading the respective articles on the issuance of the orders. Therefore, clarification on this may be required.

- Article 2

The inclusion of two definitions in para (i) and (j) for ‘child’ and ‘child user’ respectively suggests that this twofold approach is required to address child sexual abuse material and solicitation. Some Member States have asked for this to be removed and to retain one definition with a general age of 18 years.

While Malta is preliminarily in favour of this, we wish to have further information on whether this has been included because of the following reasoning: the definition of ‘online child sexual abuse’ includes both online dissemination of child sexual abuse material and solicitation of children, therefore, the definition of ‘child’ is being used to provide for instances of persons under the age of 18 years who are the subject victims of child sexual abuse material, whereas, the definition of ‘child user’ is being used to provide for instances of persons under the age of 17 years who are susceptible and/or vulnerable to instances of solicitation which leads to child sexual abuse in online and offline sexual activities. This distinction is being made to obligate relevant information society services to not allow ‘child users’ to download high-risk software applications (as per article 6 and the example used by the Commission in the LEWP meeting of 5 July 2022). Can you kindly confirm this? Did the age of sexual consent have any bearing on the decision to have two definitions? An opinion from the Council Legal Service on aligning these two definitions would be welcome, to this end, Malta supports other Member States on this request.

On the lack of definitions regarding the ‘competent judicial authority’ or ‘independent administrative authority’, Malta would be open to examples of authorities which the Commission would envisage being given the role.

- **Article 3**

With reference to the risk assessment, Malta adheres with the first principle of this legislative proposal, that is to prevent, but this should not result in overburdening the operations of relevant information society services. It should be clearer when these kinds of assessments are to be carried out and under which circumstances. On paragraph 4 of Article 3, this risk assessment should be indeed a continuous process which should have clear binding rules. Malta joins other Member States in requesting an illustrative presentation on how the risk assessment would work and any measures for non-compliance to the requirements for this assessment.

Article 4

The removal of child sexual abuse material is more effective when ‘trusted flaggers’ as specialised entities with specific expertise collaborate with online platforms and law enforcement authorities. Using this expertise can result in higher quality notice and take-down. It would be beneficial therefore for the wording on their inclusion in paragraph 1 of article 4 to be strengthened possibly by omitting the option to select which measures are chosen by the provider, rather than relying on the providers to decide.

Article 7

Malta joins other Member States in requesting an illustrative example of the issuance of the orders. For now, the process is being viewed as complex. Malta supports the concerns raised by other Member States. The traditional roles of judicial and law enforcement authorities are not clear; how will the law enforcement authorities operate in terms of this legislative proposal? The provisions indicate that the coordinating authority will be collecting the evidence and making the case for the orders, with other authorities then deciding whether to take it forward. What happens if the online child sexual abuse is first presented to the law enforcement authority? Is it the case that it will feed this information to the coordinating authority and its responsibility stops there?

THE NETHERLANDS

The Netherlands acknowledges the problem of Child Sexual Abuse Material (CSAM) and the urgency to fight this horrible crime. In recent years, the Netherlands has made great efforts to reduce the amount of CSAM on Dutch networks. The Netherlands is a big proponent of a joint European approach to combat child sexual abuse material, given the fact that the Internet crosses national boundaries. We are therefore pleased that the European Commission has published a proposal to make the fight against child sexual abuse more effective in Europe. We applaud the efforts of the Commission to strengthen the European fight against CSAM and we welcome the proposal, although we also have various questions and concerns. The Netherlands appreciates the possibility to ask questions about the proposal and looks forward to the Commission's responses.

The Netherlands appreciates it if the Commission can clarify some questions about the articles 1 – 7.

Article 1(c):

Article 1 under C only mentions hosting providers. Can the Commission clarify why the mandatory removal or disabling access of CSAM does not apply to interpersonal communication services?

Article 2(j):

Regarding the definition of 'child user' in Article 2(j), we want to ask why a child (i) is defined as someone under 18 and a child user as someone under 17? It might make more sense to define 'child user' as "*a child who uses a relevant information society service*". This since 'child' already has been defined.

Article 3, 4 & 5:

Why, as opposed to Terroristic Content Online-Regulation (TCO), is decided that all HSP's and ICS in general need to have a mandatory risk assessment (**Article 3**), take mitigating measures (**Article 4**) and to impose a reporting requirement (**Article 5**)? We can imagine that this stems from the desire to reduce the amount of CSAM as much as possible.

The question is if these requirements are still proportionate in relation to the goal? In other words, how many providers are affected by these measures and can the Commission clarify why it thinks a general obligation is necessary to reduce CSAM?

Article 5:

Concerning the coordinating authority, we wonder what is the relationship with the coordinator mentioned in the digital services act (DSA), the authority mentioned in the TCO-regulation and this coordinating authority.

Article 6:

Article 6 requires providers of software applications to consider whether their service poses a risk of abuse for grooming purposes. This requires some clarification. The Netherlands wonders at what risk measures are justified and what kind of measures it should think of?

Article 7:

- a) Firstly, we wonder what are the implications of a detection order at Interpersonal Communication Services on encryption? Can such an order be fulfilled without breaking (end-to-end) encryption? Furthermore, we are curious how the Commission wants to determine if grooming is taking place? Also, how is the right to respect for private life (and to communication/correspondence) as mentioned in Article 7 of the Charter and Article 8 of the European Convention for the protection of Human Rights and fundamental freedoms protected? How is it ensured that an intrusion into someone's personal life meets the guarantees mentioned in that same article (necessity, proportionality, subsidiarity)? We can imagine that it is more difficult to establish whether grooming is taking place. Therefore it is likely that it is necessary to make a greater infringement on personal life than in the case of CSAM.
- b) How does the obligation to detect under the detection order relate to Article 15 of the Electronic Commerce Directive (Directive 2000/31/EC) and Article 7 of the future Digital Services Act (DSA), respectively, which state that Member States may not impose a general obligation on service providers to monitor the information they transmit or store, or to actively seek out facts or circumstances indicating illegal activity? Are these provisions compliant with the Telecom Code¹ and ePrivacy directive?
- c) Another question regarding the detection order concerns the specific moment at which hosting providers are required to detect CSAM and grooming. Is the scope of the detection order limited to *published* content? Or are hosting providers also obligated to detect material before it is published?

Article 7(1):

The TCO regulation explicitly states in Article 5(8) that the obligation to take specific measures for hosting service providers does not include a general obligation to monitor the information they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. In addition, the obligation to take specific measures under TCO regulation does not include an obligation for the hosting service provider to use automatic tools. This while the CSAM-regulation provides for measures to be taken as a result of a detection order under Article 7(1) in conjunction with Article 10(1) in conjunction with Article 46 of the Regulation. Why has the Commission chosen for these different approaches?

Article 7(1)

The Netherlands wonders why the Commission chose for this specific structure, in which the coordinating authority asks another judicial or administrative authority to issue a detection order? Why doesn't the coordinating authority do this himself in accordance with regulation TCO?

¹ Telecomcode (EU) 2018/1972 , ePrivacy 2002/58/EG

Article 7(3) c

The implementation plan should be accompanied by the opinion of the Data Protection Authority. What would be the nature of the Data Protection Authority assessment?

Article 7(7)

It is conceivable that some ICS's are an easy tool for grooming by their very nature, since their main service is providing communication between persons. Can the Commission reflect on the scenario when an ICS has done everything in its power to prevent its service from being abused, but grooming still occurs with the use of this service?

Article 7(9)

The period during which a detection order may apply runs from three months up to twelve months. In case of known or new child sexual abuse it may even run up to 24 months. Considering the impact of the (execution of the) detection order on the fundamental rights of its users, this seems to be quite an extensive period. How did the Commission establish that these minimum periods of three months and maximum periods of either 12 or 24 months would be suitable and necessary for the providers to take the necessary measures to prepare and execute detection orders? Furthermore, is the amount of users affected by a detection order a relevant parameter that must be taken into account when issuing a detection order?

PORTUGAL

Following the request for comments by 8.7.2020 (Articles 1 to 7), the Portuguese delegation recalls that it has submitted a scrutiny reservation.

PT wishes, nevertheless, to contribute to the discussion with the following observations:

It should be made more explicit which type of European funding is referred to **on page 3 of the explanatory memorandum**, bearing in mind that national bodies, namely the police, have already made several investments.

Article 1(1): harmonization and the reference to the internal market seems excessive, especially since there are rules that do not contribute to the harmonization of decisions, for example in Article 35 on penalties, which does not really promote the internal market.

It would also be suitable to insert in this article the obligations imposed on software application stores resulting from article 6 and, more clearly, the obligations of each of the entities provided for in Article 2 f), as follows :

1. *This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse.*
2. *It establishes, in particular that:*
 - (a) ***all providers of relevant information society services are obliged to minimise the risk that their services are misused for online child sexual abuse;***
 - (b) ***providers of hosting services are obliged to detect, report, remove or disable online child sexual abuse;***
 - (c) ***providers of interpersonal communication services are obliged to detect and report sexual abuse material on their services;***
 - (d) ***software application store is obliged to assess whether any application that they intermediate is at risk of being used for the purpose of solicitation and, if this is the case and the risk is significant, take reasonable measures to identify child users and prevent them from accessing it***
 - (d) ***providers of internet access services are obliged to disable access to child sexual abuse material;***
 - (e) ***rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member States, the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre') and cooperation and transparency.***

As to the second part of **no. 2 of Article 1**, we suggest to consider the main place of establishment (second part of no. 2 of art. 1).

However, we have serious doubts regarding the characterization of the "providers of relevant information society services", under the terms of no. 2 f), due to subparagraph w).

Article 2 – Regarding subparagraph (m) and (n) it should be stressed that it is not necessary to use the term "potential", as this qualification can be misleading.

With regard to subparagraph p), it should be noted that the proposed definition of "online sexual abuse" as "online dissemination of child sexual abuse" does not correspond to the concept contained in REGULATION (EU) 2021/1232² with regard to the use of technologies by providers of number-independent interpersonal communications services to process personal and other data for the purpose of combating child sexual abuse online, Article 2, paragraph 4, which does not include the term "dissemination".

In addition, the Child Sexual Abuse Directive uses the expressions "distribution, dissemination or transmission".

This is of particular concern as it may have implications for the scope of the proposal. It is questionable whether simple uploading, considered to be the action of sending data from a local computer to a remote server, could be covered by the notion of dissemination.

As regards **subparagraph w)** PT considers that the understanding of the European Data Protection Board, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf, is still valuable : in fact the proposal adopts a "formalistic approach according to which companies are only established where they are registered". Yet it would be important to take into account the level of stability and the specific nature of the activities in the MS.

Therefore we point out that more proximity to Article 4(16) of the GDPR, would be desirable.

Subparagraph l): PT believes that there are areas that allow for a difficult interpretation of what is effectively material to be detected. See in particular Article 5, paragraph 7 of the Directive on the sexual abuse of minors and also the conditions under which paragraph 8 of the same article is applied.

Article 6 - PT recalls the question raised at the last meeting concerning the use by adults of applications intended for children (impersonating children), that should be looked upon

Article 7 - PT notes that the structure of the document is conducive to some confusion, since conceptually it would be clearer not to spread the competences of the national coordinating entities over several chapters.

² REGULATION (EU) 2021/1232 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC

SPAIN

Spain supports all measures to strengthen the detection and surveillance of child pornography and other sexual abuse of minors on the Internet and the idea of encouraging the cooperation of companies that offer services on the web in order to develop prevention strategies. However, this legislative development is very complicated and involves several actors, which is why Spain has a scrutiny reservation on this issue. Having said that, Spain has a general comment to share:

General comment on the scope of protection: Sexual Abuse against Children and **Vulnerable People:** The Convention on the Rights of Persons with Disabilities from the United Nations (UN-CRDP) states in article 16.1 that “States Parties shall take all appropriate (...) measures to protect persons with disabilities (...) from all forms of exploitation, violence and abuse, including their gender-based aspects”. Individuals with intellectual disability (ID) are more likely to experience sexual abuse and less likely to report it. Consent is crucial when anyone engages in sexual activity, but it plays an even greater, and potentially more complicated, role when someone has a disability. Some disabilities can make it difficult to communicate consent to engage in sexual activity, and perpetrators may take advantage of this. Persons with disabilities may also not receive the same education about sexuality and consent that persons without disabilities receive. In addition, a person with an intellectual or developmental disability may not have the capacity to consent to sexual activity as defined by state law. All of these factors make this group more vulnerable to sexual abuse online, which is why Spain believes that the scope of protection in this regulation should be extended for vulnerable persons too.



Council of the European Union
General Secretariat

Brussels, 18 July 2022

Interinstitutional files:
2022/0155 (COD)

WK 10235/2022 ADD 1

LIMITE

**JAI
ENFOPOL
CRIMORG
IXIM
DATAPROTECT
CYBER
COPEN**

**FREMP
TELECOM
COMPET
MI
CONSUM
DIGIT
CODEC**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Law Enforcement Working Party (Police)
N° prev. doc.:	9068/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations on Articles 1 to 7

Delegations will find attached the compilation of comments received from Members States on the above-mentioned proposal following the meeting of the LEWP (Police) on 5 July 2022.