Written comments submitted by Member States

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

(9068/22)

Contents

AUSTRIA

Austria communicates its written comments on Articles 8 to 24 of document ST 9068/22 (CSA proposal):

General:

Austria reiterates that it has a general scrutiny reservation concerning the whole proposal and it enters a special scrutiny reservation concerning Articles 8-24.

Austria suggests to hold a workshop concerning the related data protection matters with the involvement of national data protection experts.

Article 12 Z 2:

The obligation of the Internet service provider to inform the user concerned, when within the three month´ time period the provider receives such a communication from the EU Centre indicating that the information is not to be provided, has to be looked at critically.

The information of the user should only be done by mutual agreement with the investigating authority/Europol. Three months is too short (Austria gets about 70000 reports per year!).

Problematic is also the obligation to inform the user about the manner in which the provider has become aware of the potential child sexual abuse concerned - this is a instruction/guidance for professional pedophiles to avoid this in the future!

Article 13 Z 1 (j):

The assessment by the provider if the report requires urgent action is problematic. This assessment can only be performed by the investigating authority. Every report concerning so far unknown CSAM is urgent, because there is suspicion that the risk of abuse persists.

Article 15:

The possession of CSAM is punishable. It can´t be that a challenge of a removal order by the provider or the user has a suspensive effect.

Z 4 (a): The time period of six weeks is not acceptable. Content relevant to criminal law must be deleted as quickly as possible. The information of the user, why the content was removed, must not jeopardize the investigations. When issuing a removal order it is thus impossible to estimate how long a risk exists. During ongoing investigations the obligation to inform the persons affected by a detection-, removal- or blocking order should not be based on the Regulation on (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) but on the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Therefore the information of the affected persons during ongoing investigations should in any case only take place with the involvement of the law enforcement authority resp. of Europol.

Article 18:

par. 1: The right to challenge the blocking order before the courts is viewed with criticism. To avoid a disproportionate burden on the judiciary the possibility for direct judicial challenge should be deleted. The internet users are entitled anyway to request a review by the Coordinating Authority (see par. 5). Only if such a review is rejected the internet users should have the right to go to court.

Articles 20 and 21:

Austria requests more information about the obligations of the internet service providers regarding the information of the victims. Who determines how that it is "known child sexual abuse material" and which people are involved in the dissemination of this material? For what purposes resp. with what requirements is this information transmitted? Are victims associations empowered too to request such information?

Article 22:

The provision concerning „Preservation of information", especially the possibility for the internet service providers to preserve the information for 12 month is to be welcomed.

Data protection comments on Chapters I and II:

Regarding Art. 1 para 4/Recital 9:

Recital 9 states that the Proposal in accordance with Art. 15 para 1 of the e-Privacy Directive limits certain rights and obligations provided for in Articles 5 and Article 6 of the e-Privacy Directive. Recital 9 applies Art. 15 para 1 e-Privacy Directive by analogy because the text of Art. 15 para 1 e-Privacy Directive exclusively empowers Member States to limit the rights set out in Articles 5 and 6 by adopting national regulations for the purposes of national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. The analogous application of Art. 15 para 1 of the e-Privacy Directive seems questionable:

With regard to Art. 15 para 1 e-Privacy Directive, its Recital 11 states that – like the Data Protection Directive, 95/46/EC, – the e-Privacy Directive does not apply to legal areas that are not governed by Community law. The competence of the Member States to enact their own regulations in the areas of public security, national defence and state security as well as for the enforcement of criminal law provisions therefore remains unaffected, as long as they are appropriate, proportionate and necessary in a democratic society.

The aforementioned areas of law fall predominantly, if not exclusively, within the regulatory competence of the Member States. We would therefore argue that the reasoning behind the opening clause in Art. 15 para 1 e-Privacy Directive is that the Member States' competence to regulate these areas should not be restricted by the obligations set out in the e-Privacy Directive. Therefore, we argue that the gap in the scope of Art. 15 para 1 is intentional and cannot be applied by analogy.

Furthermore Art. 15 para 1 clearly only includes measures for the purposes of national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of electronic communication systems as referred to in Art. 13 para 1 of the Data Protection Directive.

As page 6 of the Explanatory Report mentions, the legal basis for the proposal is Art. 114 TFEU which only aims to harmonise provider obligations in order to ensure the functioning of the Internal Market. Meanwhile, the harmonisation of the Internal Market is not one of the purposes for which Art. 15 para 1 e-Privacy Directive allows limitations on the provider's obligations.

If in fact the purpose of the Proposal is the harmonisation of law enforcement measures against child sexual abuse, especially online, limitations of providers' obligations according to Art. 5 and 6 e-Privacy Directive would be permissible. Nevertheless, then the Proposal could not rely on Art. 114 TFEU for its legal basis.

In addition, it is noted that the proposed measures for monitoring and prior checking of the content of users of Internet services without concrete grounds for suspicion and without differentiation are not proportionate in the sense of Art. 15 para 1 of the e-Privacy Directive.

Accordingly, there are also massive fundamental rights concerns, in particular with regard to a violation of the right to privacy pursuant to Art. 7 GRC and the right to data protection pursuant to Art. 8 GRC (see our comments on Art. 7 of the Proposal).

→ We therefore ask the EC to clarify whether the present draft is a law enforcement measure within the meaning of Art. 15 para 1 of the e-Privacy Directive.

→ We also request the Presidency to obtain an expert opinion from the EC's Legal Service on this question and provide further explanations on why Art. 15 should be considered to contain an *unplanned* gap.

Regarding Art. 4:

Art. 4 para 3 obliges service providers to carry out age verifications in order to identify children and protect them accordingly. However, it is unclear which methods are permissible for such age verifications and what safeguards should be applied to them. Would it for instance be permissible for providers to indiscriminately profile the entire online activity of all of their users in order to "reliably identify" children?

→ We would therefore ask the EC to explain in more detail how the mandatory age verification in Art. 4 para 3 shall be implemented by the providers and where the limits of these checks are to be set.

Regarding Art. 7:

1. The proposed "detection order" evidently obliges providers to monitor all private – in particular encrypted – communications without cause. This measure represents a massive encroachment on the fundamental rights both of service providers and users of online services. **We highly doubt that the proposed encroachments on fundamental rights are proportionate in accordance with the ECJ's case law:**

The ECJ only recently addressed the question of the permissibility of the collection and storage of large amounts of data and the associated data mining in its Judgment of 21.06.2022, *Ligue des droits humains*, C-817/19, in connection with the PNR Directive (Stw. PNR) and – building on its previous case law – made the following essential findings:

It is settled case-law that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Art. 7 and 8 CFR, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to those data with a view to their use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.

This interference is made even more difficult by the fact that the aggregation of the data collected is capable of revealing precise information about the private life of the persons concerned, which may even constitute in the revelation of sensitive data.

The extent of the encroachment of Art. 7 and 8 CFR associated with automated analyses of PNR data depends on the models and criteria established in advance and on the databases on which this type of data processing is based. However, inevitably the automated analysis of PNR data will be subject to a certain margin of error, i.e. that even persons who are blameless are classified as suspects.

In order to meet the requirement of proportionality, the relevant regulation containing the encroachment must establish clear and precise rules on the scope and application of the measures envisaged, as well as minimum requirements, so that the individuals whose data have been transferred have sufficient safeguards to ensure effective protection of their personal data against risks of misuse. In particular, it must specify the circumstances and conditions under which a measure providing for the processing of such data may be taken in order to ensure that the interference is limited to what is strictly necessary. The need to have such safeguards is all the more significant when the personal data are processed by automated means. These considerations are particularly valid when sensitive information about the persons transported can be obtained from the data.

Moreover, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, the indiscriminate application by that Member State of the system established by the PNR Directive not only to extra-EU flights but also to all intra-EU flights would not be considered to be limited to what is strictly necessary.

In such a situation, the application of the system established by the PNR Directive to selected intra-EU flights must be limited to the transfer and processing of the PNR data of flights relating, inter alia, to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application.

Comparable to the PNR Directive, the present Proposal also seeks to allow collected data to be used to identify persons who are not suspected of being involved in child abuse and who should be subject to closer scrutiny. However, such a measure must be limited to what is necessary.

2. In its Judgment of 5 April 2022, G.D., C-140/20, the ECJ also stated that criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. A threat to national security must be genuine and present, or at least foreseeable, in order to justify a measure of general and indiscriminate retention of traffic and location data for a limited period of time. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed.

As regards the objective of combating serious crime, the Court held that national legislation providing, for that purpose, for the general and indiscriminate retention of traffic and location data exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. In view of the sensitive nature of the information that traffic and location data may provide, the confidentiality of those data is essential for the right to respect for private life.

Thus, and also taking into account, first, the dissuasive effect on the exercise of the fundamental rights enshrined in Articles 7 and 11 of the Charter, referred to in paragraph 46 of this judgment, which is liable to result from the retention of those data, and, second, the seriousness of the interference entailed by such retention, it is necessary, within a democratic society, that retention be the exception and not the rule, as provided for in the system established by Directive 2002/58, and that those data should not be retained systematically and continuously. That conclusion applies even having regard to the objectives of combating serious crime and preventing serious threats to public security and to the importance that must be attached to them.

→ Child pornography undoubtedly constitutes – and is also expressly confirmed to be by the ECJ – a case of serious criminal behaviour. However, in light of the case law cited above, it must be assumed that the proposed indiscriminate monitoring of all personal data of users of online services constitutes a comparably serious encroachment that exceeds the limits of what is absolutely necessary and **cannot be regarded as justified in a democratic society.**

→ Furthermore, based on a synopsis of Art. 22 in conjunction with Art. 7 and Art. 10, it cannot be ruled out that the implementation of a "detection order" does not also include the indiscriminate retention of personal data for the purpose of forwarding it to the competent authorities, which in light of the cited case law cannot be considered justified in a democratic society. **We therefore request the EC to comment in more detail on the content and practical implementation of "detection orders" and the associated data retention.**

3. The above must apply all the more to the proposed regulations in connection with combating grooming. The Draft also provides for higher hurdles for the use of the proposed instruments for combating grooming than for combating child pornography online. For example, Art. 7(7) requires evidence for the issuance of a "detection order" not only for the existence of a "significant risk" that the service is being used for the dissemination of child pornography, but also evidence that the service has actually been used for grooming in the past 12 months. In addition, Art. 7(9) orders a retention period of "only" 12 months in relation to grooming (child pornography 24 months).

→ It can therefore be assumed that, in accordance with the cited case law, the proposed monitoring of all personal data of users of online services for the purpose of combating grooming cannot be considered justified in a democratic society.

4. The procedure described in Art. 7 para 2 and 3, which is to precede the issuing of a "detection order", evidently is meant to induce service providers to comply with the national authorities request without a corresponding coercive order being issued.

→ This raises the question which **legal basis the "voluntary" monitoring** of all traffic and content data online will be based on once the derogation of Regulation 2021/1232/EU has been removed?

5. According to Article 7 para 4, the national coordinating body may only apply for a detection order if it has previously proven that there is a significant risk that the service is being used for the dissemination of child pornography or grooming. According to Art. 7 para. 5 li.t a/Art. 7 para. 6 lit. a/Art. 7 para. 7 lit. b, this is the case if it is "likely" that the online service will be used for child pornography or grooming. A more detailed specification of this term is not made in the text, but instead is transferred to the competence of the EC in the context of issuing "guidelines" according to Art. 11.

→ We therefore request the EC to describe the circumstances under which it is "likely" within the meaning of Art. 7(5)(a)/Art. 7(6)(a)/Art. 7(7)(b) that an online service will be used for the dissemination of child pornography or "grooming" and why such clarification cannot be made within the text of the Proposal.

6. According to Art. 7(6)(c)(1), an online service that does not enable the live transmission of pornographic images poses a significant risk for the dissemination of new child pornography material if a "detection order" has already been issued against the online service regarding the dissemination of known child pornography material. It remains unclear whether this is a one-time continuation of the "detection order" or whether a service against which a "detection order" has been issued is permanently burdened with a significant risk for the distribution of child pornography material?

→ We therefore request the EC to clarify whether or how an online service against which a detection order has once been issued can still dispute the issuance of another detection order based on grounds?

7. With regard to the proposed period of validity of 24 months for detection orders for child pornography pursuant to Article 7 para 9, reference again is made to the ECJ's Judgment of 21 June 2022, C-817/19. In that judgment, the ECJ held that a general retention period of five years for data collected in a blanket manner, which applies indiscriminately to all passengers, including those for whom neither the prior check nor any checks within six months of the collection of the data, or any other circumstance, have provided objective evidence of a risk in the area of terrorist offences or serious crime with an objective link to the passengers' travel, violates Art. 7 and 8 CFR as well as Art. 52 para 1 CFR.

Since this case also involves the blanket recording and storage of persons of good repute, this data may also be stored for a maximum of 6 months and must be deleted immediately if no suspicion is substantiated against the person concerned within this period.

Art. 20 and 21:

We ask for more information on online service providers' obligation to provide information to victims. In particular, we would like to know who determines in what way that a certain CSAM is "known child sexual abuse material" and which persons are involved in the dissemination of this material? For what purposes or with what specifications is the information transmitted? Are victims' representatives and associations also authorised to request such information?

Art. 22 para. 2:

The comments on Article 7, in particular on the question of the permissible duration of the data retention, also apply to Art. 22 para 2 of the Proposal, which lays down a general data retention period of 12 months that can also be extended by request of the competent national authority. The Proposal does not specify any further conditions or a maximum storage period for extensions. Again, we refer to the case law cited with regard to Art. 7.

In summary, as described above, there are a number of massive fundamental rights concerns and complex questions in connection with Article 7, which still need to be discussed intensively at EU level. Therefore, in conclusion, a scrutiny reservation is once again issued for the entire Proposal, in particular Article 7.

BELGIUM

At this moment we would like to uphold a general scrutiny reservation. We would like to confirm our previous questions and concerns which have not all been answered yet as well as the following questions which surfaced:

- Like other Member States we wonder, in a manner almost inverse to Article 9(4), whether a detection order can be prolonged or whether a renewal of a detection order could follow a simpler process. We notice that obligation to provide a new risk assessment two months before the end of the detection order, but this seems hardly sufficient to prevent a gap between two necessary detection orders taking into account the multiple steps and actors concerned in the procedure to issue a detection order.
- Like other Member States we wonder about the language regime imposed when delivering orders to the providers. In the DSA a solution was found in Article 8(2)(c) and Article 10(3) to create a balance between the different interests. We suggest to ensure coherence with the DSA solution. One of the elements consists for example of requiring only a translation of the most important elements necessary to execute the order if the authority is not using the other possible languages. Another elements concerns the possibility to use "a language broadly understood by the largest possible number of Union citizens".
- Related to Article 9 and the sending of the detection order to several actors, we wonder whether these (and possibly also other) orders should be sent to the Digital Service Coordinators for their information. These DSC will not in all Member States be used as Coordinating Authorities namely, so cooperation – including informing each other on certain matters – seems useful. It could also be useful to inform the DSC if providers are not abiding by the orders or if systematic problems arise. Also useful could be if the DSC informs the Coordinating Authorities about risk assessments under the DSA that indicate a systematic risk for CSAM.
- We wonder if the judicial or the independent administrative authority could also directly, on its own initiative issue a removal order to the provider. Like other Member States we wonder about the decision to not provide for a cross-border functioning of these removal orders, taking into account the cross-border nature of this crime.
- In relation to Article 14(5) the provider needs to inform and explain if it cannot execute a removal order "on grounds of force majeure or de facto impossibility not attributable to it". We wonder whether it would also be useful to create a similar rule for blocking orders and detection orders.
- In relation to Article 16 we confirm our previous concerns.
    - 'Blocking' means in practice that a page is made no longer visible through a reconfiguration of the domain name system (DNS) resolver. The internet access service providers do not always have their own DNS resolver to reconfigure certain URLs. Sometimes they use other providers, namely the providers of DNS resolvers. We refer also to recital 83 in the DSA that explicitly mentions 'domain registry or registrar' as a relevant partner. If Article 16 does not oblige these DNS resolver providers to cooperate, then we might in practice again still depend on voluntary cooperation to block URLs via internet access.
    - Moreover, on a technical level, if an URL needs to be blocked by the internet access service provider, this can in Belgium via the DNS only be done via the top level URL (so the whole website for example of an organization, and not a specific webpage).

- Also France and Ireland mentioned technical issues with the implementation of Article 16. We would like to know whether other Member States have similar concerns in relation to blocking a concrete web page and whether the internet access service providers can do this themselves or whether they need the providers of DNS resolvers.
- Could the Commission comment on how the internet access service providers anticipate to be able to implement this proposed obligation?

- In relation to Article 21 it seems from the text (stating the singular "a" provider in paragraph 2 of Article 21 and the singular "the" provider in Article 49(1)(a)) that the victims are not capable of asking the EU centre for assistance in deleting CSAM with all relevant providers. The victims should apparently already know which provider is concerned. Is it correct that the EU center cannot assist victims, upon their request, in verifying if certain CSAM is present on the internet also with other – not yet identified – providers?

  In relation to this we wonder if we understand correctly that voluntary detection which remains possible for hosting service providers, not subject to the ePrivacy Directive, cannot benefit from the database of indicators?

- We would like more explanation on what is meant by "*reasonable assistance*" in Article 21(1). We also wonder how a victim can 'request' such assistance.

- In relation to Article 22 we would confirmation on whether these rules are to be considered as a legal basis for an obligation to preserve data or rather as limitations applicable to another (for example national) legal basis that needs to be created separately. Also, in relation to the first sentence of paragraph 2 we would appreciate confirmation that the limited time of 12 months only applies in case of information related to "reporting, removal or disabling access".

- In relation to Article 23 we understand that the point of contact is created to facilitate contact with the provider. However, we would like to understand if more than one point of contact can or should be appointed, because from the Commission's explanation we understood that it is indeed so that a point of contact should be appointed in each Member State.

  Also, it remains unclear to us how the point of contact relates to the main establishment (or to the obligation to appoint a legal representative in case there is no main establishment in the EU). The Commission explained in relation to the obligations in Articles 8(2), 14(4) and 17(2) and (3) to inform the provider that sending the order to the main establishment (or legal representative) and to the point of contact is meant to be understood as "either, or" and thus not cumulatively. We would like to understand better how they relate to each other and also we would like more clarity in the text.

  [On a side note we recommend to place paragraphs 2, 3 and 4 of Article 17 in the same paragraph, similarly to Articles 18(2) and 14(4).]

- In relation to Article 24 we would like to understand if more than one legal representative can be appointed; this is not clear from the concrete text, although the third paragraph makes sudden reference to the plural form "legal representatives".

BULGARIA

Bulgaria would like to reiterate the position already expressed on previous LEWP meetings that the proposal is of exceptional importance. Bulgaria supports the proposal's goal to provide a unified approach in the fight against child sexual abuse. We see the added value of this act in establishing clear rules for effective interaction between law enforcement and the private sector to detect, eliminate and report online child sexual abuse.

With regard to the discussions from the LEWP's meeting on 20 July 2022 Bulgaria would like to provide the following comments:

In relation to Art. 12, Bulgaria supports the comments of Austria and France that the period for the provider's obligation to notify the user is too short. It may jeopardize the possible investigation of users who have uploaded material with illegal content. It should be taken into account that the procedure for identifying a perpetrator of criminal activity in the course of investigation may take a considerable period of time, and notifying the user could lead to the destruction of evidence that would be relevant to the investigation being carried out.

With regard to Art. 14, par. 1 and more specifically the removal and blocking of access of certain illegal content on the territory of the MS, we believe that the blocking of access within the EU is not the optimal solution because it could be possible for the illegal content to be accessed outside the Union or by using VPN services. The distribution of material containing scenes of child sexual exploitation is a serious crime. That is why the blocking of access to such content on the territory of the EU seems insufficient as there are numerous tools to mask the person's geolocation. If the detected content is located on the server of a company operating on the territory of the EU, where this Regulation applies, the access to such content should be blocked also outside the territory of the EU.

ESTONIA

Article 16 Blocking orders

Art 16(1): 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?

Art 16(6): According to art 16 par 6 the period of application of blocking orders shall not exceed maximum of 5 years. Could after this period another blocking order be issued? What measures are taken in that period to reduce CSAM on these services? What measures are envisaged in this regulation?

Article 19 Liability of providers

What is the aim of this article? Is it to enable service providers to carry out voluntary own-initiative investigations? Or does this provision change the liability regime of intermediary services by stating that they could only avoid liability for child sexual abuse offences if they carry out, in good faith, the necessary activities to comply with the requirements of this Regulation? We believe that liability for child sexual abuse offences should be kept separate from liability for the infringement of the obligations of this regulation. If a service provider does not apply with the obligations of this regulation, then they should not become liable in criminal proceedings. The infringement of the obligations of this regulation should result in administrative proceedings.

Article 24 Legal representative

These obligations are also imposed in the TCO regulation (art 15 and 17 respectively) and the DSA regulation (art 10 and 11 respectively). Could the service provider designate the same point of contact or legal representative to comply with all three regulations? What is the added value of duplicating this obligation across all regulations?

GERMANY

General

- Germany welcomes the opportunity to discuss the articles of the second chapter in further detail.
- Because the Federal Government has not yet completed its examination of the proposed Regulation, we would like to enter a general **scrutiny reservation**.

Section 2 "Detection obligations":

- According to the current version of the proposal, it is conceivable that a (court-ordered) detection order could be issued even though the data protection supervisory authority had expressed concerns when it was consulted. This could lead to conflicting decisions, as the data protection supervisory authorities would retain their corrective powers under Article 58 of the General Data Protection Regulation, including the power to impose a ban on processing. In the worst case, a provider could be confronted with a (court) order on the one hand and a ban on processing ordered by the supervisory authority on the other. Germany therefore believes that it is necessary to clarify how such conflicts are to be resolved. We kindly ask the Commission to provide an explanation.
- According to Article 9 (2) (1), when a detection order becomes final, a copy of the order is to be transmitted to the competent Coordinating Authority after the time periods given in Article 9 (2) (3) have expired. As Germany understands it (also based on the Commission's explanations in the meeting on 22 June 2022), the procedure for redress provided for in Article 9 (1) has no suspensive effect. In this context, we ask why the Coordinating Authority is to be informed only after the time periods given in Article 9 (2) (3) have expired.
- In Germany's view, the Regulation must not lead to general interception of 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. With this in mind, Germany believes it is necessary to state in the draft text, for example in Article 10 (3) (a) (new), that no technologies will be used which disrupt, weaken, circumvent or modify encryption. The Federal Government is still in the process of reviewing the use of other technologies.
- Germany also asks the Commission to explain what it means by "human oversight" of the technologies used (see Article 10 (4)) and to sketch out its proposed procedure for informing users (see Article 10 (5)).
- In view of the fundamental rights concerned, it is necessary in the interest of proportionality to ensure that the technologies to be used are sufficiently sophisticated and fit for purpose, with a minimal error rate.

Section 3 "Reporting obligations":

- Please clarify the effects of the differences in wording between Article 12 of the Commission's draft ("indicating potential online child sexual abuse") and Article 15a of the draft Digital Services Act ("giving rise to a suspicion"). Does the Commission regard these requirements as differing in substance?
- Germany believes further details are needed to specify when it can be assumed that a provider is aware of information indicating potential online child sexual abuse.

- We would like to emphasise already at this point that, in Germany's view, to process reports effectively, it is essential for these reports to be forwarded to the Member States without delay following the necessary initial review.
- We ask for further details to be added to Article 13 (f), specifying that the IP address, time stamp and port number must be included in the report. This information is already provided for in Annex III no. 5; however, given its significance for the law enforcement authorities, this information should also be required in the text of the Regulation itself.

Section 4 "Removal obligations":

- The Commission's proposal provides for removal orders. Online child sexual abuse material (CSAM) often remains available for years. For survivors of abuse, this can lead to revictimisation and interfere with their ability to deal with their trauma. That is why it is crucial to reduce the availability of online CSAM through certain services.
- We ask the Commission to confirm that service providers will still be allowed to remove illegal content voluntarily based on the Commission proposal.
- Germany asks how the orders to remove content relate to the rules on responsibilities in the Digital Services Act. According to the Digital Services Act, providers of hosting services are not exempt from liability if known illegal content is not removed immediately.
- The proposed time limit of 24 hours in Article 14 (2) seems reasonable in our view. Content subject to a removal order is clearly illegal content.
- In the interest of effective law enforcement, we have no concerns that Article 12 (2) and Article 15 (4) allow, in individual cases, for the possibility of temporarily suspending the obligation to inform users who provided the material in order to avoid interfering with investigations.

Section 5 "Blocking obligations":

- As we understand it, Article 16 is aimed at blocking individual URLs, not domains. Can the Commission confirm this?
- If a blocking order is issued, which rights of access continue to apply (staff?)?

Section 6 "Additional provisions":

- Regarding Article 22: The Commission explained that the CSA Regulation is supposed to contain the necessary legal basis for processing personal data. Article 22 is apparently intended to serve as the legal basis as referred to in Article 6 (1) (c) in conjunction with Article 6 (3) (a) of the General Data Protection Regulation. However, this provision now only covers the preservation of personal data by the provider for the purposes given in Article 22 (1) and (2). We do not currently see a sufficient provision for the processing of personal data necessary for these purposes which also includes their subsequent transmission to the EU Centre. We therefore believe further specification is needed to meet the requirements of EU data protection law and to provide legal certainty for providers. We will be happy to supply suggested wording later for this purpose.
- Re Article 23 (3): Is the Commission concerned that the language used to communicate with their points of contact is different from the language referred to in Article 76? How can the best possible harmonisation of processes and reporting channels be ensured?

GREECE

Following our oral interventions in the previous meeting, we would like to provide to you our written comments on the text of the proposal of the Regulation for CSA:

Introduction:

We avail of this opportunity to reiterate that Greece supports the proposal of the Commission for the Regulation laying down rules to prevent and combat CSA.

We would also like to underline that detecting, removing, and blocking CSA in cyberspace, from the legal perspective constitutes an interference with the rights of personal life, personal data protection, expression, and confidentiality of communications. Consequently, all relevant actions should be subject to end-to-end safeguards, complying with the principles of necessity and proportionality in all stages of the process.

Moreover, Greece has concerns on the establishment of a separate EU Centre as the proposed processes could result in delays in the process of the information exchange with law enforcement and deletion of the illegal content online. The Member States should maintain flexibility and simplification of the procedures, given that many stakeholders are involved and this may lead to low speed of removal of CSA material. Therefore, we propose to examine the necessity of the establishment of the Centre at this stage, because the new Centre is referred from the first articles.

Article 8 (additional rules regarding detection orders):

We regard it more beneficial for the competent authority issuing the detection order to transmit it (the detection order) to the requesting Coordinating Authority, facilitating circulation among the other involved parts.

Article 9 (redress, information, reporting, and modification of detection orders):

On para. 4, we propose replacing the term “request” with “suggest”, taking into account the independent character of the competent authority and the existence of the order.

Article 10 (technologies and safeguards):

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

We have concerns about par. 4 (c) because it offers a margin of appreciation to the providers through the repeated use of the word necessary. Hence, we propose the following: “*ensure appropriate human oversight that the technologies operate in a sufficiently reliable manner and human intervention when potential errors and potential solicitation of children are detected*." This proposal stems from the importance of the interference with human rights in line with the relevant case law.

Article 11 (Guidelines regarding detection obligations)

We have a reservation on this provision providing to Europol the authority to confirm that information of a subject/ user is processed in an ongoing investigation. We consider this confirmation should be provided only by the Law Enforcement Authorities of the Member States which conduct the investigations of child sexual abuse offense.

Article 14 (removal orders):

We consider that transmitting a removal order by the competent issuance authority to the requesting coordinating authority will enable circulation and execution.

Article 16 (blocking orders):

We have two remarks on this article. On para. 6, we consider that the competent issuance authority must specify the period of a blocking order and not the coordinating authority. Moreover, on para. 7, we favor replacing the word "request" with "suggest", taking into account the independent character of the competent authority and the existence of the order.

Article 17 (additional rules regarding blocking orders):

We suppose that is a written mistake in the reference at the beginning that the coordinating authority issues a blocking order. Also, we remind our suggestion for the transmission of the order by the competent issuance authority to the requesting coordinating authority, enabling circulation and execution.

HUNGARY

The scope of the Regulation is limited to hosting providers, interpersonal communications service providers, on-line application shops and internet access providers. Since content is identified by URL, excluding DNS providers from the scope of the Regulation could make DNS-based filtering by Internet access providers - which is widespread in the EU - impossible.

A further problem in this regard is that the CSA Regulation adopts the definition of Regulation (EU) 2015/2120 in its definition - Article 2(e) - which does not include DNS resolution services typically provided as an additional service by Internet access providers:

> "(2) ' internet access service' means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used."

In any case, identifying CSA content solely on the basis of URLs is not efficient, since in modern hosting frameworks a significant part of the content is accessed through dynamically generated web pages. It would be preferable to introduce a requirement for CSA content to be identified by a digital hash, which would allow content identified as CSA to be blocked at the time of upload in the case of hosting services or before transmission in the case of interpersonal communications services. In addition to a deterministic digital footprint, the possibility of AI-based content identification could also be considered.

In the case of Internet access providers, the URL-based inaccessibility described in the draft CSA Regulation is not possible in the vast majority of cases due to the commonly used encryption standards (TLS/SSL), as the provider does not have access to the URL information transmitted in the encrypted communication channel. It would be appropriate to provide for the possibility of domain name-based blocking, as in the EUROPOL IWOL list, but in this case the issue of additional filtering of other legitimate content available under the same domain name should also be regulated.

For interpersonal communication applications using end-to-end encryption, there is also no possibility to identify CSA content when it is transmitted, so it would be appropriate to consider extending the scope not only to online application stores but also to developers of communication applications and possibly to smart device and operating system manufacturers and developers (e.g. Apple/Google) that provide the platform for the applications - similar to the DMA.

Cloud service providers are also not covered by the CSA Regulation, which could be a particular concern for 5G SA networks, pereminformatics and service provider cloud solutions, where digital footprint-based identification and filtering of CSA content could be efficiently performed in the cloud.

As the technical implementation of filtering CSA content, for example by providing access to encrypted data, may also raise fundamental rights and national security issues, it is necessary to ensure that in the case of third country service providers, the Member State of the country of destination of the service is able to see the technical solutions used to identify the content and not only the designated authorities of the Member State of establishment.

IRELAND

Article 7 (see also next section)

In general, Ireland has concerns about the complexity of the processes around Detection Orders. Ireland also has concerns that responsibility is being placed on national authorities to take decisions with EU wide consequences without sufficient scope for EU wide consideration.

It would be useful to stress-test different scenarios that may arise in respect of the processes set out in Article 7 to gather the views of MS and other stakeholders. For example, what if a situation arises where different service providers, based in different jurisdictions but offering near-identical services and having available to them identical detection technologies (as provided for/approved by the EU Centre), are subject to different decisions by their host jurisdiction's Coordinating Authorities? I.e. One SP is subject to a Detection Order, and one is not? In other words, how can we ensure consistency across the internal market?

The EU Centre is structured in such a way as to enable the views of all Member States to be represented, through the composition of the Executive Board. This is one way of providing such consistency. The view of the EU Centre as set out in the proposal is only advisory; should there be consideration of some form of resolution mechanism for scenarios where the Coordinating Authority does not agree with the opinion of the EU Centre about whether a Detection Order should be issued?

On a more specific aspect of Article 7, Ireland's understanding is that the Coordinating Authority (CA) will base its "preliminary view" that the conditions of paragraph 4 have been met, as referred to in 7(3), on the risk reporting under Article 5. It is our further understanding that this preliminary view must include an assessment of the factors set out in 7(4) first sub-paragraph (b) – the question of the balance of fundamental rights. The CA cannot make an assessment on this matter without having a clear idea of the detection technologies available to Service Providers. But on matters of technology the CA will depend greatly on the views of the EU Centre, in line with 66(6)(a) and 57(1)(g). And the views of the EU Centre will not be available until the CA has already decided on its preliminary view. So we have a circular process. Perhaps the CA is intended to seek information on 7(4) first sub-paragraph (b) from the Centre under 7(2)? In which case the CA will be seeking information from the Centre in order to allow it to formulate a preliminary view in order to allow it to seek information from the Centre on which it will partially base its final view.

This is one example of the complexity of the processes set out. Ireland will continue to seek ways to improve and simplify these processes.

--

General comments on judicial authority or independent administrative authority

The Commission has stated that the judicial authority or independent administrative authority – the second competent authority – should be a court, or court-like body, and we acknowledge the Commission explanation that the second competent authority would provide an extra safeguard, and the references to CJEU case-law.

From an implementation point of view, we have concerns about having to create two separate new bodies to undertake the same decision-making exercise for every Detection Order, Removal Order and Blocking Order that is issued. And we are concerned that the expertise in relation to online child sexual abuse and especially in terms of the technical knowledge to assess the measures that the service providers have taken and the technology that the Centre has developed will have to be developed in relation to both the Coordinating Authority and the second competent authority.

And we note that the Coordinating Authority is already required to be independent, to be impartial, to be objective, to be free from influence – these are all laid out in Article 26. And it is already required to take into account the views of the Data Protection Authority and the service provider and the EU Centre, under Article 7.

We continue to have misgivings about the lack of detail in the draft Regulation about the major role of the second competent authority in the procedures set out. By contrast, the Coordinating Authority gets a 14 Article Chapter.

For example, in 7(8) the draft Regulation states:

The Coordinating Authority of establishment when requesting the issuance of detection orders, and the competent judicial or independent administrative authority when issuing the detection order, shall target and specify it in such a manner that the negative consequences referred to in paragraph 4, first subparagraph, point (b), remain limited to what is strictly necessary to effectively address the significant risk referred to in point (a) thereof.

How is it intended to give the second competent authority the capacity to "target and specify it"? While we can understand the concept of giving judicial approval to the CA's decision to issue a Detection Order, we cannot envisage a circumstance where an Irish court could take the responsibility for amending the substance of a Detection Order which has been based on a level of expertise that it is not reasonable to expect a court to have. The alternative is to create a new, quasi-judicial independent administrative authority which does have the expertise to amend a Detection Order as part of its consideration – the concerns set out above in relation to creating and resourcing two new bodies to carry out the same process would arise here.

At a minimum therefore we would ask for the deletion of the words "and the competent judicial or independent administrative authority when issuing the detection order" in the extract above. But if judicial/quasi-judicial approval is to be required for the issuance of Detection Orders, a better solution would be to define the role of the second competent authority.

For example, the role of the second competent authority could be to establish that the Coordinating Authority has fulfilled its responsibilities correctly, i.e. the CA has acted in accordance with the Regulation and national law, has taken into account all factors, especially the balance of fundamental rights, etc. But the role of the second competent authority would not be to consider all the same factors as the CA. Given that service providers can challenge the issuance of a DO in front of the courts as soon as it is issued anyway, this seems like a more proportionate system of judicial oversight.

We continue to scrutinise all references to national authorities.

--

Article 8

We are concerned that possibility for providers of interpersonal messaging services to implement voluntary detection measures will no longer exist. The Commission has stated that it is not legally possible to provide a legal basis in this Regulation for those measures. We would like further information on this and the opportunity to explore whether there are any other options.

--

Article 12

Support for the provision in Article 12(3). We know that making reporting easier can make a real difference. And that it can benefit from co-design with stakeholders, including children. So can we be more prescriptive here, perhaps by including a process to ensure there is an industry standard for service providers?

Please note that the Commission was not able to respond to this point at the WP on 20/7 (there were some technical difficulties at the meeting) so we would be particularly grateful for a response.

--

Comment about preservation of evidence

This is a comment that comes from our colleagues in the national police service. They are concerned that illegal material is not preserved by online service providers for some period of time to ensure that it can be used as evidence. If it is the EU Centre's responsibility to keep a central database of all the illegal content reported to it then we need to make sure that there is a system that can trace back the content from origin through the detection and removal process in a way that is verifiable and can be used by Member States as evidence in criminal cases.

Please note that the Commission was not able to respond to this point at the WP on 20/7 (there were some technical difficulties at the meeting) so we would be particularly grateful for a response.

--

Article 14

SE asked about whether removal orders have a cross-border effect? Commission reply was that these are not cross-border Removal Orders, they are removal at national level with application for whole of EU. We understand this to mean that, under this Regulation, a MS's authorities can only seek the removal of material that is hosted by service providers under their own jurisdiction. What if a MS wishes to have material removed that is hosted by a SP in a different jurisdiction? Is there no facility under the Regulation for this to happen? It is likely that there would be agreement between MS on the need for removal of such material. Could the EU Centre play a role in facilitating this?

We support comments from other MS that question why it is necessary to have the second competent authority issue Removal Orders, in contrast with other legal instruments. We do not think a desire for consistency between the procedures that apply to Detection, Removal and Blocking Orders is sufficient justification. The Regulation proposes very intensive procedures for Detection Orders because of the particular concerns around fundamental rights – these very intensive procedures will complicate implementation and have major implications for Member States when it comes to resources. We should not then simply replicate them elsewhere if it is not necessary to do so.

NL asked about the extension of the period during which the service provider may not disclose information in relation to removal. The Commission stated that only the second competent authority can decide to extend the period, but it must do so on the basis of an application by other national authorities. (This should be set out more clearly in the text.) We question the necessity of requiring the second competent authority to make this decision – it should be possible for the investigating authorities to do so. If the request has to be made to the second competent authority, there should be scope to request a longer extension, or repeat extensions.

--

Article 16(6)/Article 17(1) chapeau

From a drafting perspective, these two provisions appear to be missing a reference to the second competent authority (though we can support them…).

--

Section 6

We are awaiting comments from stakeholders in relation to Section 6 and will provide these at a later date. We hope to have the opportunity to discuss these provisions at the Working Party.

ITALY

Recalling our general scrutiny reservation on the Proposal, please find below some preliminary comments from IT as follow-up to the LEWP meeting on 20th July.

Article 11 Guidelines regarding detection obligations

We believe that the investigative activities ongoing or upcoming on the CSA should be considered in the guidelines.

Article 14 Removal Orders

The believe that the role and prerogatives of the Coordinating Authorities are extremely important, we would like to have further clarifications on the expected framework of the whole functioning system (and work flow) of the removal orders from first evidence of a possible CSA to the issue of the order of the judicial or independent administrative authority. Please also consider that together with the administrative procedures also criminal judicial orders can be issued (before and after the removal orders) on the CSA so we would like to know how exactly the two dimension can be harmonized and what will the impact on the new Regulation on the criminal investigations.

Article 16 Blocking Orders

We reiterate what said with reference to art. 14. In general we would like to better understand the impact on the investigative activities (ongoing and upcoming) of the CSA Regulation's orders (detection, blocking and removal).

Article 20 Victims' right to information

We wonder why EU citizens residing outside EU are not included

Article 23 Points of Contact

With reference to this provision we would like to suggest, together with the establishment of a "point of contact" for institutional communications on CSA, the establishment of a "abuse desk" which could be a collector of reports from users, in order to facilitate the detection of CSA content, facilitating the exchange of information and consequent actions and measures.

Article 24 Legal representative

We would like to have some additional clarifications on the consequences in case providers to do not comply with the obligation "to designate, in writing, a natural or legal person as its legal representative in the Union".

LITHUANIA

We do positively welcome the initiative, it is timely and needed, but we would like to highlight and pay your attention on the protection of personal data and privacy of communications. It is important to highlight, that restrictions must equivalence certain requirements. It has been clarified in the practice of European courts that in cases where access to the content of the correspondence is granted, it is considered that the mentioned condition is adversely affected / there is a risk of its violation. This must also be taken into account in the context of the CSA Regulation.

In addition, case law emphasizes the importance of security measures for electronic correspondence, including encryption. Thus, the CSA Regulation cannot include provisions that weaken the protection afforded by encryption (for example, by opting out of clauses where encryption is not used or where weaker encryption solutions are used). Security measures are basically selected based on the results of a risk assessment, but even if such an assessment has been carried out, the relevant provisions of the CSA Regulation are too abstract in this regard (for example, Art. 3 (d.c,d), Art. 4 1 paragraph‘s (a, b, p), Art. 7, paragraphs 5, 6, Art. 7 also in relation with the scope of application). CSA Regulation cannot impose an obligation on service providers not only to provide their services, but also to proactively forward electronic correspondence to third parties, thereby enabling providers to adopt weaker encryption/security solutions in order to comply with certain obligations imposed on them (thus denying respect fundamental rights).

Herewith, we provide our practical comments/remarks to the text:

Art. 3 and 5 (Risk assessment; Risk reporting):

We have a question about risk assessment control - who and in what way will ensure and assess whether companies carry out risk assessment? Will the risk assessment be used internally or will it be submitted to a law enforcement agency for evaluation?

Art. 4 (Risk mitigation):

In our opinion, service providers will have a heavy workload to carry out service monitoring, risk assessment and content removal. Small service providers, which often have only 1-3 employees, may not cope with such responsibilities. Practice shows that illegal content is often found in such companies, because they can offer good prices. Who will control these companies and enforce the CSA Regulation?

Art. 7 (Issuance of detection orders):

The proposed procedures are very complex and compared to current practice will make the process of removing content and transferring information much more difficult and lengthy. Estimated deadlines are unfathomably long compared to our everyday practice.

MALTA

General considerations

Malta appreciates and wishes to thank the Commission for the preparation of further flowcharts ahead of the next LEWP meeting in September. This greatly assists delegations as well as local authorities in understanding further the process behind the aims and objectives of this legislative proposal. Malta also wishes to thank the Commission for continuing to clarify the role of law enforcement, the nature of the coordinating authority, its interaction with existing national mechanisms and its explanation of the role of the INHOPE Network.

Comments on child protection regarding the EU Centre and its potential awareness raising role:

- While in principle this is viewed positively, this function is already being carried out by Insafe through Safer Internet Centres (SICs) and internet helplines and via the Better Internet for Kids platform by providing the sharing of expertise, case studies and resources. Should the EU Centre also assume a similar role, its contributions should be forwarded to SICs and other relevant stakeholders with a view to ensuring that the awareness raising measures created by the EU Centre are adopted amongst all Member States. Nonetheless, it is imperative to retain focus on one of the gaps that EU Centre has been envisaged to fill, that is, to produce quality reports on child sexual material. To this end, existing work strands should be viewed carefully in order to avoid duplicating the work of such other relevant stakeholders in the field and reducing the efficiency of the EU Centre. Therefore, for example, Malta would welcome a flowchart on the interaction between the EU Centre, Europol and other relevant stakeholders.
- Malta would also like to continue emphasising the work of INHOPE which has significant expertise on child sexual abuse material – being a membership organisation for a vast number of hotlines around the world. The hotline analysts, currently operating on analysing the material and classifying it, are part of INHOPE. Hence, it is essential that the expertise gained by INHOPE members and INHOPE itself, as the pioneer organisation in tackling child sexual abuse material is taken into account when further exploring the role of the EU Centre. To this end, Malta supports Estonia's call on this. Malta also welcomes the Commission's suggestion of a document or alternatively a presentation providing information on how INHOPE would function alongside this legislative proposal. In line with our previous call on continuing to recognise the important work of hotlines, Malta continues to support Belgium's and the Netherlands' suggestion to include a reference to INHOPE and hotlines to solidify their significance.
- Further information is also being requested on how the EU Centre can focus on the offline aspect of online child sexual abuse, that is, articulating better the positive impact of the legislative proposal on the support measures envisaged for victims and survivors. This is considered as a crucial aspect, regardless of whether persons affected by child sexual abuse have reached the age of majority or not. Removing or drastically reducing the 'online permanence' of photos and videos should be a key priority to assist victims and survivors in living out their lives offline peacefully. Measures and information on how such persons can be assisted from primary and secondary instances of child sexual abuse trauma would be useful and should be considered in the discussion about the functions that the EU Centre may assume.

Comments relating to further considerations on chapter 1 and 2 of the legislative proposal following deliberations in past meetings.

Article 12

Malta would like to ask for further clarification on the reporting obligations, specifically on the reasoning behind the reporting to be sent only to the EU Centre rather than including also the Safer Internet Centres and law enforcement, in order to keep relevant stakeholders informed.

Articles 20 and 21

Malta concurs with other delegations that the wording in Article 20 and Article 21 should be further articulated to ensure that persons requesting information about child sexual abuse material depicting them includes children and therefore physical persons under the age of majority (18 years old). Representation rules and familial situations including protection from parents or guardians perpetrating the sexual offence should be explicitly referred to and reference to the application of EU legislation on victim protection and support should be inserted.

THE NETHERLANDS

The Netherlands acknowledges the problem of Child Sexual Abuse Material (CSAM) and the urgency to prevent and fight child sexual abuse. In recent years, the Netherlands has made great efforts to reduce the amount of CSAM on Dutch networks. The Netherlands is a major proponent of a joint European approach to combat child sexual abuse material, particularly given the fact that the Internet so easily crosses national boundaries. We are therefore pleased that the European Commission has published a proposal that should enable the Member States to fight child sexual abuse more effectively and jointly, all across Europe. We applaud the efforts of the Commission and we welcome the proposal, although we also have various questions and concerns. The Netherlands appreciates the possibility to ask questions about the proposal and looks forward to the Commission's responses.

General remarks

The Netherlands supports the premise of the proposal that both member states and internet service providers have a joint responsibility in preventing and combating CSA. At the same time, the Netherlands has concerns about a number of aspects of the proposal because the proposal not only appears to infringe on the right to privacy, the right to data protection and the communication confidentiality of citizens, but may also harm the security of the internet. These concerns focus specifically on the obligations imposed on providers of hosting services and interpersonal communication services to scan content and, in specific cases, possibly decrypt communications. It should also be mentioned that the proposal is technology-neutral, which makes it unclear how encryption will be affected.

Consequently, The Netherlands has some questions with regard to the detection order. The questions mainly focus on how such an order fits into a proportionate and efficient approach to prevent the storage and dissemination of CSAM and the impact on the security of communications and other data.

The Netherlands considers it important that the proposal does not lead to general monitoring and that proper safeguards are applied to prevent materials from being wrongly classified as CSA, especially when automatic decision making is applied. The Netherlands is committed to tackle CSAM effectively, but that the restriction of fundamental rights should only occur when it is strictly necessary and proportionate and is accompanied by safeguards.

Questions art. 8 – art. 24

The Netherlands appreciates it if the Commission can clarify some questions about the following articles.

Article 8

- Article 8(1)(d) states that a detection order contains the specific service offered by the provider to which the order is directed. This would mean that a detection order would require a provider to detect CSAM or grooming on its entire service through the measures set out in the detection order, including the indicators and safeguards. How does this relate to Article 15 of the Electronic Commerce Directive (2000/31/EC), Article 5 of the ePrivacy Directive and Article 7 of the future Digital Services Act (DSA), which state that Member States may not impose a general obligation on service providers to monitor information they transmit or store, or to actively seek to facts or circumstances indicating illegal activity?

Article 10

10(1)

- Could the commission indicate the type of technology used to detect old and new CSAM and grooming?
- How will the Commission ensure that employees are prevented from seeing CSAM when detecting new material?
- Is it correct that the Commission considers that detection orders can be executed without weakening the encryption by applying detection to the end points? Can the Commission clarify this explicitly?
- Regarding the detection of CSAM and grooming: does the detection order in the proposal mean that material cannot be uploaded, or that it is removed after it has been uploaded?
- Can the Commission assure that the used technology is not intended to prohibit statements, in this case CSAM and grooming, before they are made public (uploaded) on the Internet? The Dutch Constitution gives everyone the right to publish their statements, this also includes CSAM. The Dutch government cannot prohibit this in advance merely based on the content.

10(3)

- Can the committee clarify why freedom of expression is not mentioned under point c?
- Regarding the use of indicators: could the Commission elaborate on the use of these indicators, and more specifically, on how the technology would ensure that information unrelated to CSAM is not extracted maliciously, for example by adding other indicators?
- Article 10(3)(c) states that the technology will be "the least intrusive in terms of the impact on the users' rights to private and family life, including the confidentiality of communications, and to protection of personal data". Could the Commission elaborate on what is meant by 'least intrusive'? We would highly appreciate it if the proposal could be more specific.
- Article 10(3)(d) states that the technology shall be "sufficiently reliable, in that they limit to the maximum extent possible the rate of errors regarding the detection". 'The maximum extent possible' could potentially still include a significant rate of errors. Does the Commission maintain a threshold of maximum rate of errors allowed before the technology is employed?

10(4)

- Article 10(4)(c) ensures regular human oversight and, in particular cases, human intervention. Does the Netherlands correctly understand that this means that the detection undertaken by the provider is significantly based on algorithms?

Article 13

- Article 13(1)(c) states that the report shall include "all content data, including images, videos and text". Could the commission clarify why all content data needs to be included and not only the relevant content data?
- Article 13(1)(g) states that the report shall include "information concerning the identity of any user involved in the potential online child sexual abuse". Does the Netherlands correctly understand that this includes information concerning the identity of the potential victim?

- Reporting the identity of an Internet user can be important for law enforcement agencies and for the protection of victims. However, there are also potential risks that come with both the detection and the dissemination of information concerning the identity of internet users. This information could be potentially used for blackmail or other types of abuse. How does the Commission intend to keep these potential risks from materializing?

Article 15 (4)

- Article 15 (4): The judicial authority or independent administrative authority might decide to extend the period referred to in point (a) by six weeks. Does the judicial or administrative authority take the initiative to extend by six weeks, and if yes, how does the authority reach this conclusion?
- Could other bodies submit a request to extend to the judicial or administrative authority, and if yes, by whom?
- Is there a maximum number of times this request can be granted?

Article 16

- Does the Netherlands understands correctly that the proposal is primarily aimed at combating CSAM by means of a removal order addressed to an hosting provider or interpersonal communication provider? And if that proves to be impossible, then only a blocking order can be issued against an Internet access provider? Can the Commission make an estimation on the number of cases in which it expects a blocking order to be necessary?
- Article 16 (6): The duration of a blocking order may not exceed five years. Considering the impact of the (execution of the) blocking order on the fundamental rights of its users, this seems to be quite an extensive period. Based on what grounds did the Commission concludes that this period would be suitable and necessary for the providers to take the necessary measures to prepare and execute blocking orders?
- Is the amount of users affected by a blocking order a relevant parameter that must be taken into account when issuing a blocking order?

Article 17

- Can the Commission clarify on why the blocking order does not provide for force majeure, similar to Article 14(5)?

Article 19

- What is the relation of proposed Article 19 of the CSA Regulation to Articles 12 to 14 of the Electronic Commerce Directive?

Article 20

- Would it be sensible to also add parents/carers to the list of those who can make a request for information?

Article 21

- Why is the request for support first sent to the coordinating authority and then forwarded to the EU Centre? Why can't a request for support be made directly to the EU Centre?

POLAND

Poland upholds an analytical reservation due to the ongoing process of national consultations. The official position of PL has not yet been developed and all comments are preliminary, resulting from the general analysis at the expert level so far.

General comments concerning hotlines - the draft regulation provides for receiving reports from service providers, but does not mention receiving notifications/reports from users of Internet products and services, (public report handling capability"), which is currently the domain of INHOPE's hotlines. With the above in mind, it is crucial to define their role in the entire process presented in the flowchart. What will the reports of natural persons look like: on the one hand, we have an obligation for the service provider to establish a mechanism for handling reports from users pursuant to Art. 14 of DSA, on the other hand, we have a well-functioning helpline system that can act as a trusted flagger also under the DSA (Art. 19). However, the hotlines work together with law enforcement authorities, in the case of PL with the Police, this fact should noted in the process of issuing warrants. The proposal does not explicitly mention the possibility of proactively searching cyberspace in terms of CSAM, which is already practiced by some hotlines.

General comments concerning judicial authorities - It should be noted that the mechanism provided for in the draft regulation for issuing orders by courts (judicial authority), seems to impose completely new additional obligations on the common judiciary. It will also be associated with the provision of appropriate full-time support and therefore requires in-depth analysis as to the justification of this solution and the possibility of its implementation. Regardless of the above, the acceptance of the procedure for issuing detection orders by courts will require appropriate preparation of judges. Judges issuing rulings in such cases will need to have legal knowledge and knowledge of new technologies. It is questionable whether issuing detection orders by courts will ensure immediate removal of harmful content. It will require the preparation of an application, its submission and then examination. These are time-consuming activities, but speed is important when removing content to prevent children from being subjected to secondary victimization.

Article 7 para 9 - the question of the duration of the removal order - we have 24 months for CSAM and 12 for grooming - how will the process carry on later? If the service provider offers the service on a permanent basis, offers the same functionalities, and children use them constantly, it can be presumed that that the risk of using them for sexual abuse is consistently at a similar level. The risk may be mitigated by detection order and application of appropriate technologies. The service provider is required to update the risk assessment 2 months before expiry period of application of the detection order, but the process of issuing a new one will take longer, taking into account all stages of the consultation. We identify a certain gap here.

Article 8 para 3 - the issue of manifest errors of orders - clarification is needed as regards what do we mean by "manifest errors" and "sufficient information". What we consider to be a sufficient formal defect to prevent the order from being executed, to eliminate the possible margin for violations and limit the flexibility to comply with the order.

Article 9 para 1 - the issue of redress (appeal) - whether taking into account the content of paragraph 1 can it be assumed that the order may be appealed against to the court that issued it?

Article 10 para 6 - the issue of informing the user about a detected CSAM - it is worth to consider to introduce general presumption that the user is not informed, pending confirmation by the national law enforcement authority and Europol (not "or"), providing that this will not interfere with the investigation.

Referring to all articles on informing responsible users by providers, i.e. perpetrators, that detection order, removal order or blocking order have been issued (Article 10 para 6, Article 12 para2 and Article 15 para 3)) - although there are reservations under which conditions such information takes place (or does not occur - when it comes to blocking), however, the very idea of providing such information may be doubtful. Moreover, while there is a possibility of not informing users, the indicated time frames (3 months in Art. 12 and 6 + 6 weeks in Art. 15) may be too short for operational and investigative activities to be properly carried out. Wouldn't it be better to apply in each of these provisions the solution adopted for Art. 10 paragraph 6 without indicating any time frame? There is no time frame indicated there, only if Europol and the law enforcement authority of the MS decide that informing the user will not interfere with preventive, investigative, detection and trial activities, the provider will be able to inform the user without any obstacles.

Why is the time frame used sometimes “once in months” and “once in weeks”? Consideration should be given to standardizing this issue throughout the draft regulation and the use of one measure, e.g. in months.

Article 12 - reporting obligations - securing the interests of law enforcement agencies and the interests of the proceedings against the person posting or creating the CSAM should be taken into account, especially when it comes to informing the user about the procedure with the content posted by him.

Article 14 - removal orders - has the EC considered differentiating between detection orders and removal orders? Has a different mode / procedure for issuing both been considered, taking into account the different degree of interference with fundamental rights? The EC explained that the reason for the different structure of issuing orders in the TCO and CSA was precisely the degree of interference with fundamental rights. While the situation is different for a long detection process involving different technologies, what is the difference when an authority has identified an online CSAM or online terrorist content - both require prompt removal, with a child being the victim in CSAM and the risk of secondary victimization is significantly bigger.

In the flowchart shown, the removal order appears as a consequence of the detection process. What will be the removal process if the detection is not necessary as the content has already been identified as CSAM and what will be the role of the EU Centre?

During the previous LEWP meeting PL has already presented the initial first impression assessment in relation to the order issuing procedure (Articles 7, 14 and 16), that the proposed structures and procedures (based on practically the same principles) for obtaining individual orders seem to be significantly bureaucratic, complex (many entities involved) and extended in time (as can be seen in the flowchart). The process of obtaining orders should be quick and easy from a formal point of view. CSAM moves quickly on the Internet and before the removal order or blocking order procedure is completed, CSAM may not be on the server anymore.

Suggestions of the topic for the workshop in September

Article 10 para 3 - in accordance with art. 10 para 3, service providers will use the technologies provided by the EU Center, those technologies "shall be (a) effective in detecting the dissemination of known or new child sexual abuse material or the solicitation of children". It should be assumed that the technologies mentioned here, in relation to "known CSAMs", will use the exchange of information about hash values, therefore it will be necessary to obtain additional information in this regard, especially which hash value lists the Center will use, including how they will create and share such lists.

In addition, any decisions regarding “notice and take down" actions should be made on the basis of reliable lists of hash values, hence the issue of the method of classifying content as CSAM used by this Center will be crucial here. A "reliable" list should be understood as one that is created as a result of a process based on a uniform CSAM classification system, taking into account the experience resulting from the exchange of information and training, especially at the international level (INTERPOL). A frequently used rule here is the verification of the classification given to the CSAM by three people in order to obtain full agreement in their opinion. Currently, it is the domain of the INHOPE helplines.

PORTUGAL

Although PT still has a scrutiny reservation on this proposal, we have the following preliminary comments.

Our major concern relates to the possibility of intrusiveness of technologies in fundamental rights, especially during the risk assessment phase; because it obliges providers to look into the manner in which users use the service.

This is particularly noticeable when we compare this phase to the other phases.

First, it appears that we do not have more than two safeguards (article 3.3 and article 3.6) none of them compulsory. At least some binding parameters could be introduced, or even a similar process or principles already in the text to this phase: for instance, this is the case of the process designed for the orders, the principles of redress and information (article 9) and the principles applied to technologies and safeguards (article 10). We could not find any provision with the consequences of not compliance of the requirements.

We also have doubts about the time limit of this kind of assessment.

We would welcome some clarification on this subject and a focused discussion on the foreseen possibilities.

Also keeping in mind our scrutiny reservation, and in general terms we find that participation of children should be included in this Regulation, as well as more attention to the rights of the victims in terms of a child friendly justice and avoid the possible duplication of circuits.

Article 8(2) The communication must be drafted in the official language of the national authority because, given the jurisdictional nature of the processing, it is subject to procedural rules of the respective jurisdiction; on the other hand, the fact that the recipient entity chooses a certain legal order in which to establish itself, this already generates legal and contractual linguistic obligations.

Furthermore, the entity to whom the communication is addressed in the case of Article 8 2§3 is a private authority probably having at its disposal means which public entities might not have. That is why it seems excessive to us that the order has to be communicated in the language that the supplier has chosen to declare under the terms of article 23, paragraph 3.

Without forgetting that this requirement translates into more costs for the National Authority, for which reason we propose a rewording of these norms.

Article 9 We agree with this standard in principle, but we wonder whether it should not also be extended to risk assessment. It is difficult to qualify who are the "users" affected by the measures taken to execute them. For example, they will include potential users of the services provided?

We note that the use of broad and indeterminate expressions such as "without undue delay" can be a difficulty.

Article 10 we consider that this principle should also apply to the risk assessment phase.

Article 10(3) We would also be in favor of the establishment of a new rule with general principles related to encryption.

It is understood that the indeterminate concepts used are not sufficiently densified in relation to the use of self-owned technologies; who is responsible to evaluate and certify the technologies that are not provided by the Centre?

The question also arises as to who evaluates and certifies the self-owned technologies?

Why not apply an impact assessment like the one provided for in Art. 7.4 b) and c)?

Article 11 We consider that the issuing of guidance should always be mandatory, even if its application is not. The article should also contain a (non-restrictive) indication of what matters should be covered by the guidelines. The more detailed the guidelines are, the more harmonization and effectiveness will be guaranteed at national level

Article 12(1) We would like to understand better the relation of this article to data protection, especially in the relationship with third states (USA).

ROMANIA

RO-supports the overall CSA Regulation proposal, as we have previously stated. Nevertheless, we have some **comments on** the draft regulation:

1. Regarding the processes described, such as detection, we think that there should be more flexibility in in the processes described, in order to avoid over-regulating. There are successful procedures that already exist and operate at national level. Involving multiple authorities in issuing removal orders would lengthen the process.

Regarding the **removal orders** for the Internet Providers or the Providers that offer hosting services, as we also previously stated, RO has the legislative framework to delete materials with pornographic content.

The same comment as above applies, that there should be more flexibility in the processes. Issuing one separate order for each step (detection, removal) would overload and lengthen the process.

The LEA's role in the Regulation should be more clearly stated.

2. The authorities involved in the process:

According to the requirements provided by the regulation, the Coordinating Authority is an administrative, independent entity.

How will this administrative entity determine whether, according to the legislation in force, a photo-video material constitutes pornographic material with minors? Will the LEA need to be involved in this process?

How will the CA verify the orders issued by a judicial authority?

3. Regarding the **establishment of the EU Center**, Romania kindly requests further clarifications on the added value it would provide:

- In the case of NCMEC reports, could this center categorize these reports in accordance with the legislation of each country and eliminate irrelevant reports?
- Will it be able to transmit other relevant checks, such as: OSINT checks regarding the entities, e-mail addresses, nicknames that appear in these reports?
- Will it be able to cross-check with other databases, such as IVAS, the Europol's database?
- What happens when a client is trying to distribute materials using an FTP service?
- Will this Center have access to the Interpol ICSE database, in order to communicate directly, when a NECMEC report is sent, if the materials are known internationally or not, or, for example, if the victim appears or is not identified in the ICSE database?
- How will it proceed in cases where we have users who use proxy or VPN services? What about the users who have saved the materials in the cloud and the server is in another country, such as the US or China? (There are technologies that can detect that such a service is being used, but it cannot give you the recipient. Therefore, other evidence is needed in order to determine to which country to send the information to.)
- In case of transmission of encrypted archive type files, what could the new Center do?
- It is important for the LEA to receive the most relevant information in order to be able to react as quickly as possible in such cases. What added value would this center bring to the support already provided by Europol?

SLOVENIA

General scrutiny reservation on the document and scrutiny reservation on articles 8 to 15.

We support the Regulation of the Commission in the field of combating sexual abuse of children.

Article 8 (paragraph 2) of the provisions makes it clear that the detection order is executed by the authority that issued the order, i.e. the court. Will this be the case in all cases? Can the court order another state body to execute the order?

General comment on the discussed articles: What will be the role of law enforcement? In what part of the process of obtaining an order or executing a detection, removal or blocking order will law enforcement be involved or they will expect to be involved?

Article 10 (Technology) - Is there technology to detect child solicitation or CSAM on encrypted networks? How good is this technology in terms of respecting the right to privacy?

Article 10 (paragraph 4) – it is clear from this paragraph that after the implementation of the detection order, IT service providers will have to check whether the technology they use for this is effective. A regular human oversight is specified in order to ensure that the technology works, especially when errors occur. Here, we have a reservation, mainly about the fact that to some extent the providers will have to assess that it is an error. In doing so, they will take on the role of determining which content is legal and which is illegal. How will the Commission avoid this?

Article 12 (paragraph 2) stipulates that in cases where, within a period of 3 months, the provider receives a message from the EU Center that the information will not be forwarded, the provider informs the users who were affected by the obtained information after the expiration of the period from the said message. This time is too short considering the amount of reports that the law enforcement authorities receive and the specifics of the investigation.

Regarding CSAM detection technology, our question is mainly if there is technology to detect child solicitation or CSAM on encrypted networks? How good is this technology in terms of respecting the right to privacy? How about VPN? We are very interested in workshops on existing technologies. However, it would be good if the information officer would also attend these workshops.

Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 08 September 2022

WK 10235/2022 ADD 2 REV 1

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.

MEETING DOCUMENT

From: To:	General Secretariat of the Council Law Enforcement Working Party (Police)
N° prev. doc.:	9068/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations on Articles 8 to 24

Delegations will find attached the compilation of comments received from Members States on the above-mentioned proposal following the meeting of the LEWP (Police) on 20 July 2022.