Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 12 April 2023

WK 10235/2022 ADD 10 REV 2

LIMITE

JAI	**FREMP**
ENFOPOL	**TELECOM**
CRIMORG	**COMPET**
IXIM	**MI**
DATAPROTECT	**CONSOM**
CYBER	**DIGIT**
COPEN	**CODEC**

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

WORKING DOCUMENT

From: To:	General Secretariat of the Council Law Enforcement Working Party (Police)
N° prev. doc.:	9068/22, 14143/22
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 12 to 15

Delegations will find attached the compilation of comments received from Members States on the abovementioned proposal following the meeting of the LEWP (Police) on 19-20 January 2023.

Written comments submitted by Member States

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

(9068/22)

Contents

BELGIUM

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

We believe in the motto, "security through encryption and despite encryption". We are therefore in favour of excluding E2EE, but would, however, propose that service providers are responsible for the management of their own networks and encryption. Meaning that a service provider should be able to "deactivate" their own encryption when a request from a judicial authority is submitted. We are in favour of continuing the automatic and systematic control for CSAM, but in regard to E2EE, we would emphasis to place the responsibility on the providers.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

We recognise the added value of voluntary collaboration and follow the advice that it should be explored further. We might propose that voluntary detection of CSAM online is followed by mandatory reporting (and removal) of the material in question.

Regarding the implementation, we mainly would like to emphasise that there cannot/should not be a gap between the termination of the temporary regulation and the implementation of the CSA regulation. We would propose to include its contents in the CSA regulation and ensure that there is no gap in the transition from temporary regulation to CSA regulation.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We are not in favour of including audio communications in the scope of the CSA regulation and would follow the reasoning of the aforementioned regulation. We consider that the costs of including audio communications are not proportional to the benefits. Audio communications are a minority of the targeted material. Currently, the material, which constitutes child pornography, usually takes the form of images or videos. Therefore, we consider that the inclusion of audio would render the scope of the CSA regulation too broad.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

We would propose that there would not be a strong obligation for including interpersonal communications, but rather the possibility for those service providers who are able to implement it. Specifically, publicly available interpersonal communication services should be covered by a legal framework allowing them to detect CSA, given that they are increasingly used for the exchange of CSAM.

However, we are curious about the current technical aspects of detection on interpersonal communications as this could help us to better understand the issue at stake. Any enlightenment at the next LEWP in this matter would be welcome.

General comments:

We are grateful for the good conduct of the negotiations, and we would like to thank the Swedish Presidency for reupdating the discussions while offering the Member States the opportunity to reaffirm their updated point of view in the light of the new reports and workshops that have been conducted since the previous LEWP-CSA.

One will notice that the written comments on these specific articles are substantially the same as the last written contributions we already send to the CZ presidency. However, we have tried to adapt it in light of the new elements that were shared during the last meeting as well as with the subsequent consultations that we carried out with – among other - the representativeness of hotlines.

On the EDPS point of view:

Reference; Doc WK832/2023

We would like to reiterate our keen interest in receiving a written support concerning the legal consideration of the commission on the EDPS report.

Additionally, before being able to share our fully finalised legal analysis of the EDPS report, we would need to acknowledge the official legal opinion of the CLS.

On article by article :

Reference: Doc 14143/22

Article 12

As for informing of the user in Article 12(2) about how the provider became aware of possible CSAM, we want to highlight the importance of safeguarding the effectiveness of the established measures. We propose to add a text here similar to the last sentence of Article 6(3) on the risk mitigation measures.

In the same spirit as the German request about the consistency with the Digital Service Act in relation to the phrase "*giving rise to suspicion*" in Article 12(1) we wonder about the terminology of "*flag*" in Article 12(3). In order to ensure clarity, we suggest replacing "*flag*" with "*submit notices*".

As a general remark, we believe it is appropriate now to start streamlining the text with the published Digital Services Act. This is also relevant to the last Articles in Chapter III as well as to our proposition for art. 13.

We support the proposal that user information be reported/reported as a standard arrangement (Art. 12), until the MS indicates that the user can be informed.

Moreover, for forwarding notifications/ reporting to MS and to Europol, the text should especially include that it is a simultaneous and parallel forwarding/ reporting. We believe that it is also important in practice that everyone knows "who sent the notifications" (in relation to our request on article 13)

Article 13

In our view, the urgency of certain reports by providers (Art. 13) is determined by whether the integrity of the child is threatened or not. Therefore, we would like to add a reference to this urgency in paragraph (1) of Article 13. The answer COM is indeed relevant but not sufficient, we consider that it is not only necessary to mention that something is "urgent" but we would like to depict more in-depth what is considered as "urgent".

We also have preliminary conclusions on how we want to better integrate the hotlines, such as our own childfocus at the Belgian level, into the whole text.

It would be interesting and would have a significant added value if the report of a "providers" notification to the Eu-Centre (proposed in article 13 of the CSA) also included the origin of the CSAM found, i.e. if it indicated whether it came from a "*trusted flagger*" (which could include, for example, hotlines), the victim, the detection technology, etc. This could help in triage and avoid possible duplication.

The term of "trusted flagger" is defined in the article 22 of REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)

Article 14

We do not support the addition of Article 14(3a). For similar reasons we request its deletion in Article 16(4) and Article 18a (3). We understand that this addition is linked to the independence requirements of the Coordinating Authorities and the competent authorities. However, we want to ask for a different solution. It is not possible for Belgium to enable such supervision over the actions of, for example, a prosecutor issuing a removal order. Moreover, the origin of this paragraph in the Terrorist Content Online Regulation is situated in the verification of cross-border removal orders, issued by other Member States. It is not suitable in the context of an order issued within the Member State. If a check is necessary, this should be done through the right to challenge a removal order before the courts as described in Article 15(1).

Article 14a

We welcome Article 14a on cross-border removal orders. However, a change is still required in Article 14(1) to correctly make Article 14a the additional rules on top of Article 14. In Article 14 the words *'under the jurisdiction of that Member State'* should be deleted to make it a coherent structure. In this way, Article 14 ensures that those rules should be followed for all removal orders addressed to all providers, while Article 14a ensures that additional rules should be followed for cross-border removal orders.

Additionally, we think it is useful to either replace '*content provider'* with '*user'* in Article 14a or to add a new definition for '*content provider'* based on Article 2(2) of the Terrorist Content Online Regulation. We would welcome the Commission's views on this.

BULGARIA

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

In the course of the discussions on the CSA Regulation, technologies were presented which are said to have the ability to detect illegal material in encrypted communication. Therefore Bulgaria does not support weakening end-to-end encryption (E2EE) as it is essential to ensure secure communications. We believe that the inclusion of E2EE safeguards could be provided in the Regulation.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

We support the need to explore whether voluntary disclosure should continue. We believe that the voluntary detection of illegal materials can be included in the CSA proposal, as this approach has proven to be effective and leads to positive results.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We support the inclusion of audio communications in the scope of the proposed CSA Regulation.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

In order to ensure the effectiveness of the Regulation, it should also cover the detection of illegal content in interpersonal communications, since a significant part of the material exchanged by the users is made through personal private messages and chats.

Furthermore Bulgaria supports the amendments in Articles 12-15 of the CSA Regulation.

CROATIA

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

HR is in favour of regulating end-to-end encryption in CSA regulation. End-to-end encryption already has negative impact on effective detection of the CSAM material and is being misused by the offenders. This topic was one of the main topics included in technical workshop. Technical workshop did not provide an answer to question are there effective ways and strategies to bypass end-to-end encryption in order to identify CSAM materials and offenders distributing CSAM. HR shares the Commission's concerns about the impact Facebook`s introduction of end-to-end encryption to FB Messenger service would have to number of NCMEC reports. Considering all those reasons it is of outmost importance to provide clear wording in the CSA Regulation that end-to-end encryption is not a reason not to report CSA material.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Voluntary detection is good tool to protect children and bring criminals to justice. It should be included in the CSA Regulation.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

Audio communication can be used for grooming purposes. It should be included in the CSA proposal if adequate tools are available for detection of grooming via audio communication.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

The right to privacy is not an absolute right. Children`s right to their privacy and life are to be protected by EU legislation as well. Vast majority of the CSAM material is being uploaded to and shared on interpersonal communications applications. Therefore those application should be obliged to share information with the law enforcement.

CYPRUS

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

The access of Law enforcement authorities to encrypted communication is necessary for the effective investigation of crimes of online sexual abuse of children and this should be regulated in the text of the Regulation. It should be taken into consideration that many times illegal activities are organized through encrypted communications and the impact of this regulation is significant because it will set a precedent for other sectors in the future. Of course, such regulation should be balanced with the need to ensure the right to privacy, taking into account the jurisprudence of the European Court of Justice.

2 Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

The voluntary detection should be continued through including its content in the CSA proposal. To ensure that there would be no gap in this respect, we should consider prolonging the Temporary Regulation (EU) 2021/1232.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

Audio communications should be included in the scope of the CSA proposal.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

The detection of CSA should be performed both on interpersonal communications and publicly accessible content, taking into consideration the need to safeguard the right to privacy.

Additionally, considering Article 14 of the Proposal, the phrase «*under the jurisdiction of that Member State*» should be deleted, while the phrase «*in all Member States*» should definitely be preserved, as this will empower the competent authority to issue removal orders in respect of material located in other MS.

CZECH REPUBLIC

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

The Czech Republic welcomes the opportunity to comment on the E2EE issue. We consider encryption to be very important as it ensures secure communication in the online environment. Given the technological neutrality of the proposed Regulation, we do not consider appropriate to explicitly prohibit the use of encryption technologies. A Regulation is an EU law that should, first and foremost, set out general boundaries.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

The voluntary detection is now performed by online service providers who are aware of their social responsibility. These online service providers are motivated to provide a safe environment for their users. In our view, these activities need to be supported. The Czech Republic considers the maintaining of the voluntary detection option to be appropriate, as it will be partially maintained after the expiry of the provisional Regulation. We believe that motivated providers will also be able to address the security of its services under the new Regulation. These providers will carry out a risk assessment of its services, set effective protective measures and, if necessary, if these providers are unable to set effective protective measures, they may apply through the Coordinating Authority for a detection order to carry out the detection.

On the question of how to ensure the detection option by the time the draft CSA Regulation comes into force, the Czech Republic is in favour to prolong the Temporary Regulation (EU) 2021/1232.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We are discussing audio communication solutions at the national level. We are not yet fully convinced of the need to exclude audio communications from the scope of the CSA proposal.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

In our view, the substantive scope of the proposed Regulation should be taken into account when addressing this issue. This Regulation should set out rules for dealing with child sexual abuse, which includes both the abuse of children in pornographic material, including its sale and the misuse of material for purposes for which it was not intended or even for unauthorised communication with children, including elicitation followed by their physical abuse.

By nature, such materials will no longer be presented in public space. Unlike, for example, a message with terrorist content, which, on the contrary, is intended to target the widest possible public. Therefore, we believe that the Regulation cannot be limited to publicly accessible content, if the purpose intended by the creation of the Regulation is to be preserved.

Written comments related to compromised text of the Proposal (14143/22):

Regarding Art 13 par 1 (c)

The Czech Republic suggests deleting of the second part of the sentence ***"..including images, videos and text;"*** . It will lead to a generalization of the wording and it will not be necessary to exclude any type of the material.

Regarding Art 14 par 3a and Art 14a

The Czech Republic understands this paragraph as a safeguard against the violation of the right to privacy and the possibility of correction of the issued removal order by reconsideration. According to Art 25, par 2, the Coordinating Authority is one of the competent authorities, it cannot happen that the removal order issued by, for example, a judicial authority of a Member State will be assessed by an administrative authority. When the Coordinating Authority will be an administrative authority, the competent authorities will also have to be an administrative authorities and vice versa.

We propose to devote more attention to this issue in the cross-border scope of the removal order according to Art 14a. An order issued by a judicial authority (in the role of a competent authority) in one Member State could, under current conditions, be assessed by an administrative authority in another Member State.

However, we believe that it is necessary to establish a procedure for the enforcement of an issued removal order in a Member State other than the State of jurisdiction of the issuing authority.

There are two possibilities:

1) Applicability in another Member State automatically without the possibility of revocation by the Coordinating Authority of the other Member State.

2) Acceptance and confirmation of applicability by the authority of the other Member State which did not issue the removal order. There is certainly a possibility of assessment by the Coordinating Authority. In case that the decision of the court is reviewed by an administrative authority, there is the possibility of annulment by the court on the request of the reviewing authority.

DENMARK

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

Denmark understands the first part as a question on whether or not encrypted material should be included in the scope of the proposed Regulation. To this end, Denmark is in favour of letting encrypted CSA material be included in the scope and thus subject to detection orders.

As regards the second part, Denmark finds it crucial that the proposal strikes the right balance between on one hand respect for private and family life and the protection of personal data as enshrined in Articles 7 and 8 of the Charter and on the other hand the legitimate intent to prevent and combat child sexual abuse. There has been a lot of debate as to whether or not the proposal should cover E2EE. It is the experience of our national police that CSAM often spreads through platforms that use E2EE. Therefore, we agree with the Commission that to exempt E2EE services would compromise the proposal's capacity to achieve its objective of preventing and combating (online) child sexual abuse. Thus, having noted the arguments put forward by EPDS and EDPB on the importance of E2EE and in order to emphasize that the CSA proposal does not prevent the providers from applying E2EE on their services, Denmark is in favour of including some wording excluding the weakening of E2EE.

2) Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Denmark is in favour of the possibility of upholding voluntary detection as well as voluntary removal and blocking alongside the Regulation. Please find our elaboration on this topic below. Denmark is therefore open to discuss how voluntary agreements regarding detection, removal and blocking can be upheld. We would prefer including voluntary detection in the proposal in order to ensure the best interplay between voluntary and mandatory detection and blocking.

3) Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

Denmark is in favour of including audio communications in the scope of the CSA proposal.

4) With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

Denmark finds that interpersonal communications should be included in the proposal. It is our experience that most of the spreading of CSAM and grooming occur in interpersonal communication and in closed groups and not in publicly accessible content.

The CSA proposal

General remarks

Denmark fully supports the intentions behind the proposal. However, Denmark finds that some of the proposed provisions contain a range of lengthy and inflexible procedures, e.g. with regards to detection and removal orders, which are inconsistent with the reality of CSAM cases where time is a crucial factor in order to effectively block and prevent the further spreading of CSAM. Denmark finds that a reasonable balance must be struck between the need for a timely and effective effort to prevent and combat child sexual abuse and ensuring the legal guarantees of the involved actors.

To this end, Denmark suggests including the possibility of precautionary measures, i.e. the principle of periculum in mora, in the proposal. For example, if the police wish to conduct a search of the property of a suspect, and the search would lose its purpose if the police had to await a court order, the police can conduct the search without a court order. As soon as possible and at the latest 24 hours after the search, it must be brought before the court in order to assess whether the intervention was lawful if requested by the affected person. This process is also used with regards to intercepted communications and seizures. Introducing a similar approach in the proposal would give the relevant authorities simpler processes to navigate while still safeguarding legal guarantees. Denmark finds that this approach could be beneficial with regards to detection orders in Article 7, removal orders in Article 14 and blocking orders in Article 16.

Denmark also finds that inspiration should be drawn from the procedures in the Regulation of the European Parliament and the Council on Preventing the Dissemination of Terrorist Content Online (TCO) in which the procedures for deactivation and removal are simpler and more flexible.

Finally, we propose that the deadlines for the Competent and Coordinating Authorities regarding the different orders in the proposal are streamlined. This would simplify the procedures for the involved authorities when carrying out the tasks provided for by the Regulation.

Voluntary agreements to continue alongside the Regulation

In Denmark, the effort to prevent and combat CSAM is currently based on a voluntary arrangement between the Danish police and Danish Internet Access Service Providers. The arrangement is called "Netfilter blocking" and has proven to be very successful and effective.

The Netfilter blocking is based on cooperation agreements between the Danish police, individual Danish Internet Access Service Providers and the Danish NGO Save the Children. If the police become aware of an internet site containing CSAM, the police will inform the Internet Access Service Provider and recommend blocking access to the internet site. The recommendation is based on the police's assessment of the material on the internet site, and the legality of the material on the internet site has not necessarily been subject to a judicial review. As access to the internet site is blocked based on the voluntary cooperation agreement, the blocking is not a coercive measure and police investigation concerning access to the internet site is not automatically initiated. The aim of the arrangements is to prevent access to and spreading of CSAM.

Furthermore, under the arrangements the Internet Access Service Providers inform the police of the previous internet site that the user accessed when trying to access a blocked internet site – so-called referrals. This information is very useful to the police since many of the users come from internet sites that also contain CSAM, and with this notification the police will be able to block these internet sites as well. If a user attempts to access a blocked internet site, the user will be presented with a message on the screen saying that the user is trying to access CSAM which is illegal according to Danish legislation. Furthermore, the user will be presented with information on how to contact a Danish public sexological clinic anonymously to get help in case of addiction to CSAM.

The arrangements have existed since 2005, and today nearly 80% of the internet in Denmark is covered by these arrangements. The cooperation enables the police to react very quickly (within a day) in order to block access and avoid further spreading of the content. The time element is essential in order to prevent both access to and further spreading of the material. Denmark considers the cooperation with Internet Access Service Providers and Save the Children to be of significant importance for the possibility to prevent access via the internet to CSAM.

Against this background, Denmark strongly advocates for the possibility of upholding voluntary agreements alongside the CSA-regulation.

Article 12

We suggest that the time period in Article 12 (2) is extended, for example to 12 months. Due to the high number of cases concerning CSAM and the processing of these, it is very likely that the police will have to request extension of the time period referred to in paragraph 2 several times, which will impose an administrative burden on the police.

Furthermore, we kindly ask the Presidency and/or the Commission to confirm that the providers will still be able to report material directly to the police after the entry into force of the CSA-regulation and that police will still be able to initiate an investigation on the basis of such report without having to await a report from the EU-center.

Article 14 and 14 a

As Denmark has previously emphasized, the Danish constitution sets certain boundaries when it comes to foreign states' exercise of authority on Danish territory.

It is our understanding, that Article 14 and 14a should be understood in such a way, that a competent authority in one Member State shall have the power to issue a removal order directly to a hosting service provider in a different Member State. It is also our understanding, that such removal order will be binding upon the hosting service provider without the prior involvement of the authorities of the Member State of establishment. Reference in this regard is made to Article 14a (2) together with Article 14 (2)

For these reasons Denmark cannot support the current wording of the provisions.

In order for Denmark to support the provisions, the process must be changed so that the competent authority issuing the removal order sends the order to the competent authority or the coordinating authority of the member state where the provider has its main establishment. In order for the removal order to become binding on its territory, the competent national authority or the coordinating authority of the Member State of establishment would have to forward the removal order to the provider in question. Denmark suggests that the necessary changes are made in Article 14 (4).

In relation to Article 14 (3a), Denmark supports the deletion of Article 14 (3a) in the recent Presidency compromise text (6276/23). If the provision is reintroduced, Denmark would support the French suggestion to replace "shall" by "may" in the second sentence of Article 14 (3a).

Article 15

We find the time period in paragraph 4 too short. Due to the high number of cases of CSAM investigated by the police, a six-week deadline will put a disproportionate administrative burden on the police. Therefore, we propose that the deadline is extended, e.g. to 12 months with the possibility of extension during the entire investigation when necessary to avoid interfering with such activities.

ESTONIA

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

If the company's service description says that no data is stored and E2EE encryption, i.e. the content, cannot be opened by them - then this detection order is essentially unenforceable. In other words, a) the company will redo the their systems if the EU imposes an obligation on it (that it must be able to decrypt the data) or b) it will shut itself down. In other words, the wording in itself is OK, in principle to set a precedent, but many countries are against it, because some think that it is a "backdoor, i.e. breaking the encryption", not "2 doors and 2 keys, i.e. it is possible for the company to access data based on need" – doesn't technically break encryption".

2. *Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?*

We're not quite sure what that actually means. Because those companies that do it anyway- OK, but the ones that don't have an obligation or don't want to do it - voluntary. Same as the previous question - if someone owns an E2EE service and their goal is complete privacy, then even if they wanted to, they can't do it on their own initiative, because the system is built on other principles.

3. *Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?*

We are a bit reserved and concerned with the potential inclusion of „audio communication". For us the question is about what communication are we discussing – FB voice messages or direct special services or applications offering only voice communication service, including encrypted ones? Secondly the initial proposal and assessment (Interinstitutional File: 2022101 55(COD)) focused mainly on visual material and sites and web links – indeed, this is the most pressing issue here. Audio communication was not included in that with a big attention scope.

This does not mean that Estonia doesn't think grooming etc. criminal activities are not important. They are and we support any action fighting against this issue! We also want to remind, that EUCJ has forbidden the state regulation retention obligation of metadata by service providers. Now, we create a regulation which forces service providers to carry out mass interception of content data, which, as we want to emphasise, was the counter-argument regarding the metadata retention in the court. This is something we don't want to do in Europe. This may also create more friction with the EU Parliament.

4. *With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?*

CSA generally does not move through public open communication, but closed groups and crypto channels are the environment in which it moves. The goal is not to break private voice communication or anything else, but that in the case of reasonable suspicion, the entire service server should not be eavesdropped on for 3 months in the case of 100,000 service users (for example encrochat legal case). This is the essence of the whole problem - detection order is missing from public channels, because this content is not protected by anything, the content is not hidden.

In regards to Articles

- **Article 7 Issuance of detection orders**
  Art 7(1): We would like to hear the **CLS opinion**, whether this order breaches the no general obligation to monitor principle. ECJ case-law emphasizes that the provider must not be required to carry out an **independent assessment to evaluate whether the content is illegal**. How is this requirement provided in this article, especially in cases of new content and solicitation?

- **Article 10 Technologies and safeguards**
  We are still unsure, what are the technologies for detecting solicitation in **e2e encrypted services**. It is still unclear, whether there are technologies available today, which would enable monitoring e2e encrypted content without compromising the security and the integrity of these services. We do not support the possibility of **creating backdoors** to end-to-end encryption solutions.

- **Article 12 Reporting obligations**
  According to our analysis many of these obligations **duplicate the obligations of the DSA regulation**. Art 12(1) duplicates the obligation in art 15a of the DSA regulation to notify law enforcement authorities of a criminal offence involving a threat to the life or safety of a person or persons. Art 12(2) duplicates the obligation in art 15 of the DSA regulation to provide a clear and specific statement of reasons to the users of any restrictions imposed regarding the content or the user account. Art 12(3) duplicates the obligation in art 14 of the DSA regulation to set up a notification mechanism. The interplay between these two regulations must be explained. Instead of duplication, reference must instead be made to the **relevant DSA provision**. If necessary, it should be **explained in the recitals** how this obligation should be fulfilled in case of CSAM. The same concern applies to **art 23-24 obligations** to determine a point of contact and a legal representative. Also, we are still worried about the **lack of transparency for users** since it could now take up to a year for them to be notified why their content was removed. If the user does not know why their use of the services is restricted, they cannot contest it.

- **Article 14a Procedure for cross-border removal orders**
  We would also kindly ask you to overlook the drafting for article 14a. Currently in the text there is no legal basis for all competent authorities to issue removal orders. New art 14a(1) refers back to article 14(1), which only gives powers to Member State of establishment. Please compare with art 3(1) of the TCO regulation, which gives powers to competent authorities of each Member State.

Some additional comments from the Estonian Ministry of Economic Affairs and Communications:

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

We are in favour of adding similar wording that excludes the weakening of E2EE. Estonia does not support the possibility of creating backdoors for end-to-end encryption solutions. End-to-end encryption is an important tool to guarantee the security and confidentiality of the internet infrastructure and the communications of users. Any weakening of encryption could potentially be abused by malicious third parties. Therefore, end-to-end encryption should not be weakened. At the same time, we can support the use of privacy enhancing technologies (PETs) that allow the analysis of encrypted content without decryption, so that the reliability, security and integrity of digital services relying on encryption is preserved.

We have **made a proposal to add a provision protecting the security of E2EE in art 7(10new)** based on recital 25 of Regulation (EU) 2021/1232):

Article 7(10): The detection order shall not prohibit or weaken end-to-end encryption or oblige the service provider to provide encryption backdoors.

2. *Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?*

We are in favour of prolonging the temporary regulation (EU) 2021/1232. We could also support including the content of the temporary regulation (EU) 2021/1232 in the CSA proposal. We share the same concerns expressed by the industry that there could be a time gap, where this proposal has not yet been implemented and the temporary regulation ceases to apply. Also, issuing a detection order is a lengthy process, which could take considerable time. We are in favour of supporting voluntary actions of communication services in protecting children and detecting illegal content.

3. *Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?*

We find that expanding the scope requires assessment on the implications of widening the scope. We believe that scanning of audio communications is very intrusive and as such better to remain outside the scope of the detection obligations set out in the proposed Regulation.

4. *With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?*

Regarding which services should be in scope, the more relevant question should be what should be detected. We are not against including interpersonal communication services in the scope and applying some obligations to them. However, we have serious concerns about the obligation to detect child solicitation. Firstly, we are unsure, whether this obligation is technically feasible in practice considering that there is no technical solution available today in which case the service provider must not apply human review, also these technologies are not available in Estonian. Secondly, we are seriously concerned how this obligation would affect the right to privacy and the rights of the child. Therefore, we have serious reservations about including solicitation in the proposal.

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
Article 4 Risk mitigation	***Article 4 Risk mitigation***	
1. Providers of hosting services and providers of interpersonal communications services shall take reasonable mitigation measures, tailored to the risk identified pursuant to Article 3, to minimise that risk. Such measures shall include some or all of the following:	1.Providers of hosting services and providers of interpersonal communications services shall take reasonable mitigation measures, tailored to the risk identified pursuant to Article 3, to minimise that risk. Such measures shall include some or all of the following:	Service providers should not be discouraged from using other possibly more suitable or effective risk mitigation measures, which could better protect the privacy and the fundamental rights of the users.
3. Providers of interpersonal communications services that have identified, pursuant to the risk assessment conducted or updated in accordance with Article 3, a risk of use of their services for the purpose of the solicitation of children, shall take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the mitigation measures		We are concerned about how gathering large amounts of data or identifying users to determine their age could affect the right to privacy and the principal of data minimisation. Therefore, we especially support the introduction of age recognition technologies where the age of the user is identified in a reliable way by a third party, providing only information on whether the user is a child user to a specific service provider.
	4a. Any requirement to take risk mitigation measures shall be without prejudice to Article 8 of Regulation (EU) 2022/2065 and shall entail neither a general obligation for intermediary services providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. Any requirement to take specific measures shall not include an obligation to use automated tools by the hosting service provider.	Important to preserve the no general monitoring principle stated in the DSA, which rules this regulation does not affect. The requirement to implement risk mitigation measures should not lead to a general obligation to monitor or to engage in active fact-finding or to an obligation to use automated tools. However, it should be possible for intermediary service providers to use automated tools if they consider this to be appropriate and necessary to effectively address the misuse of their services. Same provision as art 5(8) in the TCO regulation.
Article 7 Issuance of detection orders	***Article 7 Issuance of detection orders***	**General comments:** We are still analysing the file and whether the detection order breaches the prohibition of the no general obligation to monitor principle. We would like to hear the CLS opinion, whether this order breaches the no general obligation to monitor principle. The no general monitoring principle also applies to orders issued by national authorities. During the

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
		negotiations of the General Product Safety Regulation, the CLS expressed its opinion that the obligation for online marketplaces to check the products and services offered on the platform against the RAPEX database for dangerous products constitutes a general monitoring obligation, which is prohibited. Later case-law emphasizes that the provider must not be required to carry out an independent assessment to evaluate whether the content is illegal. How is this requirement provided in this article, especially in cases of new content and solicitation?
5. (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.	5. (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.	The issuing of the detection order must be based on concrete evidence about the specific service. It should not be possible to issue detection orders preemptively without there being evidence that the service is being used for child sexual abuse. The detection order is aimed at two specific types of services found to be especially at risk - hosting services and interpersonal communications services. Are all these types of services considered comparable services to which detection orders could be issued?
6. As regards detection orders concerning the dissemination of new 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 that, despite any mitigation measures that the provider may have taken or will take, the service is used, to an appreciable extent, for the dissemination of new child sexual abuse material;		Which indicators would be used to indicate new child sexual abuse material? If the abuse material is new, then how could it be assessed that the service is used for this kind of dissemination.
6. (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	6. (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,~~	See comments for sec 5(b).

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
in the past 12 months and to an appreciable extent, for the dissemination of new child sexual abuse material;	having been used in the past 12 months and to an appreciable extent for the dissemination of known child sexual abuse material.	
7. As regards detection orders concerning the solicitation of children, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met: (a) the provider qualifies as a provider of interpersonal communication services; (b) it is likely that, despite any mitigation measures that the provider may have taken or will take, the service is used, to an appreciable extent, for the solicitation of children; (c) 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 solicitation of children. The detection orders concerning the solicitation of children shall apply only to interpersonal communications between where one of the users is a child user and an adult.	7. (c) 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.	See comments for sec 5(b). Regarding the detection orders concerning the solicitation of children, the age of sexual consent in Estonia is 16. Also, it is not a crime if acts of sexual nature take place between a child 14-16 years of age and an adult up to five years older than the child (19-21). Therefore, in Estonia, there is no legal basis to monitor the communications between 16–17-year-olds and adults. Additionally, solicitation is a very nuanced crime taking place over a prolonged period and involving many different episodes. We are concerned whether such prolonged monitoring of personal messages is proportional and respects fundamental rights. "Solicitation" under directive 2011/92/EU Article 6, as referred in the Article 2(o) of the CSA, consists of three independent elements – the proposal, intent to commit an offence and a following material act (such as a meeting). For a service provider to identify a proposal as solicitation (or attempt thereof) is to place independent assessments and to determine evidence for a criminal offence without the authority or even a criminal proceeding concerning the user. Which indicators would be used to indicate the solicitation of children? Also, there are no tools available at the moment, which are able to detect solicitation in Estonian. How could service providers comply with the obligation to stop the solicitation of children in Estonia?
9. The competent judicial authority or independent administrative authority shall specify in the detection order the period during which it applies,		According to this paragraph the period of application of detection orders shall not exceed maximum of 12 or 24 months. Could after this period another detection order

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
indicating the start date and the end date. The start date shall be set taking into account the time reasonably required for the provider to take the necessary measures to prepare the execution of the detection order. It shall not be earlier than three months from the date at which the provider received the detection order and not be later than 12 months from that date. The period of application of detection orders concerning the dissemination of known or new child sexual abuse material shall not exceed 24 months and that of detection orders concerning the solicitation of children shall not exceed 12 months		be issued? What measures are taken in that period to reduce CSAM on these services? We are concerned it would be disproportional to make obligations permanent through orders. This would make them legal obligations, which proportionality and impact needs to be properly assessed.
	10. The detection order shall not prohibit or weaken end-to-end encryption or oblige the service provider to provide encryption backdoors.	End-to-end encryption is an important tool to guarantee the security and confidentiality of the internet infrastructure and the communications of users. Any weakening of encryption could potentially be abused by malicious third parties. Therefore, end-to-end encryption should not be weakened. **Estonia does not support the possibility of creating backdoors for end-to-end encryption solutions.** At the same time, we can support the use of privacy enhancing technologies (PETs) that allow the analysis of encrypted content without decryption, so that the reliability, security and integrity of digital services relying on encryption is preserved.
Article 8 Additional rules regarding detection orders		
2. The order may also be transmitted in the language of the authority issuing the order, provided that it is accompanied by a translation of at least the most important elements necessary for the execution of the order into the language declared by the provider in accordance with article 23(3).		Unclear why this provision would be necessary since the detection order is issued by the competent authorities of the countries of establishment.

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
Article 10 Technologies and safeguards		
1. Providers of hosting services and providers of interpersonal communication services that have received a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46.		What are the technologies for detecting solicitation in e2e encrypted services? Are there technologies available today, which would enable monitoring e2e encrypted content without compromising the security and the integrity of these services? Does the service provider have to presume that it will be the subject of a detection order and thus, already when designing and developing a service, must implement backdoors for itself to monitor any and all communications or is the service provider allowed to design and develop services with absolute confidentiality for its users and worry about breaking this down only after receiving a detection order? In the cases in which gaining access to service's communication data would be technologically impossible due to the way the service is built (which might be the case for some e2e encrypted communications), would the service provider be at fault for not being able to comply with the detection order? Especially when the technologies made available by the EU Centre prove to be ineffective?
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).		How does this obligation relate to the obligation in art 18 of the DSA regulation to notify law enforcement authorities of a criminal offence involving a threat to the life or safety of a person or persons?

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
2. Where the provider submits a report pursuant to paragraph 1, it shall inform the user concerned, in accordance with the following sub-paragraphs 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 six 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. The time period of six months refered to in this subparagraph shall be extended by up to 6 months where so requested by the competent authority referred to in Article 48(6), point a. 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.		How does this obligation relate to the obligation in art 17 of the DSA regulation to provide a clear and specific statement of reasons to the users of any restrictions imposed regarding the content or the user account? According to this paragraph it could take up to six months before the user is informed. How does it affect the user transparency and effective means for redress? If the user does not know why their use of the services is restricted, they cannot contest it.
3. The provider shall establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to flag to the provider potential		How does this obligation relate to the obligation in art 16 of the DSA regulation to set up a notification mechanism? Are the providers obliged to set up two separate

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
online child sexual abuse on the service.		notification mechanisms – one for CSAM and another for other types of illegal content?
Article 14 Removal orders		
1. The competent authority of each Member State shall have the power to issue a removal order requiring a provider of hosting services under the jurisdiction of that Member State to remove or disable access in all Member States of one or more specific items of material that, after a diligent assessment, the competent authority or the judicial authorities or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material.		According to this article, only the Coordinating Authority of establishment can issue a removal order. How does this relate to art 9 of the DSA regulation where national judicial or administrative authorities from all Member States could order the service provider to act against illegal content? Why was a different approach chosen here compared to the DSA and TCO regulations?
Article 16 Blocking orders		
1. The competent authority ~~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.	1. The competent authority ~~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.	Internet access service providers should only be obliged to block access to the material provided to them by competent authorities. They should not be obliged to monitor and block new CSAM since they only provide access to the internet and have no means of controlling the content of websites. It must be considered that it is technically impossible for ISPs (internet service providers) to block access to a specific post, subsection or subpage of the website containing CSAM and they can only block the whole website or service. Is it considered proportionate for ISPs to block access to the whole webpage or service in case it contains CSAM? How is it provided that the blocking of access is proportionate?
~~6. The Coordinating Authority shall specify in the blocking order the period during which it applies, indicating the start date and the end date. The period of application of blocking orders shall not exceed five years.~~		Does the deletion of par 6 mean that blocking orders could be issued permanently? What measures are taken to reduce CSAM on these services? What measures are envisaged in this regulation? Need to assess the proportionality of a permanent obligation.

COMMISSION PROPOSAL	DRAFTING SUGESTIONS	COMMENTS
Article 17 Additional rules regarding blocking orders		
1.(a) (a) In case of known child sexual abuse material the reference to the list of uniform resource locators, provided by the EU Centre, ~~and the safeguards to be provided for, including the limits and safeguards specified pursuant to Article 16(5)~~ and, where applicable, the reporting requirements set pursuant to Article 18(6);	1.(a) (a) ~~In case of known child sexual abuse material the reference to~~ the list of uniform resource locators **of known child sexual abuse material**, provided by the EU Centre, **and the safeguards to be provided for, including the limits and safeguards specified pursuant to Article 16(5)** and, where applicable, the reporting requirements set pursuant to Article 18(6);	Concerned that this point is moving in the wrong detection as ISPs should be obliged to only remove known CSAM and the limits of their blocking capabilities must be taken into account.

FINLAND

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

We have serious concerns on the possible negative impact that CSA-proposal might have on the confidentiality of communications, including on the use of end-to-end encryption in electronic communication services. So far, this has remained unclear. Considering the importance of encryption to confidentiality of communications (respect for private or family life), freedom of speech, high level of data protection as well as cybersecurity, this Regulation's impact on end-to-end encryption should not remain unsatisfactorily ambiguous.

In the digital world, encryption of communication is central, as it secures digital systems on the one hand and protects privacy and personal data of the users on the other. Finland draws attention to the fact that the proposal's restrictions on strong encryption of electronic communications must not endanger cyber security or the security of communication and information systems. We are concerned about the impacts of the proposal on the use of strong encryption, which is an essential tool to guarantee trust in the online environment. In particular, we are worried that this proposal might lead to undermining the security of communication systems and services, and any backdoors for justified purposes could potentially be abused by malicious third parties.

We consider that more information should be obtained about the technical and organizational means behind the detection order during the negotiations. We encourage the Presidency/Commission to provide more information about measures and technologies that would not undermine use of encryption and would not jeopardize security of information services and systems, but that would help fight CSAM online. Finland believes that service providers must also have responsibilities in creating a safer online environment, and we would emphasis to place the responsibility on the providers.

Finland still has several reservations regarding Article 7 of the proposal. The proposal should be examined in more detail in relation to the Charter of Fundamental Rights of the EU in the negotiations. While existing case law of the ECJ does not include cases where the challenged legislation would be identical with the proposed regulation, there is already a series of judgments of relevance, as regards the general requirements applied to limiting fundamental rights under Article 52 of the Charter, including strict necessity and proportionality of the limitations on the relevant rights. See, in particular, Grand Chamber judgment of 8 April 2014, Digital Rights Ireland, in joined cases Joined Cases C- 293/12 and C- 594/12, and Grand Chamber judgment 21 December 2016, Tele2 Sverige AB, in Joined Cases C-203/15 and C-698/15 , as well as judgment of 6 October 2020, La Quadrature du Net and Others, C- 511/18, C- 512/18 and C- 520/18. Depending on the impact of the regulation on the confidentiality of communications, it seems there is also an apparent conflict with the Finnish Constitution.

2. *Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?*

Yes, FI supports exploring measures that could allow voluntary detection measures also in the future. The need for which the Temporary Regulation was drafted has not disappeared, and if the basis for voluntary detection measures is repealed, this would lead to the inconsistent requirements and processing in the EU, based on each member state's national legislation – exactly the reason why the Temporary Regulation exists.

FI is in favour of including the provisions of the Temporary Regulation to the CSA proposal – for example in connection with art. 4 risk mitigation measures. Voluntary measures could be implemented e.g. in cases, where the risk assessment indicates that there is a need for such detection. Also provision of voluntary measures should fully comply with the general requirements for limitation of fundamental rights, thus not only providing for a legal basis of processing but setting out the rules under which the voluntary measures may be taken.

The impacts of both voluntary and mandatory detection processes being in place at the same time must still be assessed. However, as the detection order is meant to be used only as the last resort, this should not lead to significant legal uncertainty – less intrusive measures must be exhausted before detection order could be issued. Also the aim of protecting children would support allowing voluntary measures to be implemented without waiting for the possibly lengthy process of issuing the detection order. Voluntary processing should be taken into account as a part of risk assessment and risk mitigation measures. Voluntary measures should not be as intrusive as mandatory detection measures.

3. *Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?*

The definitions of criminal offences should not be extended in substance in this Regulation from those defined in Directive 2011/93. We would therefore exclude amending to CSAM definition to audio communications in this Regulation.

4. *With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?*

FI supports the approach of the proposal that various service providers would assess their services and the risks related to their use, and that the service providers are encouraged to address these identified risks. These mitigation measures should be the primary measure to intervene in case of high risk services.

Firstly, we welcome that number-based services have been excluded from the scope of interpersonal communications. However, we still have reservations regarding the scope of Article 7 and its impact on the privacy and confidentiality of communications. The proposed regulation (Article 7) concludes that the detection order should be limited to what is "strictly necessary". Nevertheless, taking into consideration the vagueness of the key terms in Article 7 (e.g. "significant risk") and still open questions about technology, it remains unclear that the application of Article 7 together with Article 10 would not de facto result in a general monitoring obligation of private communications. In this respect, we have serious doubts regarding some elements of the detection order. These particularly relate to detecting new CSAM and solicitation of children. First, while it is clear that the proposed legislation has a legitimate aim, it is not clear how it is ensured that the means included in the proposed legislation for detecting new CSAM and solicitation of children is proportionate to the aim pursued. Also, we have some questions as to whether the detection order, in all respects, necessarily constitute an effective means to prevent CSAM. For instance, has the Commission analysed in the impact assessment, whether and to what extent there could be risks that criminals increasingly would start using other means not targeted by the Regulation, as knowledge of the new legislation spreads? It is also unclear to us to what extent other available measures that interfere less with fundamental rights have been taken into account in the impact assessment of the proposal.

While FI supports the goal of improving the protection of children against these particularly heinous crimes, the proposed regulation raises some unprecedented questions about general monitoring of confidential communications whose effect are not limited to this proposal. These questions should be very carefully and thoroughly scrutinized and the obligations imposed under this regulation have to be targeted both in text and in practice, ie. when these rules are actually applied.

GERMANY

General remarks

- We look forward to the upcoming meetings under the Swedish Presidency. We would like to submit the following general comments in advance.
- Combating the sexual abuse of children and young people has the highest priority for Germany's Federal Government. That is why the Federal Government has welcomed the Commission's proposal from the start as a shared European project which will create a clear and lasting legal basis. Establishing a single European regulatory framework with effective reporting channels and a new, independent and decentralised agency (EU Centre on Child Sexual Abuse) are crucial steps in the fight against the sexual abuse of children. As part of this effort, it is important to make the providers of relevant information society services more accountable.
- At the same time, the planned provisions of the CSA Regulation must uphold fundamental rights, in particular when it comes to protecting the confidentiality and privacy of communication. The Federal Government has serious concerns about the provisions on detection orders in the proposed Regulation. For the Federal Government, a high level of data protection and cyber security, including complete and secure end-to-end encryption in electronic communications, is essential. With this in mind, Germany believes it is necessary among other things to state in the draft text that no technologies will be used which disrupt, weaken, circumvent or modify encryption.
- This means that the draft text must be **revised** before Germany can accept it.

  We will submit these and other specific requests for revisions soon. The Federal Government will continue to contribute actively and constructively to the negotiations on the CSA Regulation.
- As the Federal Government has not yet completed its examination, we maintain our general **scrutiny reservation**.

Joint Opinion 4/2022 of EDPS and EDPB

Presentation by EDPS and exchange of views

- Germany thanks the European Data Protection Supervisor (EDPS) for participating in today's meeting of the Law Enforcement Working Party and for his comments on this important dossier.
- In Germany's view, the presentation raises the following questions in particular:
  - What is the EDPS's assessment of existing providers of age verification services (such as Privately or Yoti)?
  - Which age verification technologies requiring a minimum of data (apart from certified procedures such as eID) does the EDPS find preferable?
  - What does the EDPS think of using intermediaries to conduct trustworthy age verification that requires a minimum of data?
  - If the EDPS believes that the detection orders as provided for in the draft CSA Regulation do not comply with applicable law, we would be very interested in (technical and non-technical) alternatives which the EDPS finds suitable for protecting the rights of all users in the digital space, as well as the children and young people concerned.

- With regard to the legal basis for data protection in the CSA Regulation: Article 22 only explicitly governs the storage of data. It does not explicitly govern the collection of data, which necessarily precedes data storage. Does the EDPS believe that an explicit legal basis is needed in the CSA Regulation for the collection of data as well, or does the EDPS find the reliance on Article 6 (1) (c) of the General Data Protection Regulation permissible and sufficient? Looking in particular at Article 22 (1) (e) of the CSA Regulation, Germany questions whether the legal basis should be formulated more clearly.
- (Question for the Commission) In the Commission's view, what consequences will the EDPS's comments have for the law enforcement aspects of the proposed legislation, especially with regard to the proposed cooperation between the EU Centre and Europol? How does the Commission plan to deal with these consequences?

[*Positionierung zu Artikeln 1-11 sofern Debatte hierzu unter Anwesenheit des EDPS aufkommt]*

Article 2

- Article 2 (l), (j): We would like to repeat once again that the Regulation should take into account decisions of national legislators concerning the age of sexual consent and whether certain content and conduct is punishable. As they now stand, the definitions in Article 2 (l) mean that the CSA Regulation would also cover content and conduct which does not constitute a criminal offence in Germany. Further, we and other Member States are critical of raising the age of a "child user" to below 18 years. We therefore ask that inserting a national opening clause be considered with regard to the impunity of certain content and conduct under national law, and we refer to the proposed wording we have submitted for this purpose. We are very interested in the views of the other Member States.

Article 4:

- We are pleased that the Commission has indicated its openness to making the risk assessment requirements more specific. In the interest of legal certainty and predictability, we believe that providers and users alike should know which data and/or parameters the risk assessment is (or can be) based on and how they are weighted. We therefore agree with other Member States (such as Belgium) that have called for further specification of the proposed text.
- Article 4 (3): We would be interested in the EDPS's view of this provision as well.
- Mandatory age verification (according to Article 4 (3) and Article 6 (1) (c)) must allow for anonymous or at least pseudonymous use of the services in question.
- The Federal Government is testing whether pseudonymous age verification using electronic identification (eID) is permissible. We are very interested in the position of the EDPS in this context.

Article 7:

- The Federal Government has serious concerns about the provisions on detection orders in the proposed Regulation. The wording must be much more specific to ensure the greatest possible protection for all fundamental rights affected.

- This includes in particular specifying the undefined legal terms “significant risk” (Article 7 (3)) and “to an appreciable extent” (Article 7 (5), (6) and (7).
- The fundamental rights of users of information society services who receive a detection order must be considered along with the fundamental rights of children and young people affected by sexual abuse.

- With this in mind, we are currently carefully examining the conditions under which detection orders could be permitted and with which scope of application.
- We believe that audio communications should be removed from the scope of Article 7 of the proposed CSA Regulation.
- Whether detection orders can be permitted to apply to interpersonal communications services and personal cloud storage is currently being examined. Questions also arise with regard to new material and grooming.
- We would be very interested in hearing what other Member States think about possibly limiting the scope of detection orders.

Article 9:

- We have no objections to the revisions in Article 9 (2). If the majority agrees with these revisions, then in our view it will be necessary to revise similar wording in Article 15 (2), Article 18 (2) and Article 18c (2).

Article 10:

- As we have already explained, the Regulation must not lead to general interference with private, in particular encrypted, communication where there is no suspicion of wrongdoing, or to the weakening or circumvention of seamless and secure end-to-end encryption. We are currently examining the extent to which the scope of possible detection orders must be reduced to ensure that this is the case. The Federal Government is also in the process of testing suitable technologies. Germany believes it is necessary to state, for example in Article 10 (3) (a) (new), that no technologies will be used which disrupt, weaken, circumvent or modify encryption.
- We agree with Member States that have argued that detection technologies should be subject to stricter requirements.

Examination of the proposal as of Article 12 – 14143/22

Article 12:

- In our view, the reference to Article 48 (6) in Article 12 (2) is not entirely clear: we understand it to mean that the competent national authority would inform the EU Centre of such an extension, and the EU Centre would then receive the provider’s information.

Article 14:

- The new paragraph 3a in Article 14 resembles the provisions of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (TCO Regulation) dealing with cross-border matters. The new paragraph 3a does not seem very practical for purely domestic matters. We therefore ask for a review to determine whether the process described in Article 15 (1) could help.

- With regard to the revision in Article 14 (5), we would like to know whether the Coordinating Authority should nonetheless be informed that a removal order cannot be carried out. We assume that, in such a case, the competent authority issuing the order will inform the Coordinating Authority. It would therefore be preferable, as in the original text, if the provider (also) informed the Coordinating Authority directly.

Article 14a:

- We would like to point out that, unlike Article 14, Article 14a (2) explicitly provides for necessary measures to be taken to reinstate content or access to it if a removal order has been issued wrongfully. As we understand it, the provider must take such measures also in the case of Article 14. The wording in both articles should be revised to ensure consistency.
- It is also necessary to specify the length of time the data may be stored, when they are to be finally erased and at whose order.

Please note, the Federal Government has not yet completed its examination, we maintain our general scrutiny reservation.

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

The planned provisions of the CSA Regulation must uphold fundamental rights, in particular when it comes to protecting the confidentiality and privacy of communication. The Federal Government has serious concerns about the provisions on detection orders in the proposed Regulation. For the Federal Government, a high level of data protection and cyber security, including complete and secure end-to-end encryption in electronic communications, is essential. With this in mind, Germany believes it is necessary among other things to state in the draft text that no technologies will be used which disrupt, weaken, circumvent or modify encryption.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

As the Federal Government has not yet completed its examination, we maintain our general **scrutiny reservation**.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We believe that audio communications should be removed from the scope of Article 7 of the proposed CSA Regulation.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

Whether detection orders can be permitted to apply to interpersonal communications services and personal cloud storage is currently being examined. Questions also arise with regard to new material and grooming.

As the Federal Government has not yet completed its examination, we maintain our general scrutiny reservation.

HUNGARY

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

Hungary is committed to ensure the highest possible level of protection for children, and we agree that cooperation with companies is an essential part of the fight against such online content. We are concerned that end-to-end encryption, which is becoming more widespread, is also leading to a significant increase in the latency of online sexual exploitation offences. We must find a solution to this problem that is proportionate to the fundamental principles of privacy and data protection.

Our problems are not a necessary consequence of technological progress. Rather, it is the result of the full end-to-end encryption used by online platforms, which makes classic data interception activities via electronic communication service providers impossible.

In this context, new methods of data interception and access are needed to maintain law enforcement capabilities, based on cooperation with major international online platforms and smart device manufacturers.

Establishing national jurisdiction would be essential to ensure data interception and access for online platform providers and smart device manufacturers.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Yes, it is absolutely a crucial point. We suggest to prolong the TR, since we do not have any guarantee for finalizing the negotiations on the concerned instrument in time

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We are advised to strive for technology and format-neutral regulation. Only in this way can we create a timeless framework covering all CSAMs.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

The issue of access to encrypted content is currently being examined because of its complexity, on which we do not yet have an established position. This issue needs to be looked at more broadly, not just in relation to CSAs.

6. As regards detection orders concerning the dissemination of new 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 that, despite any mitigation measures that the provider may have taken or will take, the service is used, to an appreciable extent, for the dissemination of new 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 new child sexual abuse material;

(c) for services other than those enabling the live transmission of pornographic performances as defined in Article 2, point (e), of Directive 2011/93/EU:

(1) a detection order concerning the dissemination of known child sexual abuse material has been issued in respect of the service;

(2) the provider submitted a significant number of reports concerning known child sexual abuse material, detected through the measures taken to execute the detection order referred to in point (1), pursuant to Article 12.

7. As regards detection orders concerning the solicitation of children, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met:

(a) the provider qualifies as a provider of interpersonal communication services;

(b) it is likely that, despite any mitigation measures that the provider may have taken or will take, the service is used, to an appreciable extent, for the solicitation of children;

(c) 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 solicitation of children.

The detection orders concerning the solicitation of children shall apply only to interpersonal communications **between** ~~**where one of the users is**~~ a child user ~~and an adult~~.

Commented [TZ1]: We suggest to keep the original text, the new proposal makes be the regulation circumventable.

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;

( ) the source of the information (from the victim, from another person, as a result of technological detection or from another organisation or authority);

(c) all content data, ~~including images, videos and text~~;

(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 **of upload, with associated date and time zone, and port number**;

(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.

Commented [TZ2]: Identifying the source of the information may significantly support to establishing the likelihood of the abuse.

Commented [TZ3]: It is proposed to delete this section as it may lead to misunderstandings in the application of the Regulation. With the deletion, the definition of "content data" would be used by Article 2(s).

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 **competent authority issuing the order** ~~Coordinating Authority of establishment~~ of those grounds, using the template set out in Annex V.

   The time period set out in paragraph 21 ~~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 **competent authority issuing the order** ~~Coordinating Authority of establishment~~, using the template set out in Annex V.

   The time period set out in paragraph 21 ~~1~~ shall start to run as soon as the provider has received the necessary clarification.

7. The provider shall, without undue delay and using the template set out in Annex VI, inform the **competent authority**, **the** Coordinating Authority of establishment and the EU Centre, of the measures taken to execute the removal order, indicating, in particular, whether the provider removed the child sexual abuse material or disabled access thereto in all Member States and the date and time thereof.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annexes IV, V and VI where necessary to improve the templates in view of relevant technological developments or practical experiences gained.

Article 14a

Procedure for cross-border removal orders

1. **Subject to Article 14, where the hosting service provider does not have its main establishment or legal representative in the Member State of the competent authority that issued the removal order, that authority shall, simultaneously, submit a copy of the removal order to the Coordinating Authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established.**

2. **Where a hosting service provider receives a removal order as referred to in this Article, it shall take the measures provided for in Article 14 and take the necessary measures to be able to reinstate the content or access thereto, in accordance with paragraph 7 of this Article.**

3. **The Coordinating Authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established may, on its own initiative, within 72 hours of receiving the copy of the removal order in accordance with paragraph 1, scrutinise the removal order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter.**

Commented [TZ4]: Article 14a does not regulate the cross-border removal procedure for service providers who are not established in the EU and do not have a legal representative, although Article 33(2)(2) establishes the jurisdiction of the country of destination in such cases, and we therefore propose to add an article 14a.

Section 5
Blocking obligations

Article 16

Blocking orders

1. The **competent authority** ~~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.

The competent authority shall also have the power 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 with an unencrypted URI scheme 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 indicated by the uniform resource locators, regarding the provider's policy to address the risk of dissemination of the child sexual abuse material and regarding the provider's financial and technological capabilities and size;~~

~~(c) request the EU Centre to provide the necessary information, in particular explanations and assurances regarding the accuracy of the uniform resource locators in indicating child sexual abuse material, regarding the quantity and nature of that material and regarding the verifications by the EU Centre and the audits referred to in Article 36(2) and Article 46(7), respectively;~~

~~(d) request any other relevant public authority or relevant experts or entities to provide the necessary information.~~

Commented [TZ5]: Under Article 16(1)(2), the designated authority may order the blocking of all URLs on the EU Centre's list. As the list is likely to include URLs of content accessible via an encrypted protocol (HTTPS), which could only be achieved by blocking the entire domain included in the URL, together with a number of other potentially lawful content, it is proposed that it should not only be possible to block the entire list, but also a part of it that is not accessible via an encrypted protocol (HTTPS).

Formatted: Font: Not Bold, Not Italic, Font color: Auto, Not Highlight

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 **and 31** 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.

The Coordinating Authorities shall be free from any external influence~~, whether direct or indirect~~ and shall neither seek nor take instructions from any other public authority or any private party.

Commented [KSAd6]: The coordinating authority is likely to be a body funded from the state budget, so we would like to avoid any text that would give the opportunity to question its independence on this basis.

~~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;~~

~~(d) neither seek nor take instructions from any other public authority or any private party;~~

~~(e) are not charged with tasks relating to the prevention or combating of child sexual abuse, other than their tasks under this Regulation.~~

~~3. Paragraph 2 shall not prevent supervision of the Coordinating Authorities in accordance with national constitutional law, to the extent that such supervision does not affect their independence as required under this Regulation.~~

4. The Coordinating Authorities shall ensure that relevant members of staff have the required qualifications, experience~~, integrity~~ and technical skills to perform their duties.

5. The management and other staff of the Coordinating Authorities shall, in accordance with Union or national law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks. Member States shall ensure that the management and other staff are subject to rules guaranteeing that they can carry out their tasks in an objective, impartial and independent manner, in particular as regards their appointment, dismissal, remuneration and career prospects.

Section 2
Powers of Coordinating Authorities

Article 27

~~*Investigatory powers*~~ *Powers of inspection*

Commented [KSAd7]: These are not investigative powers in the classical sense, but rather administrative procedure. In our view, the current wording is not acceptable, even though the DSA regualtion contains this wording, as the DSA is not a law enforcement source of law.

1. Where needed for carrying out their tasks, Coordinating Authorities shall have the following powers of ~~investigation~~ inspection, in respect of providers of relevant information society services under the jurisdiction of the Member State that designated them:

   (a) the power to require those providers, as well as any other persons acting for purposes related to their trade, business, craft or profession that may reasonably be aware of information relating to a suspected infringement of this Regulation, to provide such information within a reasonable time period;

   (b) the power to carry out on-site inspections of any premises that those providers or the other persons referred to in point (a) use for purposes related to their trade, business, craft or profession, or to request other public authorities to do so, in order to examine, seize, take or obtain copies of information relating to a suspected infringement of this Regulation in any form, irrespective of the storage medium;

   (c) the power to ask any member of staff or representative of those providers or the other persons referred to in point (a) to give explanations in respect of any information relating to a suspected infringement of this Regulation and to record the answers;

   (d) the power to request information, including to assess whether the measures taken to execute a detection order, removal order or blocking order comply with the requirements of this Regulation.

2. Member States may grant additional ~~investive~~ ~~investigative~~ powers to the Coordinating Authorities.

3. Member States shall ensure that, where their law enforcement authorities receive a report of the dissemination of new child sexual abuse material or of the solicitation of children forwarded to them by the EU Centre in accordance with Article 48(3), a diligent assessment is conducted in accordance with paragraph 1 and, if the material 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 inspective~~investigatory~~ and enforcement measures to ensure compliance with this Regulation.

Commented [KSAd8]: What is the legal basis and information that allows the Commission 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 asses 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 inspections~~investigations~~

1. Coordinating Authorities may participate in joint ~~investigations~~inspections, 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~~inspections 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~~inspections 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.

IRELAND

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation ((EU) 2021/1232)?

The extent to which E2EE services are already being used to facilitate CSA, taken in conjunction with plans by major service providers to expand the use of E2EE, means that to exclude encrypted services from the Regulation would be to effectively turn our back on many cases of child sexual abuse and its victims. Ireland agrees with the principle that E2EE should not be prohibited or weakened, and we would be open therefore to considering the inclusion of a Recital and the precise wording thereof. We would be opposed, however, to including any wording that might have the effect of restricting the effectiveness of the Regulation, including in the context of future developments in detection technology.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

The current voluntary system of detection provides law enforcement agencies with invaluable information to counter child sexual abuse. Ireland believes that voluntary detection should continue until the CSA Regulation is in place and sufficient time has been allowed for the first risk assessment and mitigation processes to be completed and Detection Orders issued, if that is what the national competent authorities decide. We also believe that the feasibility of the continuation of voluntary detection as part of the new Regulation should be explored.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

This matter is being considered in Dublin. With reference to Regulation 2021/1232, we note that this applies only to number-independent electronic communications services.

In order to be able to respond to this question we are requesting clarification on the following points:

a. Is it the case that "interpersonal communications services" in the Regulation includes number-independent and number-based services, or only the former?

b. If number-based services are included, what is meant by "audio communications"? For example, does it include telephone calls?

c. In the context of number-independent services, what is meant by "audio communications"? For example, does it include WhatsApp audio calls? Or only voice notes/messages?

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

Given that a large proportion of reports of CSAM originate in interpersonal communications services, we believe that both interpersonal communications and publicly accessible content should remain within the scope of the proposal (but, in line with point (a) above, the definition of interpersonal communications service has to be clarified).

Ireland comments on Articles 12 to 15

Article 12 Reporting obligations

We support the current text in 12(1) and (2) – the service provider should make reports to the EU Centre; the service provider should inform the user of a report when it has permission to do so. We could support a further extension of the time available to law enforcement agencies to investigate before the user is informed.

In relation to 12(3), we know that making reporting easier can make a practical difference to preventing and combatting child sexual abuse, including grooming. Reporting mechanisms can benefit from co-design with stakeholders, including children. As previously suggested, we would recommend providing for the establishment of an industry standard for this process.

Article 13 Specific requirements for reporting

Ireland supports the retention of the word "all" in 13(1)(c) and (d). From a drafting perspective, the meaning might be made clearer by the deletion of the words "available data other than content" in (d).

Article 14 Removal orders

In general, Ireland is in favour of simplifying and streamlining the procedures set out in the Regulation where that is possible.

Ireland can support the addition of cross-border removal orders (Article 14a) if that is the consensus view. This can be achieved by deleting the words "**under the jurisdiction of that Member State**" from 14(1).

Suggested wording

1. The competent authority of each Member State shall have the power to issue a removal order requiring a provider of hosting services ~~under the jurisdiction of that Member State~~ to remove or disable access in all Member States of one or more specific items of material *that, after a diligent assessment, the* ***competent authority*** *~~Coordinating Authority~~ or the ~~courts~~* ***judicial authorities*** *or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material.*

We do not regard the scrutiny provision set out in paragraph 14(3a) as necessary, given the opportunities for redress in Article 15. We can support the retention of the first sentence in 14(3a).

See below for a possible addition to Article 14 that relates to Articles 14 and 14a.

Article 14a Procedure for cross-border removal orders

We do not regard Article 14a as necessary and would favour deletion or a complete reworking to make it less complicated and more complementary to the CSA Regulation. In particular, we cannot accept 14a(4).

14a recreates the mechanism for cross-border removal orders set out in the TCO Regulation. However, the CSA Regulation is quite different from the TCOR, and CSAM is different to terrorist content.

In line with 14a(3), we can accept a role for Coordinating Authorities of establishment to assess, on their own initiative, whether such orders seriously or manifestly infringe the Regulation/Charter. But we cannot accept a role for Coordinating Authorities of establishment in adjudicating on complaints from hosting service providers or content providers about cross-border removal orders. Such as role is unnecessary and no reason has been provided for it.

If hosting service providers or content providers wish to object to a Removal Order, it should be dealt with by the authorities or the courts of the Member State who identified the material as CSAM and issued the Removal Order.

There are several other reasons in support of our position:

- The procedures in Article 14a give rights to hosting service providers and content providers in relation to cross-border removal orders that we do not give to them in relation to domestic removal orders. [If a hosting service provider/content provider objects to a cross-border removal order they will have a reasoned decision in 72 hours; if it is a domestic removal order there is no equivalent process or guarantee.]
- We should not be adding further layers of complexity to an already complicated Regulation.
- Terrorist content can much more easily be confused with extreme but lawful politics, satire or journalism, and is more likely to engage ideas of free speech, which might justify an additional layer of scrutiny. CSAM is in a different category.
- It goes against ideas of mutual trust to empower the Coordinating Authority in one MS to overrule the competent authority in another. The authorities and courts of the issuing Member State are best placed to scrutinize Removal Orders and to provide remedies to content providers and hosting service providers affected by the Removal Orders they have issued.
- It is more likely that the content provider will reside in the Member State issuing the Removal Order and be better able to access justice there.

We propose therefore deleting Article 14a or, as a fallback, the deletion of 14a(4).

Drafting proposal

If it is helpful, one option the Presidency could consider, in place of unwieldy new provisions for scrutiny of cross-border removal orders, is the provision of an administrative review mechanism for all removal orders (domestic and cross-border). This could perhaps be added to Article 14:

1. **The competent authority that issued the removal order shall provide a mechanism for administrative review of the order. Such reviews may provide for the revocation, withdrawal or amendment by the competent authority of an order or decision. Such reviews may be initiated by application from the affected provider or affected user [not later than X months after the order has been issued].**
2. **Where the competent authority that issued the removal order is not the Coordinating Authority, the competent authority that issued the removal order shall inform the Coordinating Authority of any reviews sought under the first sub-paragraph and the outcome thereof.**
3. **The provision of an administrative review mechanism shall not affect any of the rights extended to providers and users under Article 15.**

ITALY

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

Even if we gave for granted that the tools used by the providers could theoretically identify CSA material, also with regard to the encrypted communications, imposing an obligation to verify automatically them, appears to be a disproportionate measure, as it would represent a generalized control on all the encrypted correspondence sent through the web. The present detecting activity, carried out on a voluntary scan, seems to provide a good balance with privacy. therefore, it might appear inappropriate to alter this system, because it would imply the risk of new limitations on file detecting. Besides, the automatic scan would reveal such a huge number of images, that it would be hard to handle with, also due to the related considerable amount of false positives thus impacting on the effectiveness of the Police activity, as well as privacy

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

We are in favour of continuing with voluntary detection, which has produced excellent results, without jeopardizing the privacy to communications. We could include this content in the final draft, putting aside the mandatory detection.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

With regard to vocal messages, we deem that, by their nature they could not be considered CSA material, but elements supporting the suspicion of grooming. In order to consider vocal messages CSAM, they must be contextualized.

Besides, considering the vocal messages as CSAM, it would mean an unlimited access to all the vocal registration exchanged in ordinary communications.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content.

It would be better to have a detection activity including also interpersonal communications, in order to identify timely grooming

LITHUANIA

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

The EDPS opinion absolutes the protection of rights, does not strike a balance between the tools available to law enforcement and the enforcement of privacy, thus putting children at risk of not being protected online. Law enforcement activities are subject to strict requirements and therefore the presumption of mistrust in law enforcement should not be formulated by imposing excessive restrictions. The business is profit oriented, so too much confidence in their self-regulatory mechanisms posses. It should also be noted that the self-regulatory mechanism of large companies may be sufficient, but the self-regulatory mechanism for smaller companies is questionable.

In our opinion Access to encrypted content is acceptable, failing which it will be "hosting" cases of child abuse online.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Lithuania is in favour of voluntary detection, and we would like to include it in the CSA proposal, as we do think that the broader scope of cooperation with different stakeholders, e.g. hotlines, have shown in practise of various MS that is extremely valuable in detecting such crimes.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

Regarding audio communications, we note that we support its inclusion in the scope of the CSA proposal. It is worth to mention, that audio communications are usually encrypted and also may be additional material to investigate CSA cases.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

Interpersonal communication is acceptable, it can be important evidence in investigation. What is more, "grooming" is also the object of the CSA.

Lithuania does not have drafting suggestions and comments on Articles 12 to 15 of doc. 14143/22.

MALTA

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

Malta continues to note the sensitivity of the proceedings on combatting child sexual abuse while complying with fundamental human rights. Significant legal risk is being envisaged if the Proposal is passed as it stands. Nevertheless, there are valid arguments allowing for detection orders and ensuing decryption of communications, in view that, law enforcement authorities across the EU continue to struggle against investigating and prosecuting this crime without access to the illicit content itself. The question is whether other alternative options which are proportional and necessary can be tabled to reach the general objective of this regulation to facilitate law enforcement work in combatting this crime.

Malta expresses concern in view of, as stated in the EDPS's opinion that there are no comparable cases on the envisaged encroachment to the confidentiality of communications and ensuing protection of fundamental human rights under the case law of the Court of Justice of the EU. If it is irrelevant to distinguish the proposed targeted monitoring from general and indiscriminate monitoring as explained by the Council Legal Service, Malta questions whether the current text is suitable if it may be successfully challenged in front of the Court of Justice on the basis of general and indiscriminate monitoring with the pertinent articles being declared null and void. Therefore, Malta agrees in principle that while combatting child sexual abuse, measures which undermine fundamental human rights should be examined further and if necessary, substantive safeguards should be added to the procedure suggested for detection orders.

Nevertheless, Malta would like to understand further how the derogation for service providers to voluntarily detect under the Interim Regulation has worked in relation to the wording under recital 25. Malta would be in favour of using the already established recital 25 in Regulation 2021/1232. This could be one of the substantive safeguards which could lead to a compromise on this issue. Malta calls for alternative solutions which will not indiscriminately interfere with encryption of telecommunication means.

Furthermore, Malta wishes to ask the Commission about how less effective the Proposal would be, if detection orders would be altogether removed and obligations emanating from risk assessments including mitigation measures be respected. Malta is basing this reasoning on paragraphs 47 and 48 of the EDPS Opinion following Austria's intervention on this possibly being the next best measure before detection orders. If restrictive mitigation measures may be enhanced by empowering further Coordinating Authorities to independently enforce such measures, detection orders may then no longer be required.

Lastly, providing such an exemption in this Proposal could set a precedent in other fora. It could be possible to consider access to encrypted data on illicit content in terms of law enforcement in a dedicated legislative proposal and in conjunction with other Council preparatory bodies. Malta therefore supports the Estonian intervention about caution to avoid unforeseen precedents in others areas and wishes to see discussion in such other bodies.

Malta also wishes to support the Danish intervention in the first session of the LEWP meeting which cautioned against a possible disturbance in law enforcement acting on CSAM in view of the judicial review process under the detection orders. In Malta, child protection authorities and law enforcement authorities work effectively and efficiently together to act on reports of child sexual abuse online. It reiterates therefore that national established structures and their effectiveness should be respected throughout the negotiations of the Proposal. Malta continues to support emphasis on the importance of hotlines integrated within national systems.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Malta would be in favour of this option although note is taken of the Commission's explanation that if such detection continues to be voluntary it would undermine the single digital market. Malta would like to point out that in this Council preparatory body, precedence should be given to efforts to combat the specific crime-type being discussed. It questions therefore the suitability of the forum to entertain discussion pertaining to the single digital market. If voluntary detection is a possibility, then Malta considers that this working group should continue discussion on this front, even more so in view of the fact that service providers are actively engaged in voluntary detection with the blessing of Member States.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

The Malta position on including audio communications is not yet finalised largely for the matter that it remains undecided on the implications of the Proposal if encryption is undermined.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

In view of the fact that a large amount of illicit CSA material is distributed via providers of interpersonal communication services, it would not follow to limit such orders to providers of hosting services and publicly assessable content only. Nevertheless, the Council Legal Service has advised that there is significant legal risk in introducing detection orders in the private domain.

THE NETHERLANDS

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

The Regulation holds no obligation for providers to decrypt information on their servers at any stage of the procedure.[1] Such an obligation to decrypt information is neither desirable *nor necessary* in order for providers to comply with all of their obligations under the CSAM Regulation. Currently, subject to further research regarding their successful deployment on a large scale, there are two technologies which may allow for automatic detection of CSAM while at the same time leaving end-to-end encryption intact. They are described in the Commission's impact assessment on page 309 under 4 (a) (for old material) and 4 (d) (for new material). These are both on-device solutions where there is no third party involved. The way they work is that CSAM is detected *before* the material is encrypted and sent to one or more recipients. This technology, in a way, functions somewhat similar to how spam is detected or 'auto-correct' dictionaries function on most phones today.[2]

Any technology used to detect CSAM will likely be expensive. Many companies will therefore be bound to use the technology provided for by or through the Commission in order to comply with their obligations under the Regulation. While recital 25 of Regulation (EU) 2021/1232 touches on the importance of end-to-end encryption, it does not actually prevent the scenario by which, in practice, a company is stuck using an expensive technology (developed or offered by the Commission or a subsidiary body) that is incompatible with its end-to-end encryption software or its software in general. That is why, during previous sessions of the LEWP on October 19 and November 24, as well as during its last session held in January, the Netherlands proposed adding the following text to article 10 sub 3 of the Regulation:

> "no technologies that make end-to-end encryption impossible".

On 5 July 2022, our Parliament has adopted a resolution specifically instructing the Dutch government not to accept proposals which make end-to-end encryption impossible. Our parliament and government wish to prevent the practical outcome by which – even if this was wholly unintended from the outset - companies are forced to disable their end-to-end encryption because it is incompatible with technology (i.e. software offered by or through the EU-centre) necessary to detect CSAM. It is, therefore, of key importance to the Netherlands that this concern is addressed in the Regulation itself.

The Netherlands is aware that the CSAM Regulation aims to be 'technology-neutral' and, as such, applauds this concept. However, it stresses that this does not mean the technologies used should not comply with basis minimum standards set in advance by the Member States[3]. These criteria are meant to serve as a minimum floor to which the technologies offered by or through the Commission

[1] In the case of end-to-end encryption services, most service providers would not be able to carry out such an obligation as they are unable to access this information themselves.

[2] This paragraph, *inter alia*, describes the possibility of detecting new material through the technologies provided for in the impact assessment while leaving end-to-end encryption intact. As described elsewhere, the Netherlands has serious concerns regarding the detection of new material as well as the range of materials falling within the scope of the detection order (e.g. the inclusion of "voice" in article 2 (s) of the Regulation).

[3] Another example of such a criterium for the technology used could be that it 'should not result in racial bias'. This criterium **does not impose any technical requirement on the technology itself**, but it requires that the results rendered using the technology to comply with certain basic minimum (in this example: human rights) standards.

should comply. It would therefore encourage the Presidency and Member States to ponder on such requirements, as they can prevent any patently unwanted outcomes from the use of these technologies in the future.

Alternatively, if for any reason the Commission or the Member States should be unwilling to include the proposed text in Article 10 of the Regulation, the Netherlands urges that recital 25 is strengthened so that its concerns are appropriately addressed. This could, for example, be achieved by adding the following text to recital 25:

> "End-to-end encryption is an important tool to guarantee the security, integrity and confidentiality of the communications of users, including those of children. Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption. **Any technology developed to detect CSAM as a result of this Regulation shall be fully compatible with the use of end-to-end encryption.**

Due to time constraints, the Dutch government reserves the possibility of proposing additional text to this recital to ensure that its concerns and that of its Parliament are adequately addressed.

2. *Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?*

The Netherlands is in favour of exploring if voluntary detection should be continued. The purpose of detecting **known material** is to clean the internet of such material and prevent repeated victimisation. Companies that want to voluntarily contribute to this important aspect in the fight against CSAM should be encouraged to do so. This principle has also been recognized in article 7 of the recently adopted Digital Services Act, that allows for voluntary detection of online illegal content. The Netherlands would like to stress that the aim should be to encourage companies to voluntarily detect material or to investigate, subject to the other requirements of the DSA. These positive initiatives should not be discouraged by the threat of legal action. Once providers are aware that there is a possibility such material is hosted by them, for example following the risk assessment in Article 3 of the proposed regulation, further investigation should be encouraged instead of turning away from it. In voluntary detection, it is also important to consider freedom of expression, right to privacy and respect for one's private life. Moreover, it is necessary to contemplate countering chilling effects.

On national level we have good experiences with voluntary detection and public-private partnership. The last few years the Netherlands has invested heavily in the cooperation with the sector. Our Dutch Online Child Abuse Expert Office (EOKM) has been recognized by all parties a 'trusted flagger' to report child sexual abuse material to the online service company and/or law enforcement requesting its removal from access and circulation. The sector has signed a covenant stating that a report of CSAM will always be followed up within 24 hours. In addition, the companies are offered a HashCheckService which is an instrument that help hosting providers keep their servers clean. It is a free service that allows ICT companies to voluntarily scan their servers with hashes for known CSAM. The Dutch Technical University Delft developed special monitoring software that traces notifications of CSAM from the EOKM. This tool can accurately identify who is hosting CSAM, where it is stored, how long it has been available online after a notification and how many CSAM is circulating online. The monitor has shown that 87% of the reports of CSAM sent by the EOKM are followed up by companies with the removal of the content within 24 hours.

3. *Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?*

The Netherlands has serious concerns regarding the inclusion of voice communication in the scope of the CSA proposal. Similar to grooming, voice detection is complex because it involves spoken words whose content and interpretation depend on context. Annex 9 to the impact assessment also does not foresee in any technology regarding the analysis of, for example, encrypted voice communications. Absent any information in this regard, the Netherlands is concerned that the automatic analysis of all voice communications would in and of itself be disproportional to the purpose it intends to serve. In addition, in the case of end-to-end encrypted voice communications, it most likely will also require measures that are inconsistent with the European Court's jurisprudence on data retention.[4] As far as the Netherlands is concerned, the detection order for voice communications does not meet the requirements of necessity and proportionality and cannot remain in the scope of the Regulation.

4. *With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?*

The Netherlands supports the premise from the proposal that providers of hosting services and interpersonal communication providers have a responsibility in preventing and combating online child sexual abuse. At the same time, the measures in the proposed regulation infringe on a number of fundamental rights. An infringement of fundamental rights is only allowed if it is necessary (relevant to achieve the intended purpose) and meets the requirements of proportionality (is the interest proportionate to the infringement) and subsidiarity (can the purpose also be achieved by a less intrusive means).

With a view to detecting known CSAM, the Netherlands is open to explore detection performed on interpersonal communications and publicly accessible content. The detection order for **known CSAM** at providers of hosting service and interpersonal communication providers violates a number of fundamental rights. However, if the detection is done by hashing the Netherlands is open to explore the possibilities of hashing and under which conditions detection should be done. In the case of providers of hosting service, according to the Dutch constitution an expression may not be prohibited in advance solely on the basis of its content. The detection order should not require the use of an upload filter. For detection on interpersonal communication infringement is more severe than for detection performed on hosting services. The conditions under which infringement can be justified should be examined. The criteria in the proposed regulation are currently too vague and the timeframe is too long.

According to our technical experts 'on device detection' is the only form of detection where end-to-end encryption may not be compromised. This means that in Annex 9 of the Impact Assessment, only options 4a and 4d remain as techniques worthy of further investigation. For the public part of the internet, the criteria in Article 7 ("it is likely", "to an appreciable extent") should be more clearly defined. In addition, the duration of 24 months is too long for such a far-reaching infringement. Moreover, safeguards should be included on the uploader's side conform Digital Service Act).

[4] This would be the case if, for example, the technology requires voice communications to be translated immediately to text in order to function in an end-to-end encrypted environment. The Netherlands wonders where and how that text would subsequently be stored and reserves the right to ask further questions to the Commission regarding the technical background on this part of the proposed Regulation.

In general terms, for the detection of **new CSAM** by providers of hosting services and interpersonal communication providers, whether an infringement is justified depends heavily on the substantiation of necessity in that case and the reliability of the technology used (and thus proportionality). The Netherlands strongly doubts that necessity and proportionality can be sufficiently substantiated, given the currently available technologies.

While the Netherlands will continue to combat **grooming** - a particularly egregious crime which deeply impacts many young victims' lives - in any way it can, it finds that the detection order for grooming by interpersonal communication providers simply does not meet the requirements of necessity and proportionality and cannot remain in the scope of the Regulation.

Additional comments based on the discussions in the LEWP on 19 and 20 January 2023

Article 10 (3)

The Netherlands wants to tackle CSAM effectively, but for the Netherlands it is very important that end-to-end encryption is not made impossible. We would like to do a text suggestion, as we think it is important that this is specified in the regulation. We suggest adding the following text to **Article 10(3)**:

(e) no technologies that make end-to-end encryption impossible.

Article 12

2. Where the provider submits a report pursuant to paragraph 1, it shall inform the user concerned, **in accordance with the following sub-paragraphs** 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 **six** ~~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. **The time period of six months refered to in this subparagraph shall be extended by up to 6 months where so requested by the competent authority referred to in Article 48(6), point a.**

   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.

The Presidency suggested that the notification to inform the user should be done by the Coordinating Authority instead of the provider. Under the first paragraph of Article 12, a notification from the provider should go to the EU centre. The Coordinating Authority is not informed of the notification. If we want the Coordinating Authority to inform the user, it needs to be arranged that the Coordinating Authority is aware of the notification.

Article 13 (1)(c)(d)

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:

   (c) all **relevant** content data, including images, videos and text;

   (d) all available **relevant** data other than content data related to the potential online child sexual abuse;

Article 14 (1)

The Netherlands is in favor of simplifying the process of the removal order. However, the question is whether the proposed process of the Presidency in article 14 is legally possible and does not violate our constitution. The Presidency didn't adopt the Netherlands' earlier comments on the revised text of Article 14. We would kindly ask to reconsider this.

An important distinction can be made between information on the internet that is available to the public and information that is not. Regarding the latter, the Dutch Constitution consists of the right to freedom of 'telecommunication'. The provision concerning this right only allows this right to be infringed after a prior decision by a judge.

When assessing the new proposal of the text of Article 14, concerning the rules about the removal order, a key basis for the Netherlands is that removal orders can only be issued by the Coordinating Authority if the order is limited to material that is available to the public. If the revised text of Article 14 also enables Coordinating Authorities to issue removal orders with regard to material not available to the public, the Netherlands cannot support it.

It is for this reason that the Netherlands proposes to amend the text of Article 14, Paragraph 1, as follows:

> **The competent authority of each Member State shall have the power to issue a removal order requiring a provider of hosting services which stores and disseminates information to the public under the jurisdiction of that Member State to remove or disable access in all Member States of one or more specific items of material** that, after a diligent assessment, the **competent authority** ~~Coordinating Authority~~ or the ~~courts~~ **judicial authorities** or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material.

The Netherlands prefers to include either Article 14a in the regulation or to remove the cross-border option. The question is whether every country will judge the same whether something is CSAM or not. Therefore, The Netherlands wants to maintain **under the jurisdiction of that Member State** in article 14 (1).

2. The provider shall execute the removal order as soon as possible and in any event within 24 hours of receipt thereof.

The Netherlands wants to maintain the Commission's text proposal, where providers execute a removal order as soon as possible and in any event within 24 hours. SMEs do not always have 24-hour staffing. This would mean that these companies would be unable to comply with the Regulation from the start. According to the Netherlands, that is not the intention of the Regulation. The purpose of the Regulation is, among other things, to prevent the spread of CSAM. All companies should have the opportunity to be able to comply with the Regulation. According to the Netherlands, the execution of a removal order within 1 hour is not feasible. The norm should be that once providers have become aware of CSAM on their services they remove it as soon as possible with a maximum of 24 hours.

POLAND

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

We are in favour of including in the Regulation provisions aimed at avoiding the weakening of end-to-end encryption. The development of this technology is key to ensuring secure communications in the European Union. Its role is highlighted in the NIS2 Directive, which, in recital 98, indicates that encryption should be developed and promoted. In addition, this directive requires key actors to have a cryptography policy in place. Therefore, provisions should not be introduced that may jeopardise the achievement of the objectives of NIS2 directive. However, protecting E2EE should not be absolute and exposing children to threats. There are two important instances where E2EE can be lifted:

1. It should be made possible for the parent or the legal guardian to make an informed choice to decrypt the communication of the child being their own or under legal care.
2. By court order

In PL's view no other concessions should be made in order to weaken encryption. Going further would probably add to creating backdoors to undermine E2EE.

Suggested wording for a recital in CSA based on recital 25 of temporary regulation could be as follows:

> ”End-to-end encryption is a key ~~important~~ tool to guarantee the security and confidentiality of the communications of users, including those of children. However, given that nothing in this Regulation should be interpreted as prohibiting or weakening end-to-end encryption, the practical application of this tool should always take into account the best interest of children, in particular those who are victims of sexual exploitation and sexual abuse ”.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

We find voluntary action by industry to detect and remove CSAM very valuable and in our opinion a legal basis for such action should remain in force. In this respect, it is crucial to ensure that such legal basis is in place uninterruptedly until the CSA Regulation comes into force. We should avoid the gap between the termination of temporary regulation and entering into force new requirements from CSA. Therefore, in such circumstances we would exceptionally support extending the application of Regulation (EU) 2021/1232. Ultimately, however, all solutions to fight CSAM should be contained in a single piece of legislation. In the further course of legislative work, we propose to include voluntary detection in CSA regulation as a permanent option, parallel to the obligatory detection. The process of voluntary detection should be as transparent as possible, under the guidance provided by new EU Centre. The temporary regulation could be prolonged only if, the CSA legislation process and its application is not completed before August 2024.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

PL supports the initial Commission's proposal as regards the scope of CSA, which does not include exceptions for audio communications. As far as we understand the current wording of CSA proposal, audio is included likewise any other content data. In our view, audio communication could be covered by the CSA Regulation, especially as this type of service is offered by popular messenger services. PL considers that the risk of solicitation or exploitation of children in audio communication is comparable to the other forms of communication and there are already identified cases of such offences. At the same time, however, this means that more technologies need to be adapted to scan another form of communication. If this is easily achievable and does not distort competition in the market then it could be covered by the CSA regulation.

In this context, as far as reporting obligations are concerned, PL supports deleting "*including images, videos and text*" from art. 13 (1) (c) and keeping the current reference to the definition of *content data* from e-evidence Regulation in art. 2 (s) which means "*any data in a digital format, such as text, voice, videos, images and sound, other than subscriber or traffic data"*.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

In our view, such narrowing of the scope of this document would be excessive and would not realistically address the problem of CSAM on the Internet. This change would completely exclude cases of grooming from the scope of this regulation. In addition, interpersonal communications may include the transmission of files containing CSAM, which would hardly be considered publicly available. Consequently, narrowing the scope of the regulation would take a significant part of CSAM material out of the scope of this legislation. Therefore we oppose to suggested limitation.

The exchange of CSAM and grooming take place as parts of the exchange of broadly understood interpersonal communication, and not in a public domain. Focusing only on "public environment" undermines the effectiveness of the activities carried out. PL does not find any justification for such limitation. It should be strongly emphasized that both interpersonal communication and public accessible content should be taken into account when developing detection measures.

Articles

- **art. 7 (*detection orders*) -** There is a risk, that the reasons for issuing the detection order could not outweigh the 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 (including right to privacy). We share the doubts presented by the EDPB and EDPS which observed in their respective opinion that even with the specifications in Article 7(5)-(7) of the Proposal, the conditions for the issuance of a detection order are dominated by vague legal terms, such as 'appreciable extent', 'significant number'.

  It is to be highlighted that vague notions make it difficult for providers, as well as for the competent judicial or other independent administrative authority empowered, to apply the legal requirements introduced by the Proposal in a predictable and non-arbitrary manner.

Appropriate safeguards are needed. The technologies detecting new CSAM and online grooming are continuously improving, however, given their current shape their application may lead to more challenging enforcement than for known CSAM. Reliance on such technologies may result in potential for actions against users, interfering with their privacy and data protection rights. Therefore, we see the need for further in-depth discussion on the proposed provisions of Article 7.

We support the continuation of work on the content of the regulation in order to develop solutions that will allow effective detection of cases of sexual abuse and sexual exploitation of children, and at the same time will not undermine the rights and freedoms of citizens. Moreover, it is also not clear which specific technologies will be chosen by service providers, which will make it difficult to assess in advance whether they do not violate civil rights and freedoms. Therefore, we propose to link the discussion on Art. 7 with articles on applied CSAM material detection technologies (e.g. Articles 10 and 50).

- **art. 12 (3) - (r*eporting obligations*)** – PL suggests adding the word "effective" as follows: "the provider shall establish and operate an accessible, effective, age-appropriate and user-friendly mechanism that allows users to flag to the provider potential online child sexual abuse on the service.;
- **art. 13 (1) (c) (r*eporting obligations*)** – we support HU proposal to delete "*including images, videos and text*";
- **art. 14 (3a) – (r*emoval obligations*)** – Bearing in mind the outcome of the discussion during the last LEWP meeting and already mentioned doubts concerning the mutual relations between the competent authority and Coordinating Authority at the national level, PL suggests to leave in para. 3a. only the first sentence, namely: "If the competent authority issuing the removal order is not designated as the Coordinating Authority of its Member State, it shall address a copy of the removal order to its Coordinating Authority without undue delay". The rest of para 3a in art 14 should be deleted;

  general remark on orders and relation with DSA – PL is of the opinion that further elaboration is required as regards mutual relations between Coordinating Authority from CSA and Digital Services Coordinator from DSA. It may turn out a bit challenging if a Member State decide to separate this functions or establish two different authorities. For example, according to art. 8 para. 3 DSC is obliged to send a copy of an order to all other Digital Services Coordinators. Therefore it is worth to consider to include in the text an obligation for coordinating authority to inform not only CA but also DSC about the issuance of an order. It can be done also during the implementation of regulation at the national level, however has to be taken into account in order to ensure coherence.
- **art. 14a (cross-border removal orders) -** PL supports other Member State's voices aiming at simplification of the procedure; issue requires further elaboration;

- **art. 16 (4)** (*blocking orders)* - by analogy to art. 14 (3a) – there should be no scrutiny procedure conducted by Coordinating Authority with reference to orders issued by competent authority.
- **art. 17(3)** (***blocking orders***) - the term "where relevant", which refers to the obligation to communicate, seems problematic (*Where relevant, the blocking order shall also be communicated to the providers of online search engines under the jurisdiction of the competent authority*) and may be considered unclear. To enhance the effectiveness of Art. 17, we propose to delete “where relevant”;
- **art. 19** (***Liability of providers***), we suggest including "if"; related to the need to show good will. Exclusion of liability as referred to in art. 19 (*Providers of relevant information society services shall not be liable for child sexual abuse offenses solely because they carry out*) should depend on the "good will of the service provider", and not only on the "mere fact of the actions taken", as they may be façade. In this case, the regulation will be ineffective and its implementation will be entirely dependent on individual providers, so it is proposed to modify the wording e.g. as follows: “Providers of relevant information society services shall not be liable for child sexual abuse offenses if they carry out, in good faith, the necessary activities to comply with the requirements of this Regulation (...).

ROMANIA

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

If there is serious concern that someone is using end-to-end encryption (e2ee) to facilitate crimes, we agree that law enforcement agencies should use legal tools to try to stop this type of crime and apprehend the individual. These may include obtaining a warrant to search the individual's property or devices for evidence, using court-ordered surveillance to monitor the individual's online activity, or working with internet service providers or technology companies to gain access to the individual's encrypted communications. Additionally, law enforcement agencies could also use decryption tools or techniques to try to gain access to the individual's encrypted communications.

The extent to which encrypted child sexual abuse material (CSA) can be affected by a detection order depends on the specific details of the order and the technology used to encrypt the material.

If the encryption used is relatively weak and easily broken, a detection order may allow law enforcement agencies to gain access to the encrypted CSA material. In this case, the detection order would be an effective tool for detecting and investigating the distribution of CSA.

However, if the encryption used is strong and difficult to break, a detection order alone may not be sufficient to gain access to the encrypted CSA material. In this case, law enforcement agencies may need to use other legal tools or techniques, such as working with internet service providers or technology companies, to try to gain access to the material.

It is known that some countries have laws that would force companies to decrypt data on demand with a legal order, which are known as "backdoors" or "exceptional access". Also, experts argue that these methods weaken the security overall, as they would require the creation of vulnerabilities in encryption technology that could be exploited not only by authorized government agencies but also by malicious actors.

Ultimately, the effectiveness of a detection order in relation to encrypted CSA material will depend on the specific circumstances of the case and the technology used to encrypt the material.

We agree that nothing in the proposed CSA Regulation should be interpreted as prohibiting or weakening end-to-end encryption, but also we don’t want that E2EE encryption to become a “safe haven” for malicious actors. Therefore, we tip the scales towards protecting children.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Voluntary detection of child sexual abuse material (CSA) by internet service providers and technology companies has been seen as a way to proactively identify and remove illegal content from their platforms. It is a complex and ongoing process, and companies may face challenges in identifying and removing all illegal content from their platforms.

We agree that these voluntary efforts, should be continued and strengthened with support from law enforcements agencies, in order to help reduce the availability of CSA on the internet and make it harder for individuals to access and distribute illegal content.

The crimes regarding CSA materials are serious ones, and it's crucial that the agencies in charge of investigating and prosecuting these crimes have the necessary resources and all the help and support to do so.

Therefore, we agree that voluntary detection should be continued whether is extended through the Temporary Regulation (EU) 2021/1232 or is included in the CSA proposal.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

Including audio communications in the scope of detecting child sexual abuse material (CSA) can be a challenging task, as audio files may not contain the same visual indicators that are present in images or videos. Additionally, the detection of CSA in audio files can be hindered by factors such as background noise, poor audio quality, and encryption.

However, there are technologies and techniques that can be used to detect CSA in audio files. These can include:

- Audio Fingerprinting: This technique involves creating a unique "fingerprint" of an audio file, which can be used to identify and match the file against a database of known CSA.
- Speech-to-Text: This technology can be used to transcribe audio files into text, which can then be searched and analyzed for keywords or phrases that may indicate the presence of CSA.
- Machine learning algorithms: These can be trained on a dataset of known CSA audio files, and can be used to identify and flag new audio files that contain similar content.
- Human Moderation: Trained human reviewers can review flagged audio files and determine if they contain CSA.

The detection of CSA in audio files is less frequent than in other media types, however, as technology advances and more and more communication is done through audio, this might change in the future, so our opinion is that that audio communication should be included in the scope of the CSA proposal.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

Detection of child sexual abuse material (CSA) can be performed on both interpersonal communications and publicly accessible content, but there are important legal and ethical considerations to take into account when deciding which type of content to focus on.

Focusing on publicly accessible content, such as websites and social media platforms, can be more straightforward and less resource-intensive than monitoring interpersonal communications. This is because publicly accessible content is visible to anyone and can be easily found and flagged for review by automated tools or human moderators.

On the other hand, monitoring interpersonal communications, such as email, instant messaging, and end-to-end encrypted communications, can be more complex and resource-intensive. This is because these types of communications are intended to be private and are often encrypted, making it more difficult to detect and review the content. Additionally, monitoring interpersonal communications can raise significant legal and ethical issues, such as privacy concerns, and may require government agencies to have warrant or other legal authorization to access the content.

Bearing in mind that CSA related crimes are very serious ones, detection of CSA should be performed on both interpersonal communications and publicly accessible content, but the focus should be on publicly accessible content. However, it's important to consider the legal and ethical implications of monitoring interpersonal communications and the resources available for this task.

Regarding art. 14, point 2, we believe that the term of 24 hours is much too long if providers already know that that material is subject to an investigation. Our opinion is that once the providers report according to art. 12, they should be in expectation and be prepared for a possible removal order. Therefore, we think that the term of 1 hour is sufficient to execute the removal order, in such cases.

SLOVAKIA

General remarks

The Slovak Republic would like to thank the Presidency for holding a second reading of the proposal using a monothematic meeting format of the LEWP. We wish the Presidency best of luck in the upcoming negotiations.

As the national processes of examining the proposal have not yet been finalised, we recall our **general scrutiny reservation** on the proposal as well as on the amendments made by the previous Czech Presidency. The following comments are to be regarded as preliminary.

Comments on Presidency's questions

1. *To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?*

In general, the Slovak Republic supports a **high degree of technological neutrality** of the proposal with the aim of creating a long-term legal framework for tackling child sexual abuse. At the same time, the proposal needs to provide a sufficiently high degree of flexibility to the service providers in performing the obligations arising from it. Against this background, while the Slovak Republic agrees with the opinion expressed in the joint opinion of the EDPS and the EDPB, according to which end-to-end encryption is the main tool for guaranteeing information security and an essential means of enabling the digital economy and the protection of fundamental rights, including the right to privacy and freedom of expression, we are nevertheless of the opinion that the **use of end-to-end encryption** (or any other forms of encryption) **by a service provider cannot in itself justify non-compliance with the obligations** under this proposal.

As stated during the meeting, we note the fact that, according to Annex 9 of the Commission's Impact Assessment, technological solutions to the execution of detection orders in cases of service providers using end-to-end encryption do exist, but to a greater or lesser extent in the form of a trade-off between their effectiveness in detecting illegal material and users' privacy. We agree with the Commission that a solution to such apparent incompatibility would be further technological development, led either by online service providers themselves or the EU Centre. We believe such technological development will be stimulated as a consequence of adopting this proposal. At the same time, we acknowledge that the assessment of the suitability of technologies which are intended to be used in carrying out a detection order, is subject to a balancing exercise by the Coordinating Authority, as envisaged in Art. 7, to be assessed on a case-by-case basis.

In the light of the above, we do not see an urgency to add wording referring to E2EE, nevertheless, **we could accept one that does not go beyond that of recital 25 of the Interim Regulation**, provided that it is included in the non-operative part of the proposal and it is accompanied by wording "**nothing in this Regulation should be interpreted as exempting providers of relevant information society services from their obligations under this Regulation by the virtue of the type of technology they use**" or similar. As voiced by several delegations, the intention of the Slovak Republic is to ensure that a reference to E2EE would not result in creating a legal loophole that might create a safe harbour for CSAM or grooming.

2. *Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?*

While the Slovak Republic does see great value in voluntary detection provided for by the Interim Regulation, we consider such voluntary measures uneven and insufficient given the extent of child sexual abuse. We therefore support the proposal aiming to establish a long-term legal framework applicable to all providers of relevant online services offering such services in the EU's single digital market, which would ensure legal certainty and strike a balance between taking into account the rights and interests of child victims of sexual abuse on the one hand and service providers and users on the other hand. As a logical consequence of adopting the proposal, the Interim Regulation would need to be repealed and voluntary detection by providers of interpersonal communication services would be replaced by the detection obligations pursuant to the proposal. **Allowing for parallel voluntary detection regime would undermine the proportionality considerations** with respect to fundamental rights of parties concerned, as they were built into the proposed system of detection orders. We consider the balance struck in the proposal rather delicate as it is.

Having said that, the Slovak Republic is of the opinion that the proposal could take a more practical approach in considering the reality on the ground, i.e. the fact that the risk of misuse of services for the purposes of child sexual abuse can be *a priori* assumed in cases of certain service providers who do routinely carry out detection, either on the basis of the Interim Regulation, the GDPR (in case of hosting services providers) or even outside of the scope of EU law (e.g. US law). Accordingly, we are open to **exploring potential differentiation of risk assessment (not detection) obligations of service providers according to whether they are carrying out voluntary detection and do routinely detect large volume of CSAM at present.** This could take a form of tightening the 3 months period for the first risk assessment as well as the period for subsequent risk assessments. Alternatively, we might consider a simplification of the process leading up to the issuing of detection orders in cases of service providers already carrying out voluntary detection and routinely detecting large volume of CSAM, in justified cases even without the need to carry out a (full) risk assessment.

As for the question of extending the period of application of the Interim Regulation, this would, in our opinion, depend on the date of adoption of this proposal and the agreed date of application. The Slovak Republic, adding its voice to several other delegations, would like see an extension of the date of application (to at least 12 months) in view of the considerable scope of system obligations on the part of online service providers that are being introduced, as well as in view of the legislative and administrative work associated with the setting up the tasks of the Coordinating Authority and other relevant national authorities (and in line with the request for extension of the deadline for designating one or more competent authorities stipulated in Article 25). We appreciate the need for the earliest possible application of this proposal in view of the expiry of the Interim Regulation on 3 August 2024 and the related need to prevent a legal vacuum with regard to the (voluntary) detection and removal of CSAM and the detection of grooming. For this reason, while it would have been preferable not having to prolong the Interim Regulation, **we are open toward any proposals aiming to preventing gaps in detection**. In particular, we are open to amending the proposal in such a way that the repeal of the Interim Regulation will not occur on the date of application of the proposed regulation, but only after a certain time has passed from the date of application of this regulation (e.g. 3 months).

3. *Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?*

Scrutiny reservation. The Slovak Republic acknowledges that the **interception of interpersonal audio communication for the purposes of detecting grooming would present the most significant interference with the fundamental rights** of the affected subjects and an exception to the principle of confidentiality of communication enshrined in the ePrivacy Directive. At the same time, we are concerned that the ability of providers of audio communication services to fulfil the risk assessment and mitigation obligations is rather limited by the requirements of the ePrivacy Directive. This is because the content of transmitted communications is not stored and cannot be monitored while performing content moderation or applying mechanisms for verifying suggestions for illegal content might be impossible to carry out. While we have heard the argument of the Commission that it would be preferable to have audio communications covered by the proposal as a long-term legal framework given the expected rise of misuse of such services for CSA with future technological development, given the lack of data on this issue, lack of the discussion on the possible technological solutions for targeted detection of grooming in audio communication and the high interference with privacy, we are **not convinced of the need to have audio communications covered** by this proposal. Nevertheless, we are also **open to proposals adding more robust safeguards of fundamental rights** if audio communications were to be included.

4. *With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?*

Scrutiny reservation. The Slovak Republic acknowledges that restricting the detection of CSA to publicly accessible content would significantly undermine the aims of this proposal given the extent of abuse of interpersonal communication services for CSA. Given the high degree of legal risks involved, however, we await the opinion of the Council Legal Service on the matter and are also open to proposals adding more robust safeguards of fundamental rights for detection of CSAM in interpersonal communication.

Article 12

Paragraph 2: Where the provider submits a report pursuant to paragraph 1, it shall inform the user concerned, in accordance with the following sub-paragraphs 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.

Justification: It is of utmost importance that the provision of information to users does not potentially frustrate any potential investigations by law enforcement authorities and that the user receives no information beyond that which is strictly necessary for the exercise of their right to redress.

Article 15

Paragraph 2: The competent authority Coordinating Authority of establishment may request, when requesting the judicial authority or independent administrative authority issuing the removal order, and after having consulted if necessary with relevant public authorities, that the provider is not to disclose any information regarding the removal of or disabling of access to the child sexual abuse material, where and to the extent necessary to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

In such a case:

(a) the judicial authority or independent administrative competent authority issuing the removal order shall set the time period not longer than necessary and not exceeding **~~six~~ twelve** 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 the competent authority shall inform the provider of its decision, specifying the applicable time period.

The competent 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~~ twelve** weeks, where and to the extent the non-disclosure continues to be necessary. In that case, the competent 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.

SLOVENIA

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

Detection orders must necessarily also apply to encrypted networks, with emphasis that all other measures cannot prevent sexual abuse of children or ensure their security in such a network. Sexual abuse of children that takes place on publicly available Internet does happen, but most perpetrators of sexual abuse of children are aware that they will be discovered earlier in this way, so they use encrypted networks. In most cases, the only ones who can detect such abuse are the providers of such services. For detection in an encrypted environment, we must use or develop technology that will interfere as little as possible with the right to privacy of those who do not commit sexual abuse. By including the record in the proposal as written in Article 25 of Regulation EU2021/1232, we must be careful, as this may affect the use of technology that has been or will be developed that can detect child sexual abuse in an encrypted network without breaching privacy rights of everyone else.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

I agree to consider whether voluntary detection should continue. The Slovenian police is inclined to extend the temporary Regulation, as this is a safer way for the law enforcement authorities to continue receiving reports if the proposal for a new regulation is not adopted in time.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We are in favour of including audio communications in the draft regulation. If the regulation is technologically independent and we do not know what kind of technology we will develop in the future, then the only logical thing is to include the entire spectrum of mutual communication. Already now, of course, the so-called grooming occurs also via audio communication.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

The purpose of the proposed regulation is that the detection of sexual abuse of children is carried out comprehensively, that is to say also in mutual communications. Sexual abuse of children mostly takes place in mutual communication, because the perpetrator is safer there, it is easier to manipulate the victim, etc.

We currently have no comments on Articles 12 to 15.

SPAIN

1. To what extent can encrypted CSA material be affected by a detection order? Are you in favour of including some wording in the Regulation excluding the weakening of E2EE (see, for example, recital 25 of Regulation (EU) 2021/1232)?

If a detection order is issued in connection with the use of encrypted CSA material, the encrypted material may be significantly affected. First, in many cases, the ISP will be able to access encrypted data. This means that the provider may have the ability to decrypt the encrypted CSA material. Secondly, the Law Enforcement Authority (LEA) could request access to the encrypted material and, if the internet service provider refuses to provide it, the LEA could present a judicial order to obtain access to the encrypted data. If the judicial order is issued, then the encrypted material could be decrypted.

Ideally, in our view, it would be desirable to legislatively prevent EU-based service providers from implementing end-to-end encryption.

This is highly controversial, proposing as a solution that encryption with automatic decryption be carried out at some intermediate server of the communication. Obviously, this endpoint should be informed to the user, being an automatic detection not accessible to the user, being an automatic detection not accessible to any human operator.

There is no specific wording in Regulation (EU) 2021/1232 that explicitly refers to E2EE weakening. However, recital 25 of Regulation (EU) 2021/1232 concerns the protection of personal data through the adoption of appropriate technical and organisational measures, including information security. Therefore, language excluding E2EE weakening could be discouraged to ensure an adequate level of protection of other personal data, even to the detriment of early detection of CSA. However, the exact level of E2EE weakening that would be excluded should be determined by EU Member States according to their national regulations.

Law enforcement authorities must have the means to be able to continue to fulfil their legal obligations now that many criminals have moved to the virtual world.

It is imperative that we have access to the data - for which they must be retained - and it is equally imperative that we have the capacity to analyse them, no matter how large the volume.

It is our obligation, this is not an option: we must have the necessary technical, human, innovation and training resources. And among those resources we need to, at least, maintain our current levels of effectiveness against crime, as well as an advanced, flexible and balanced legal framework that encourages innovation while fully respecting the citizens' rights and freedoms.

2. Are you in favour of exploring if voluntary detection should be continued? If so, would you rather prolong the Temporary Regulation (EU) 2021/1232, or include its content in the CSA proposal?

Yes, we are in favour of continuing voluntary screening by service providers. It is interesting to extend the Temporary Regulation (EU) 2021/1232 to give companies and organisations more time to adapt to the requirements of CFS detection. This would allow for a gradual transition and allow agencies to adapt to the new requirements without undue pressure.

Regarding this question, we support the Czech delegation's statement. The idea of developing this new proposal is due to the weaknesses presented by the voluntary content of the temporary regulation.

3. Are you in favour of including audio communications in the scope of the CSA proposal, or would you rather exclude it as in Regulation (EU) 2021/1232?

We do agree on including audio communications in the scope of the CSA proposal. We believe that, as proposed by the Hungarian Delegation, the Proposal should delete the concrete references to the different kind of materials (images, texts, videos or audios) and be more general so the proposal tackles any kind of CSA-related material online.

We would like to highlight that Article 3(1) of the 1989 UN Convention on the Rights of the Child and Article 24(2) of the EU Charter of Fundamental Rights states that in all actions related to children, whether undertaken by public authorities or private institutions, the best interests of the child shall be a primary consideration. It is also noted that the definition of child pornography was already outlined by the Council of Europe in 1989 as "any audio or visual material in which a child is used in a sexual context" (Recommendation (91) 11). This debate is something that should have been resolved, bearing in mind the latest technological developments.

4. With a view to detecting CSA, do you wish that detection be performed on interpersonal communications and publicly accessible content, or be limited to publicly accessible content?

As it is done by major service providers in the US, automatic content detection in interpersonal communications is the key. Automatic detection informed to the user in the terms of use of the services, so as not to infringe the user's right to privacy.

It is recommended that detection is carried out both in interpersonal communications and in publicly accessible content. This would help to ensure that any CSA-related content is identified and appropriate assistance is provided to victims. We reiterate what was reported in Question 1.