Council of the European Union
General Secretariat

**Interinstitutional files:**
**2022/0155 (COD)**

**Brussels, 13 December 2022**

**WK 10235/2022 ADD 9**

**LIMITE**

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

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

**WORKING DOCUMENT**

| | |
|---|---|
| From:<br>To: | General Secretariat of the Council<br>Law Enforcement Working Party (Police) |
| N° prev. doc.: | 9068/22, 14143/22 |
| Subject: | Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse<br>- comments from delegations on Chapters I to III |

Delegations will find attached the compilation of comments received from Members States on the abovementioned proposal following the meeting of the LEWP (Police) on 24 November 2022.

**Written comments submitted by Member States**

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

**(9068/22)**

## Contents

# AUSTRIA

Regarding Article 7:

In the past AT has been especially critical of **Article 7** of the Proposal. As the current, second compromise text on Chapter II does, again, not contain any changes to Article 7, the Ministry of Justice refers to the past written comments on Article 7, especially from 22.7.2022, which, for good measure, are also included in the attachment.

Again, we point out that we harbour major concerns regarding the **infringement of fundamental rights**, especially the right to privacy and the right to data protection, and therefore call on the Presidency to arrange a meeting or workshop where data protection concerns regarding the Proposal can be discussed.

Furthermore, we strongly suggest that the entire provision is overhauled and simplified linguistically. It is apparent that the proposed instrument represents a serious encroachment upon fundamental rights, therefore the provision establishing it must be **as clear and precise as possible**.

As we understand it, the Presidency is currently awaiting the expert opinion of the Council Legal Service particularly on the compliance of Article 7 with the Union's fundamental rights regime. In this context we would like to make note of the **Joint Opinion of the European Data Protection Board and the European Data Protection Supervisor, No. 04/2022**, which was published on 28 July 2022 and contains a detailed analysis of the proportionality of the envisaged measures (see EDPB/EDPRS Joint Opinion 04/2022, p. 16 Paragraph 38 et seq.)

In the analysis the EDPB/EDPS list and consider all factors that contribute to the assessment of the proportionality of detection orders (see p. 19 Paragraph 49 et. seq.) and concludes that the detection order as it is currently proposed raises serious concerns and "invites the co-legislators to amend the proposed Regulation, in particular to ensure that the envisaged detection obligations meet the applicable necessity and proportionality standards and do not result in the weakening or degrading of encryption on a general level" (see p. 36, Paragraph 137).

Regarding Articles 12(2) and 22(2):

There is a need for in-depth discussion in order to take the requirements of the Law Enforcement Authorities into account accordingly.

Regarding Article 26:

Taking into account the tasks of these authorities and their intervention intensity, especially the intense encroachment on fundamental rights, they have to be absolutely independent.

Data protection comments on Chapters I and II of the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse:

Due to current time restraints it has not yet been possible to examine Articles 8 to 24 in detail; therefore, we would like to enter a special scrutiny reservation for these Articles in addition to our general scrutiny reservation concerning the entire Draft.

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 refered 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.

We therefore strongly suggest that a special workshop should be organised which focuses on the data protection aspects of the Proposal with the involvement of national data protection experts. Alternatively, the VS could also consider organising a Joint WP Meeting with LEWP and WP Data Protection.

# BELGIUM

We are grateful for the interesting discussions that have taken place during the past months on this file, together with the Czech Presidency, the Member States, the Commission and the Council Legal Service. We maintain a positive scrutiny reservation the whole text of the proposal, but welcome warmly the spirit of the amendments that have been made so far by the Czech Presidency. We are still studying the impact of these amendments. We look forward to the further work on the text, that should enable an effective and proportionate result to prevent and fight CSAM. Our current comments on Chapter I, II and III can be found below.

**Article 1**

We confirm our doubts about including audio communications in the scope of the proposal.

We support the suggestion to refer to the Europol Regulation in paragraph 3 of Article 1, to ensure that the new possibility of a direct exchange between Europol and private partners concerning CSAM is preserved.

**Article 3**

We suggest to look into a more detailed formulation of paragraph 6 of Article regarding the Commission's guidelines on the risk analysis. This could help form a better and more clear basis for the evaluation of the remaining 'substantial risk' in Article 7 to determine whether a detection order is necessary and proportionate.

**Article 7**

We would like to hear about the different possibilities to ensure there is no gap between two necessary detection orders. Is the updated risk assessment to be provided now four months before the end date of the detection order sufficient, taking into account the lengthy procedure for a detection order? We would also like to inquire whether the possible adaptation of the detection order in the second section of Article 9(4) could also include a prolongation (which would in time still be limited to the maximum period of 24, or in case of grooming 12, months).

Like the Commission and some other Member States, Belgium has a preference to return to the original formulation in paragraph 7 of Article 7. In reality grooming can also take place by, for example, a 17-year-old towards a 13-year-old. In Belgium as in other Member States grooming by a minor is also a crime. We thus prefer the original formulation because this ensures action in all cases of groomed minors.

**Article 9**

We support the request to streamline the amendments in Article 9(2) throughout the text. This requires similar changes in Article 15(2), Article 18(2) and Article 18c(2).

**Article 10**

We are interested by the Finnish suggestion to include in Article 10 some additional requirements for the detection technologies, namely that they should be 'be effective, suitable and not easily circumvented (…)' in Article 10(3)(a) and that they should 'not be able to extract or deduce any other information (…)' in Article 10(3)(b).

**Article 12**

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

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

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

**Article 14**

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

**Article 14a**

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

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

**Article 16**

We confirm our current understanding that blocking of new CSAM by internet access service providers is not an option and not desirable. We would like paragraph 1 of Article 16 to refer only to known CSAM as originally formulated.

Furthermore, we have strong doubts about the deletion of all elements requiring proportionality of blocking orders in paragraphs 4 and 5 of Article 16. It seems like an important guarantee to ensure a well-balanced mechanism.

We have requested multiple actors and multiple Member States but have found no situations in which individual URLs other than the top-level URL can be blocked by the internet access service provider. We would like to ask the Commission about the countries that supposedly have this technical possibility.

We would like to see the blocking order also addressed to the DNS (domain name system) service providers in paragraph 1 of Article 16, because it is less and less the case that the internet access service provider himself manages and therefore can block the domain names. This addition is very important to ensure the implementation of a blocking order. A definition of the DNS service providers can be found in the NIS (Network and Information Security) 2 – Directive.

We understand the reasoning that the blocking order ideally is considered if a removal order proves fruitless, for example because a hosting provider in a third country is not giving effect to it. However, we wonder how all the Member States will be informed about the non-execution of a removal order. Every Member State has a stake in this, because every Member State would have to order its own internet access services providers and its DNS service providers to block a certain URL. So how do Member States know that it is time to consider a blocking order? This is also linked to the fact that the authority issuing a removal order can request the assistance of the EU center to assess the implementation of a removal order by the provider, as referred to in Article 25(7)(d) and Article 49(1)(b).

Furthermore, we wonder whether the hosting provider also requires a right to challenge the blocking order, next to the user and the internet access service provider.

In Article 16(7) we notice that the coordinating authority would be the authority to assess the necessary modifications to the blocking order. We believe this should be entrusted to the competent authority itself, because they are best placed to evaluate the necessity of a blocking order.

**Article 17**

We would like to learn more about the reasons for including the sentence *"Where relevant, the blocking order shall also be communicated to the providers of online search engines under the jurisdiction of the competent authority"* in paragraph 3 of Article 17. Is this linked to the liability of a provider of search engines, namely that they are liable if they are informed of a blocking order and they do not act upon it? What are the Commission's views on the consequences of the fact that the URL list of known CSAM in this way would be sent to providers of online search engines without any individual assessment?

**Article 18**

In paragraph 5 of Article 18 it seems that the question whether the access of users was wrongly blocked and the question whether there is a need for modification or revocation should be assessed by the issuing authority, namely the competent authority. This is based on similar reasons as listed above for deleting Article 14(3a).

**Article 18a**

We wonder about the used phrase "a particular website", which is different from the terminology "URL" used in Article 16(1). Only with search engines "website" is used in the Regulation. Should we not use "URL" everywhere?

**Article 21**

We are grateful for the addition in paragraph 3 of Article 21 that clarifies that victims should be able to indicate the specific providers and are open to moving this to paragraph 2.

**Article 22**

We support Article 22 as a legal basis for data retention. It is essential to foresee this in the Regulation in order to be able to effectively address CSAM. We should however be sure that the text cannot be interpreted in a way that current legal possibilities in the Member States, such as for example legislation that enables data retention for certain entities or other crimes is not affected. We should be ware of minimalistic interpretations that would conclude that data can only be preserved for those purposes as listed in paragraph 1. In the English, Dutch and French versions at least we interpret the words chosen to mean that those providers can only preserve data for those purposes and not for other purposes (even if national legislation permits this). Furthermore, if we follow the reasoning of the Commission that the textual structure in paragraph 2 foresees that Member States can also limit the period to less than 12 months, it seems also that Member States could limit the purposes for which the providers should preserve the data. We believe that these elements should probably be clarified in the text to avoid misinterpretation later on.

As related to the content of the Article, we believe all the necessary elements are covered. No further rules related to the access by law enforcement authorities and justice actors should be included. The national rules and conditions play an essential role in this regard, taking into account also the relation with other data retention rules on the national level. Next to this, we consider 12 months to be an appropriate time period. This time period is necessary in our experience.

**Article 23**

We are still not clear on the difference and the relationship between the point of contact and the legal representative, if both should be established in the EU and only one of each should be created. Is the point of contact meant to make sure certain well-established contacts with one specific Member State can be preserved? Or is it desirable for a provider to be legally present in one Member State but practically operating from another? We would like some clarifications on this.

**Article 24**

In paragraph 3 of Article 24 we suggest to use the singular of "*legal representatives*" because, as we understand it, each provider will only have one legal representative.

**Article 25**

- In the title of section 1 of Chapter III we recommend using either "*Authorities of the Member States for child sexual abuse issues*" or "*Coordinating Authorities for child sexual abuse issues and other competent authorities*" as in Article 25. National authorities is a term that will probably not be appropriate in all cases if for example also local prosecutors are designated to act.
- As a minimum we would like to suggest a period for appointing the competent authorities in paragraph 1 of Article 25 similar to the periods in the Terrorist Content Online Regulation or the Digital Services Act, namely respectively 13 and 15 months after the entry into force.
- We confirm for paragraph 7(d) of Article 25 that it remains useful for the authorities to be able to request an opinion of the EU center about the effectiveness of a removal order. This is useful in order to assess whether as a subsequent step blocking orders are necessary.
- Paragraph 9 of Article 25 seems to have as a consequence that each competent authority (for example the police) needs to have all the investigatory and enforcement powers of Articles 27 through 30 and needs to be able to carry out searches on publicly accessible material following Article 31. This seems contradictory to the attempt to be able to delegate certain tasks to different authorities.
- Paragraph 9 also needs to be assessed together with the independence requirements in Article 26, see our comment below.

**Article 26**

The addition in paragraph 1 of Article 26, read together with paragraph 9 of Article 25 is not acceptable to Belgium. For example, the police receives instructions from the prosecutor's office and could therefore then not be a competent authority in this Regulation. We prefer to work on the basis of the text in the Terrorist Content Online Regulation. We have a scrutiny observation for this element, because we would like to know for which tasks and aspects (which kind of) independence is required for Coordinating Authorities and competent authorities.

**Article 32**

In Article 16 of the Digital Services Act are minimal requirements listed that apply to notices that arrive via the Notice and Action Mechanism of the provider. It should be clear – at a minimum via the recitals – that those remain valid, which could be subject to doubt due to the different formulations in Article 32 of the CSA Regulation. Also, we still would like to see a concrete reference in the text to Article 16 of the DSA 'Notice and Action Mechanisms', to make sure the link is evident.

**Article 34**

We are interested in possible suggestions on how to make the complaint mechanism better through possible formats for forwarding the complaints to the Member State of establishment (which could be designed by the Commission later-on) or through listing requirements before forwarding.

**Article 37**

In Article 37(1) we would like to know why the Commission is given the task to recommend a Coordinating Authority to assess an infringement if at least three Member States are involved. How would the Commission become aware of the related information? Why is the EU center not better placed for this? Which services of the Commission would be tasked with this?

**Article 38**

Belgium reiterates the request – also of several other Member States – to amend Article 38 on joint investigations and to make it more concrete and explicit concerning the potential partners, the leading authorities, etc. Also, the coexistence with Joint Investigation Teams and other cooperation mechanisms should be clarified. A Coordinating Authority could, via the delegation of certain tasks to competent authorities, be also a law enforcement agency or the prosecutor's office. Therefore clarity is needed on coexistence with cooperation as coordinated by Europol and Eurojust.

In relation to Article 38(2) we note that the Commission is listed to receive the results of those joint investigations. We would appreciate some clarification about the reasons for this and about the nature of those results to be shared. Joint investigations seem to be able to deal with for example the issuance of orders but also about infringements of the Regulation as well as concrete requests of victims.

**Article 39**

A similar request concerns the reasons for including the Commission in Article 39. What are the specific tasks for which the Commission requires for example access to the information sharing systems?

**Proposals for the recitals**

- We propose to make (more) explicit reference to the existing and remaining obligations in recital 22 and Article 6 of the Digital Services Act to act expeditiously to remove or disable access to CSAM upon obtaining actual knowledge thereof. It should be clear that providers are not to wait for removal orders or notifications by authorities.
- We propose to make (more) explicit reference to general rule as described in recital 27 of the Digital Services Act to direct orders to the specific provider that has the technical and operational ability to act against CSAM. Reminding this would help to establish the proportionate nature of detection orders where they are necessary.

# CROATIA

Concerning the revised Chapters I, II and III of the CSA Regulation (compromise text in document 14143/22), Croatia can support the following changes to the Regulation:

Chapter I

The amended definition of the term "child user" is supported, which now means any natural person under the age of 18, in order to harmonize all definitions regarding the age limit. The proposed age limit of 18 years is in accordance with the legislation of the Republic of Croatia.

Chapter II

The proposal of the Presidency is supported in section 4, 5 and 5a, which refer to the provisions on the issuance of orders for the removal, blocking of content according to which the said orders would be issued by a competent judicial body or another independent administrative body.

Chapter III

Croatia supports the position of Member States, which believe that it is particularly demanding to devise effective solutions for the establishment of coordinating authorities in accordance with the TCO Regulation, DSA regulation and this proposal, while respecting the requirements stipulated by those acts.

Croatia also supports the compromise text on this chapter and the proposed change from Article 25, according to which the deadline for appointing Coordinating Bodies in the State is extended to 6 months from the date of entry into force of the Regulation, as well as the proposed change in Article 26, which refers to the flexibility of requirements for the independence of coordinating bodies and definitions of independence from state administration must be adhered to.

Moreover, concerning document 15077/22, referring to the annual work program of the ATLAS network for 2024/2025, Croatia can support document 15077/22 and we have no additional written comments.

Finally, concerning documents 14808/22 and 14809/22, we currently have no comments.

# ESTONIA

Hereby we send Estonian positions on the draft Regulation of the European Parliament and of the Council, laying down rules to prevent and combat child sexual abuse (attached). Besides that we have some specific comments on chapters 1-3:

**Art 7** – We would like to hear the CLS opinion, whether this order breaches the no general obligation to monitor principle. Thank you for organizing the workshops! They were very useful. However, we are still unsure what kind of indicators would be provided by the database of indicators in cases of new CSAM and solicitation. Also, all the technical solutions available on the market today for detecting new content and solicitation require human oversight whether the content is CSAM. CJEU case-law on the general obligation to monitor principle emphasizes that the provider must not be required to carry out an independent assessment to evaluate whether the content is illegal. How is this requirement provided in this article, especially in cases of new content and solicitation? Also, there are no tools available at the moment, which are able to detect solicitation in Estonian.

**Art 7(5-7)** – We propose to delete the possibility to issue detection orders preemptively without there being evidence that the specific service is being used for child sexual abuse. The issuing of the detection order must be based on concrete evidence about the specific service.

**Art 7(7)** - Regarding the detection orders concerning the solicitation of children, the age of sexual consent in Estonia is 16. Also, it is not a crime if acts of sexual nature take place between a child 14-16 years of age and an adult up to five years older than the child (19-21). Therefore, in Estonia, there is no legal basis to monitor the communications between 16–17-year-olds and adults. Additionally, solicitation is a very nuanced crime taking place over a prolonged period and involving many different episodes. We are concerned whether such prolonged monitoring of personal messages is proportional and respects fundamental rights.

**Art 7(10 new)** – A provision protecting end-to-end encryption should be added to this article. End-to-end encryption is an important tool to guarantee the security and confidentiality of the internet infrastructure and the communications of users. Any weakening of encryption could potentially be abused by malicious third parties. Therefore, end-to-end encryption should not be weakened. We do not support the possibility of creating backdoors for end-to-end encryption solutions. At the same time, we can support the use of privacy enhancing technologies (PETs) that allow the analysis of encrypted content without decryption, so that the reliability, security and integrity of digital services relying on encryption is preserved.

We propose to add the following text to the article: ***The detection order shall not prohibit or weaken end-to-end encryption or oblige the service provider to provide encryption backdoors.***

**Art 14a** – we have here analysis reservation.

**Art 16(1)** – We prefer the COM original proposal and clear indication that only URLs included in the database of indicators should be blocked. Internet access service providers should only be obliged to block access to the material provided to them by competent authorities. They should not be obliged to monitor and block new CSAM since they only provide access to the internet and have no means of controlling the content of websites. This would infringe the no general obligation to monitor principle. Also, 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)** - Does the deletion of par 6 mean that blocking orders could be issued permanently? What measures are taken to reduce CSAM on these services? What measures are envisaged in this regulation? Need to assess the proportionality of a permanent obligation.

## EXPLANATORY MEMORANDUM

**Estonia's positions on the draft Regulation of the European Parliament and of the Council, laying down rules to prevent and combat child sexual abuse**

### 5. ESTONIAN GOVERNMENT'S POSITION

**5.1 Estonia supports the creation of a harmonised legal framework in the European Union with the aim of assisting the prevention of child sexual abuse on the Internet, including the republication of offending materials on the Internet, and to bring the perpetrators of such offences to justice.**

We consider the joint activities of the EU Member States, authorities and Internet service providers critical in preventing child sexual abuse and also emphasise the importance of cooperation with third countries.

**5.2 The definitions used in the Regulation must be clearly worded and the entitled and obligated persons, unambiguously definable. It is important to ensure the mutual coordination of the definitions in the provisions of different legal acts.**

Article 2 of the proposed Regulation contains a list of terms/definitions used in the document. Paragraph (i) explains that a "child" means any natural person below the age of 18 years, but the next paragraph (j) on the same page explains that a "child user" means any natural person below the age of 17 years. It is unclear what causes such a distinction between a "child" and a "child user". The Convention on the Rights of the Child defines that a child is a person below the age of 18 years and the definition of a child in the legal acts of the Republic of Estonia is similar. Therefore a "child user" should also be any natural person below the age of 18 years.

We find that even if it may generally be right to establish the definition of a child user on the basis of the age of sexual consent, the principles of terminology would not allow for a definition within the Regulation to be used as a component to define another term in the same legal act, but have a contrary meaning. This means that if a "child" is a person below the age of 18 years, a "child user" should also be a user below the age of 18 years. In the interests of clarity, a more suitable term should be found for the definition of a "child user", if possible. One possibility would be "protected child user". It may be appropriate to resolve the contradiction between the terms by not linking the definition of a child user to a specific age, but, for instance, to the age of sexual consent which indeed differs from country to country (in Estonia, this is currently 14 years, but will be 16 years as of 1 November 2022).

There is a significant amount of confusion over who would be the authorities that would fulfil the obligations established in the draft Regulation and this should also be taken into account when defining the terms. All the terms used in the Regulation must be explained, including "Coordinating Authorities of establishment"; "Competent Authorities"; "competent judicial authorities"; and "independent administrative authorities". Currently in the draft Regulation, the definitions are provided in the content text of articles (e.g. Article 25(1), 25(2)). There is no clarity as to which authorities are "Coordinating Authorities" or "designated Coordinating Authorities" and which ones are not Coordinating Authorities "of establishment" (Article 37(1)).

**5.3 The proposed Regulation must be drafted on the basis of: Article 3 of the United Nations Convention on the Rights of the Child and Article 24(2) of the Charter of Fundamental Rights of the European Union, pursuant to which the best interests of the child shall be a primary consideration in all actions concerning children. Children must be protected from sexual abuse in order to ensure their right to life, health and free self-fulfilment, while consideration must also be given to the children's right to have their private and family life respected and their right to personal data protection.**

In Estonia's opinion, the Regulation does not sufficiently take into account the need to respect the children's private and family life and the need to protect personal data, as it does not establish an exemption for intimate image and text material shared in mutually consenting children's communication. Such cases do not constitute materials of sexual abuse or an offence and therefore the identification and blocking of such material would unjustifiably violate the children's right to have their private and family life respected and their right to personal data protection.

Children and young people use communication platforms for mutually sharing intimate images and videos of themselves. Online communication has become a natural and important part of relationships between young people, including sexual relationships. Such activities are not condemnable or punishable, if done upon mutual consent between children of sufficient age. Directive 2011/93/EU also stipulates that the Member States may decide not to criminalise the attendance of a pornographic performance taking place in the framework of sexual relationships based on mutual consent, if the child has reached the age of sexual consent or if the performance takes place between peers who are similar to each other in terms of their age and psychological and physical development or maturity, if the said acts do not include abuse or exploitation and no money or any other form of compensation or payment is given for said pornographic performance. Several countries, including Estonia, have adopted this option. Such cases do not constitute materials of sexual abuse or an offence and therefore the identification and blocking of such material would unjustifiably violate the children's right to have their private and family life respected and their right to personal data protection and would not take into account the interests of the children. With regard to the procedures prescribed by the draft Regulation, a distinction should therefore be made between situations which involve intimate image and text materials shared in the mutual communication of two persons below the age of 18 years, and situations which involve re-sharing of such material and making it accessible to the public or to a communication group. This risk has been mitigated to a greater degree in the case of solicitation of children, as pursuant to Article 7 detection orders addressing the solicitation of children are applied only to interpersonal communication, if one the users is a child user (i.e. the other user is an adult). At the same time, the right to privacy may be prejudiced by the fact that according to the draft Regulation a "child user" is a natural person below the age of 17 years, but in Estonia the children's age of sexual consent, defined as having the ability to consent sexual intercourse or performing any other act of sexual nature, or the age at which soliciting a person younger than is punishable as an offence, is 16 as of 1 November this year. In Estonia it also does not constitute an offence, if the age difference between an adult person and a person aged fourteen to sixteen years is not greater than five years. Conversely, the draft Regulation also allows monitoring messaging in the case of which committing an offence is not possible due to the age of the persons. This right to extensively monitor and check private messaging significantly restricts child users' right to privacy, the protection of private life, message confidentiality, freedom of speech and expression, and sexual self-fulfilment.

The explanatory memorandum to the draft Regulation has highlighted this negative effect, but it merely states that the other positive effects of the Regulation outweigh it. No possibilities to mitigate this negative effect have been substantively assessed. We note that regulation of detecting, removing and blocking material constituting abuse provided for in the Regulation is primarily aimed at mitigating the consequences of abuse that has already taken place, while greater attention should be given, both at the level of the Member Stated and the EU, to the prevention of sexual

abuse and the provision of respective education in order to increase the children's awareness of dangers and teach how to avoid them.

**5.4 Estonia finds that the regulation of the draft act is not sufficiently clear and unambiguous with regard to the obligations placed on software application stores and therefore creates a risk that the act could disproportionately restrict the children's right to use Internet-based information society services. We primarily consider it necessary to describe in greater detail the criteria for defining applications of "significant risk".**

Article 6(1) obligates the providers of software application stores to prevent child users from accessing applications in the case of which they have identified a significant risk that the use of the service provided by those applications may be used for the purpose of solicitation of children and said apps must take the necessary age verification and age assessment measures to reliably identify child users on their services. The risk of child abuse is presumably present in the case of many widely common communication applications – as we know, the online grooming and exploitation of children does, indeed, take place via so-to-say ordinary and widely used applications – which must therefore be reflected in the risk assessment. It remains unclear whether the point of the Regulation is to prohibit the use of those applications for all child users or a certain target group, and if so, which one? The criterion "significant risk" which the providers of application stores must assess is not sufficiently clear – does it mean that a certain group of children (if so, how large a group) must have already become or may become a victim of abuse to quantify this definition of risk, or some other such metric? It must also be emphasised that if there is a significant risk that the service may be used for the solicitation of children referred to in that Article, this is not the same as the significant risk that the service is used for child abuse by disseminating child sexual abuse material as referred to in Article 7(4) and explained in greater detail in Article 7(5). The use of the term "significant risk" in different contexts and meanings makes the regulation difficult to understand. The grounds for restricting the children's use of services is not clearly defined, which creates the risk that the regulation may not be purposefully implemented and may instead start unjustifiably restricting the children's right to use various software applications and services. Furthermore, the Article makes no reference to the fact that in addition to the identification of risk, risk mitigation measures taken by the service provider could also be taken into account, as these may significantly mitigate even a high level of risk. If the ultimate goal of the Regulation is, indeed, to prohibit certain age groups from using certain software applications, in the case of which significant risks exist and the mitigation of such risks is complicated or impossible, it would be expedient to clearly make such a relevant proposal in the draft Regulation and provide relevant justification and a comprehensive analysis of the effect the proposed clause would have on children's fundamental rights.

**5.5 Estonia finds that the draft Regulation should more clearly stipulate the children's right to ask and receive information, assistance and support from relevant authorities, in a child-friendly manner accessible to them.**

Article 20(1) of the draft Regulation stipulates that persons residing in the European Union shall have the right to receive, upon their request, from the Coordinating Authority, designated by the Member State where they reside, information regarding any instances where the dissemination of known child sexual abuse material, depicting them, is reported to the EU Centre. On the basis of paragraphs 1 and 2 of Article 21, both the providers of hosting services and the EU Centre are to be founded via the Coordinating Authority which in turn will designated by the Member State and on request the Coordinating Authority shall provide, reasonable assistance and support to persons residing in the Union who seek to have one or more specific items of known child sexual abuse material, depicting them, removed or access thereto prohibited. The persons referred to in these Articles are mostly children whom the sexual abuse materials depict and it must be possible for them to protect their rights also without the assistance of an adult (above all, a parent or a legal

guardian). It unfortunately remains unclear from the provisions how the aforementioned possibilities and access to such services and support should become known to the children in question. We deem it necessary for the Regulation to emphasise, in addition to people with special needs, the children's right to ask and receive such information, assistance and support, in a child-friendly manner accessible to them.

**5.6 In Estonia's assessment, the requirements established for the Coordinating Authorities of the Member States are not relevant and go beyond what is necessary for achieving the objectives of the draft Regulation. Estonia does not support the established requirements concerning the creation of a separate new Coordinating Authority in each Member State and the complete administrative independence of that authority.**

With regard to the requirements concerning Coordinating Authorities, the Regulation is in contradiction with the principle of proportionality, on which the activities of the EU are based and pursuant to which, the measures taken by authorities may not go beyond what is necessary for achieving the objectives of the Treaties. The Member States must have the right to shape the system of administrative authorities necessary for the fulfilment of the objectives of the Regulation, according to the needs and specifics of each Member State. In the course of negotiating the Regulation, the provisions must be developed so as to allow the Estonian Police and Border Guard Board to cooperate with other authorities (including the Prosecutor's Office) and organisations (e.g. NGO Estonian Union for Child Welfare which currently acts as the Safe Internet Centre in Estonia, supported by the European Commission, and which one of the tasks of which it is obligated to offer, is an online hotline for preventing the dissemination of materials with illegal content on the Internet) in order to jointly act in accordance with the requirements established for a Coordinating Authority. Article 26(1) stipulates that the Member States have to ensure that "the Coordinating Authorities perform their tasks under this Regulation in an objective, impartial, transparent and timely manner". Pursuant to subparagraph (a) of paragraphs 2, the Coordinating Authorities must also be legally and functionally independent from any other public authority; must be free from any external influence, whether direct or indirect (subparagraph (c)); neither seek not take instructions from any other public authority or any private party (subparagraph (d)). Seeing as it is in the area of administration of the Ministry of the Interior and included in the national resource planning process, the Police and Border Guard Board as well as other public authorities cannot be considered "independent" in this context, as the level of priority of the activities and capacity development of the authorities and matters related to resources are settled by national strategies.

Considering Estonia's small size, the level of consolidation of the public sector and the proportionate state administration, subparagraph (2) of the same Article, pursuant to which the Coordinating Authority may not be charged "with tasks relating to the prevention or combating of child sexual abuse, other than their tasks under this Regulation", is the most problematic for the state. In Estonia's assessment, processing capacity is of central importance from the viewpoint of preventing and combating child sexual abuse.

It is also Estonia's objective to have it integrated into the existing state administration model in the best possible way, despite the already bureaucratic and comprehensive legal mechanism. For comparison, The Terrorist Content Online Regulation, which is in principle analogous with this proposal, establishes no administrative independence requirements for the national competent body, but refers to independence in the fulfilment of the obligations, established by the regulation (second sentence Article 13(2)). In Estonia, the Internal Security Service has been appointed as the respective body for the aforementioned obligations, and caries them out with the required independence, alongside its other duties.

**5.7 We find that in order to organise the work of the hotlines operating in the European Union, the draft Regulation should contain a clearer description of their role and inclusion.**

In Estonia, the police, the Prosecutor's Office, courts and NGO Estonian Union for Child Welfare (a member of the international association INHOPE) take part in detecting and processing cases related to child sexual abuse materials. NGO Estonian Union for Child Welfare has offered a free of charge online hotline service (www.vihjeliin.ee) since 2011. The hotline allows Internet users to forward information about materials with illegal content – child sexual abuse, child trafficking (human trafficking) – disseminated on the Internet. Information can be forwarded anonymously without forwarding personal data. The Estonian hotline joined INHOPE as a full member in 2012. In 2021, the hotline received 893 notifications, of which 484 contained information about online environments that presented child sexual abuse. These were mostly public online environments registered outside Estonia. The Estonian Union for Child Welfare has an operational cooperation agreement with the Police and Border Guard Board, on the basis of which the notifications to the hotline are processed and the relevant information is forwarded. If the country of location of material with illegal content is Estonia, a relevant notice is sent to the Police and Border Guard Board's contact person.

We find that the role of the hotlines should be more clearly described in the Regulation, as it has currently not been addressed at all. At the same time, the hotlines currently fulfil a very important role in the detection and removal of child sexual abuse materials from the Internet. The Regulation should allow such organisations with existing knowledge and proven capability to be competent bodies and systemic cooperation partners.

**5.8 In Estonia's assessment, the creation of a separate European Centre to prevent and counter child sexual abuse may be necessary to ensure efficiency and independence, but this should be done by optimising the existing resources. At the same time, we see a risk that it will duplicate the law enforcement activities of Europol in the area of cybercrime and organised crime. We consider it necessary for the European Union level implementation system to be as cost-efficient as possible and take into account the criminal investigation needs of the Member States.**

Currently there are many existing mechanisms for the potential organisation of resources this area of enforcement and these should be used to the maximum degree and reorganised as necessary before the creation of new mechanisms. Child sexual abuse is a wide-spread form of serious and organised crime, which is why operative forwarding and analysis of criminal information and the prosecution of the relevant persons is of critical importance, in addition to detecting and removing content.

Page 3 of the Draft Regulation explains that "In particular, the EU Centre will create, maintain and operate databases of indicators of online child sexual abuse that providers will be required to use to comply with the detection obligations." In addition, the Centre should help assist the Member States in fulfilling the tasks arising from the Regulation and support the fulfilment of the obligations of the providers. It is described on page 12 of the Regulation that placing the two agencies (Europol and the EU Centre to be created) in the same city will hopefully create "greater opportunities to create a knowledge hub on combatting CSAM". Followed by: "It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol (HR, IT including: cybersecurity, building, communication). Sharing such support services is more cost efficient and ensures a more professional service than duplicating them by creating them from scratch for a relatively small entity as the EU Centre will be." Both the argument of a "knowledge hub" and the argument of joint support services are enhanced in a situation where two agencies are integrated into one, by subordinating them to one structure and having them operate under a uniform

organisational logic, using the existing communication, data management, analysis and exchange capabilities created by Europol.

It also remains unclear how the communication and movement of operative information will take place between the (to be created) EU Centre, the national Coordinating Authorities, the supervisory institutions (e.g. the Data Protection Inspectorate, or DPI), the providers, the service users, the victims, the investigative bodies and law enforcement bodies, while taking into account the differences in the criminal proceedings of the Member States. Pursuant to Article 12(2) of the draft Regulation, the user must be notified of the restriction of the material immediately, if the EU considers the information irrelevant or after the expiry of three months, if the EU Centre has not prohibited notification within that period of time, whichever occurs first. In practice, this may create a situation where the EU Centre does not prohibit the notification of the user, but the relevant competent body of the Member State considers the prohibition of notification important, or vice versa – the EU Centre prohibits notification, but the user is already notified in the course of national proceedings. We find that the initiative must be clear and concrete and must not excessively intervene in the criminal proceedings of the Member States.

In the case of such a truly extensive law enforcement project, the central management of data, the immediate protection of the rights of victims and the removal of content and the assistance and organisation of the removal of content from the Internet is an important part of the Regulation. However, we cannot place less importance on addressing the original cause, i.e. bringing the criminal organisations and individual child sexual abusers to justice. Europol is already handling the closely related categories of crime of human trafficking and child sexual exploitation in the framework of combating and analysing organised crime. So far, Europol has created five area-specific units: the Operational and Analysis Centre, the Serious and Organised Crime Centre, the Cybercrime Centre, the Counter Terrorist Centre and the European Financial and Economic Crime Centre. As the activities established in the Regulation are classified as European law enforcement cooperation, the necessity of a separate European Union authority or centre should again be thoroughly discussed in negotiating the Regulation, taking into account the European Commission's impact assessment.

**5.9 The Member States must retain sufficient flexibility in determining the suitable authorities for issuing detection, removal and blocking orders to providers.**

In the context of detection orders, removal orders and blocking orders, we are concerned about the expected increase in the workload of the courts.

As a small country, Estonia does not support the creation of a separate authority in order to ensure the fulfilment of the requirements of Article 26(2). The Regulation could allow flexibility in the selection of the relevant competent body, and we prefer assigning tasks to the existing state institution(s) that have the capacity and the competence to fulfil the required tasks.

Section 2 of the draft Regulation empowers Coordinating Authorities, which have become aware – through a risk assessment or other means – of evidence that a specific hosting or interpersonal communications service is at a significant risk of being misused for the purpose of online child sexual abuse, to ask the competent judicial or independent administrative authority to issue an order obliging the provider concerned to monitor and detect the type of online child sexual abuse at issue on the relevant service (Articles 7 and 8).

Section 4 empowers Coordinating Authorities to request the competent judicial or independent administrative authority to issue an order obliging a hosting service provider to remove child sexual abuse material on its services or to disable access to it in all Member States, specifying the requirements that the order has to fulfil (Article 14).

Section 5 empowers Coordinating Authorities to request the competent judicial or independent administrative authority to issue an order obliging a provider of internet access services to disable access to uniform resource locators indicating specific items of child sexual abuse material that cannot reasonably be removed at source (Article 16 and 17).

In the context of detection orders as well as removal orders and blocking orders, we are concerned about the expected increase in the workload of the courts. On the one hand, it is definitely important to ensure the enforcement of the obligations assigned to the providers under the Regulation, but on the other hand we find that this may create a large additional workload and the work of the courts will need to be extensively reorganised to accommodate that. The obligations in question are not a mere formality, but require large-scale substantive work from the courts and the existence of a sufficient number of judges with specific subject knowledge.

Although the said tasks may be fulfilled by an independent administrative authority instead of a competent judicial body, this does not, in Estonia's opinion, solve the bottlenecks, as pursuant to the Regulation any such body must be an authority different from the national Coordinating Authority, while the substantive competence of the authorities should be quite similar in order to fulfil all the said tasks. We do not consider it reasonable to create two new administrative authorities with similar competence for the fulfilment of the tasks established in the Regulation in all countries, particularly in Estonia.

**5.10 Estonia considers it important that this area-specific Regulation is in conformity with other legal acts that regulate information society services, including the general rules of the Digital Services Act, and that the unnecessary duplication of the content of legal acts is avoided.**

With regard to the accountability and responsibilities of the providers of intermediary services, it is important to ensure conformity with the Digital Services Act (DSA) currently being processed, which establishes the general rules applicable to all the providers of intermediary services. It must be ensured in negotiating the draft Regulation that there are not contradictions between the general rules of the DSA and the specific rules established in this area-specific act. Under the DSA, the providers of hosting services have extensive due-diligence obligations in detecting illegal content and transparency obligations in notifying users. Different legal acts establish identical obligations and therefore it is important to ensure that there are no contradictions of unjustified differences between those obligations. In such cases, the providers should introduce different mechanisms for handling illegal content of different types, which will incur additional expenses on the development and continued operation of mechanisms.

Article 12(3) of the draft Regulation establishes the obligation to establish an accessible, age-appropriate and user-friendly mechanism, that allows users to flag potential cases of child sexual abuse. An obligation to establish a similar mechanism for flagging illegal content derives from paragraph 1 of Article 16 of the DSA and therefore it is unclear whether the providers are obligated to establish two separate mechanisms, one of which is for potential child sexual abuse content and the other for the remaining content.

Under Article 17 of the DSA, the providers of hosting services are obligated to notify the user of any restriction of the visibility of the content created by the user. Pursuant to Article 12(2) of this draft Regulation, the user has to be notified of the restriction of child sexual abuse material only if the EU Centre has not prohibited notification. The content of the information given to the user upon restriction under the two articles is also different. Thus, the providers are placed under a special treatment obligation in handling certain types of illegal content – to wait for the consent of the authorities before notifying the user – which creates additional workload and expenses for the providers.

Pursuant to Article 9(1) of the DSA, the law enforcement bodies of all the Member States have the right to demand that providers, established in another Member State, remove illegal content in their jurisdiction, the jurisdiction of other Member States and from the entire EU. Pursuant to Article 14(1) of this draft Regulation, only the competent judicial body of the country of location of the provider has the right to demand that the provider remove child sexual abuse content in the entire EU. It needs to be clarified why it has now been decided to make an exception from the DSA and the Terrorist Content Online Regulation (TCO), in which the right to issue cross-border removal orders is granted to the competent law enforcement bodies of all the Member States.

With regard to the obligations of the providers of interpersonal communication services and the providers of Internet access services, it is important to ensure conformity with the General Personal Data Protection Regulation[1] (GDPR) and the ePrivacy Directive (currently being reviewed and made into a EU regulation), from which an exception is made with regard to paragraphs 1 and 3 of Article 5 (confidentiality of the communications) and paragraph 1 of Article 6 (traffic data relating to subscribers). It must be ensured in negotiating the draft Regulation that there are not contradictions between the general rules of the ePrivacy Directive (the transposed Electronic Communications Act) and the specific rules established in this area-specific act. The Regulation on the prevention and combating child sexual abuse establishes extensive due-diligence obligations for the providers of interpersonal communication services and the providers of Internet access services in detecting illegal content, reporting obligations (Articles 12 and 13), storing this information, and transparency obligations in notifying the users.

**5.11 Estonia does not support the possibility of creating backdoors to end-to-end encryption solutions. At the same time, we may support the use of technologies which preserve privacy and allow analysing the encrypted content without decrypting.**

Article 7 of the Regulation establishes the obligation of fulfilling detection orders for the providers of hosting services (web hosting services, platforms) and the providers of interpersonal communication services. Pursuant to this provision, a competent body has the right to issue a detection order obligating a provider of hosting services or interpersonal communication services to detect known and new child sexual abuse material and the solicitation of children. The providers who have received a detection order must install and use a technology for detecting the dissemination of known or new child sexual abuse material or the solicitation of children on the basis of the relevant indicators presented by the EU Centre.

Regulation (EU) 2021/1232 of the European Parliament and of the Council currently applies, according to recital 25 of which "*end-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption.*" Article 88 of the draft Regulation repeals Regulation 2021/1232. This in turn allows – by issuing a detection order under Article 7 – giving the providers an obligation which surpasses the requirement of end-to-end encryption and allows the extensive monitoring of messages and other such communication. Pursuant to the recitals of the Regulation, the providers must find suitable technical solutions for fulfilling detection order even in the case of encrypted content. Thus, the Regulation obligates the providers to create backdoors into encrypted services to make monitoring the content transmitted via the service possible.

[1] Regulation (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) (OJL L 119, 4.5.2016)

This right of extensive monitoring and checking private messaging significantly restricts the users' right to privacy and the protection of private life, message confidentiality, freedom of speech and expression and sexual self-fulfilment. It also creates a dangerous trend in the European legal system, as it creates the possibility of requiring the creation of backdoors into encryptions. This in turn increases the probability of cyber incidents, as the existence of such access path would so-to-say invite cyber criminals to seek ways to access other information being exchanged. The creation of backdoors reduces the security and integrity of services, as it is technically impossible to make a backdoor, solely for the providers themselves or for security and law enforcement bodies, which only they would be able to access encrypted information. Joint opinion No. 04/2022 of the European Data Protection Board and the European Data Protection Supervisor opposes the creation of such backdoors and finds that the draft Regulation causes various risks to privacy and the security of electronic communication.[2]

Estonia is exploring the use of various privacy enhancing technologies which allow analysing encrypted content without decrypting. At the same time, we emphasise that these technologies must not reduce the reliability, security and integrity of the digital services based on encryptions. For instance, (fully) homomorphic encryption might be one such technology. However, the potential and instances of use of such technologies is still being mapped. The Estonian Ministry of Economic Affairs and Communications is planning to commission a relevant study in the near future.

We see the fulfilment of detection orders as particularly problematic in the context of preventive detection of grooming of children, where it may entail the obligation of constant automatic scanning of interpersonal messages (content). Taking into account that grooming mainly takes place via interpersonal communication services and such grooming may take place episodically, over a very long period of time (lasting for months, if not years) and consist of several individual partial acts, the fulfilment of such an obligation may in practice mean mass monitoring and recording of publicly used communication services in a very great extent, which is in conflict with the European Charter of Fundamental Rights and the former EC practice (exceeding the limits of allowed targeted monitoring) and limiting the further use of the information obtained in the course of monitoring criminal proceedings (matters of permissibility of evidence).

**5.12 Estonia considers it important that proportionality is preserved in regulating the detection obligation and that the Regulation does not go into conflict with the principle of prohibition of a general monitoring obligation.**

In the course of negotiating the Regulation, no obligation must be established for the providers of intermediary services to monitor all content forwarded or disseminated to the public regardless of if the aim to detect and remover child sexual abuse content. Such an obligation is in contradiction with the principle of prohibition of a general monitoring obligation established in the E-Commerce Directive and confirmed in the DSA, pursuant to which the providers of intermediary services do not have the obligation to generally actively look for illegal content and circumstances indicating illegal activities. The principle of prohibition of a general monitoring obligation prohibits the Members States from establishing a general obligation for providers to monitor information which it forwards or stores or to actively look for facts or circumstances indicating illegal activities. The European Court has repeatedly found that measures obligating providers to establish, at their own sole expense, filtering systems which mean general and constant monitoring in order to prevent any future violation are in conflict with the prohibition of a general monitoring obligation.[3]

[2] Joint opinion No. 04/2022 of the European Data Protection Board and the European Data Protection Supervisor, sections 96-102. Available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

[3] Scarlet Extended, C-70/10, sections 36–40; SABAM, C-360/10, sections 34–38.

Pursuant to subparagraph (c) of paragraph 3 of Article 1 of the draft Regulation, this Regulation does not have an effect on the application of the DSA and therefore the principles of the providers of information society intermediary services apply, including the principle of prohibition of a general monitoring obligation. Competent authorities may require the providers of intermediary services to remove or block access to specific illegal content, e.g. the removal of specific photo or video content, provided that the provider does not have to conduct an independent assessment of the content. In conclusion, the right of a competent body to issue a detection order obligating the provider of hosting services to detect child sexual abuse material, on the basis of the relevant indicators presented by the EU Centre, must be in conformity with the prohibition of a general monitoring obligation.

The orders can only demand the removal of content based on a specific indicator, the illegality of the content indicated must have been previously established by an authority or a court. Any obligation for the providers of intermediary services to introduce a filtering system, in order to detect possible child sexual abuse material for which there are no indicators, would violate the prohibition of a general monitoring obligation. In any case, it is not reasonable or practical to demand that providers themselves conduct an assessment of the illegality of content.

**5.13 Estonia considers the requirement established by the draft Regulation that balance between the fundamental rights must be ensured upon issuing a detection order important. This requirement requires clearer criteria as to what threshold services constitute higher risk services, where risks cannot be mitigated with less invasive measures.**

Considering that the capability of filtering algorithms, to distinguish child sexual abuse material or communication from other content, is limited, now and in the near future, the proposed solution inevitably means that in order to fulfil the detection obligation, providers would need to access to and in many cases process interpersonal communications and content that do not contain child sexual abuse material. In this light, it is required that pursuant to subparagraph (b) of paragraph 4 of Article 7 other effects on fundamental rights must also be assessed. However, in the course of the negotiations, it is important to assess what "appreciable extent" means[4] in relation to the dissemination of child sexual abuse material within the meaning of Article 7(6), and to ensure that the obligation specified in Article 7 could only be established for particularly problematic cases.

**5.14 Estonia supports the obligation to establish the necessary age verification and age assessment measures to reliably identify child users on services, which do not disproportionately restrict access to digital services. Above all, we support the introduction of age determination technologies where the age of the user is reliably determined by a third party, who only transmits information on whether the user is a child user or not, to a specific provider.**

The obligation to establish reliable measures for determining the age described in Article 4(3) of the draft Regulation presumably means that a person's own confirmation of being an adult is not sufficient. This may be justified, as many problematic incidents take place namely in anonymous environments, but as this is still an extensive interference with both the freedom to conduct a business (shaping a service model) and the right to privacy (particularly from the perspective of the protection of personal data), we emphasise that this solution should be further critically assessed in the course of the negotiations.

At the same time, it is worth keeping in mind that there is generally no separate right to anonymity. Neither is there a right (an absolute right) to use digital services anonymously, although this has long been a custom or an option. With regard to personal data protection and anonymity, the Court

[4] According to recital 21, appreciable extent means more than in isolated and relatively rare instances.

of Justice of the European Union has recently made a preliminary judgment in case number C-817/19, in which it confirmed that the PNR Directive is in principle in conformity with Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union, stating that a person does not have the right to fly anonymously. This is a matter the boundaries of which are still being clarified via case-law.

We can agree that the reliable determination of age prejudices the users' right to privacy, but such a restriction may be necessary in a democratic society. The legitimate aim of such a restriction would, in the context of this legal act, be the protection of the rights of a child – particularly the protection of a child from sexual abuse – which is also considered very important in Estonia (see KRPOL 2030, the Violence Prevention Agreement, the Internal Security Development Plan 2020-2030). We could support reliable measures for age determination, in the case of which a person may present himself or herself via a pseudonym in communicating with other users, because the objective of Article 4(3) is to keep certain children away from services (if a provider of interpersonal communication services has identified a risk of use of its services for the purpose of the solicitation), not to ensure that persons present themselves under their own name. Such a measure would allow a certain protection of privacy to users, while also ensuring that in the use of services in the case of which a risk of solicitation of children has been identified, such an offence cannot be committed anonymously, i.e. in a way in which law enforcement bodies would be unable to identify the suspect. We agree that it has to be considered here which technological possibilities exist and what kind of problems may arise in connection with these.

The principle of data protection by default derive from the GDPR, which does not require that personal data processing necessary for the protection of other persons also has to be prevented. Thus, we do not see that the draft Regulation necessarily contradicts the principle of data protection by default, but the said principle definitely has to be taken into account. The draft Regulation must not result in people having to reliably identify themselves (e.g. by way of authentication with an ID card) for the use of any digital services and to share extensive personal data to digital service providers in order for the provider to be able to verify that the person is not a minor.

We support the introduction of age determination technologies less prejudicing privacy, where the age of the user is reliably determined by a third party who only transmits information on whether the user is a child user or not to the particular provider.

**5.15 Estonia holds that the draft Regulation should not make the termination of violations or the removal of threats more difficult and must not make criminal proceedings more difficult.**

It should also be clarified how this initiative affects the Member States' existing possibilities and the right of their competent bodies to issue orders for the removal of illegal content as well as for preserving such content. While investigative bodies currently have a relatively broad authority (inter alia, as law enforcement bodies) to issue orders for the termination of violations of law and for the removal of threats, the Regulation initiative repeatedly stipulates the requirement for a permission from a court or another independent administrative authority.

**5.16 In order to achieve legal clarity and the uniform implementation of the Regulation, the responsibilities and accountability established for providers must be specified and clarified. It must be ensured in the course of the negotiations that the responsibilities established for providers are appropriate, necessary and proportionate. The proposed measures must not exclude other more efficient and novel measures for mitigating risks.**

It must be ensured that in the course of the negotiations, the criteria established for determining the scope of application of obligations, to the providers of intermediary services, are appropriate, justified and prevent unequal treatment among the providers. The requirements must only apply to those undertakings and services that are necessary for achieving a specific objective. For instance, the probability of an undesired effect manifesting may be small due to the nature of the service and therefore the establishment of a measure may be unjustified, or the size of a provider may be of such a small size that their platform does not necessarily allow for an undesired effect created in the provision of that service, which is why we support a risk-based approach.

Article 4(1) of the draft Regulation lists three options which the providers of intermediary services and the providers of interpersonal communication services must apply to mitigate the risk that their services may be used for transmitting or publishing child sexual abuse content, while also noting that the providers must apply some or all three options. It must also be possible for the providers to apply other relevant and efficient measures which are not included in the list but which allow mitigating the child sexual abuse risk. The introduction of automated mechanisms is a risk mitigation measure must remain voluntary for the providers. The same principle has been established in the Terrorist Content Online Regulation, pursuant to Article 5(8) of which the requirement to take risk mitigation measures does not include the providers' obligation to use automatic means.

Pursuant to the draft Regulation, a competent body may issue a detection order, established in Article 7, to a provider even if no child sexual abuse content has previously been detected on their services, but there is evidence that such content has occurred in other similar services. Issuing a detection order to a provider, before determining if the risk mitigation measures taken by the provider do not work and there is illegal content on the service in question, is not proportionate nor justified. In preparing the draft Regulation, the legislator has already assessed that accommodation services and private messaging services entail particular risks for the transmission or publication of child sexual content. Thus, these services are of high risk by their nature and a competent body may therefore in essence establish a detection order for all such providers, unless they have already introduced an automatic filtering system as a risk mitigation measure. Based on the above, the draft Regulation will lead the majority of providers to use automatic content detection systems for detecting illegal content, which is conflict with the principle of prohibition of a general monitoring observation.

With regard to the time-limited obligation arising from the draft Regulation, it is not clear how legal clarity and legal certainty is ensured for the providers – that authorities cannot endlessly issue them orders obligating them to take such measures. On the basis of Article 7 of the Regulation, a competent body has the right to demand, in a detection order, the introduction of automatic filtering systems for a maximum of 12 or 24 months, depending on the type of the content detected. Pursuant to Article 16 of the Regulation, a Competent Body may demand in a blocking order that the providers of Internet access services block all the known domain names on a list managed by the EU which contain child sexual abuse content for a maximum of 5 years. The draft Regulation does not specify what ensures the expiry of the need to take measures after the arrival of the term established in the order. Neither does the draft Regulation exclude the issuance of a new order before the arrival of the term of the first order. There is thus a risk that Competent Bodies may repeatedly issue orders demanding that measures be taken and that those temporary measures, taken on the basis of an order, become permanent obligations which are in conflict with the principles of

legal clarity, legal certainty and foreseeability. The draft Regulation must restrict the right to issue several consecutive detection orders to the same provider. If there is a wish to establish permanent due-diligence obligations for the providers in the draft Regulation, in order to avoid the transmission or publication of illegal content via these services, such obligations should be established in the legal act so that the lawfulness and proportionality of such obligations can be assessed.

**5.17 Estonia holds that the Regulation should prescribe sanctions only for the more serious violations by legal persons, ensuring that the Member States have the maximum flexibility with regard to sanction rate, type and proceedings.**

The wording of Article 35 of the draft Regulation will probably entail the need to amend the rates of sanctions for misdemeanours in the general part of the Penal Code. Estonia considers it important that the administrative-law nature of penalties is not emphasised in the case of the draft Regulation. The definition of an administrative penalty has never been given context in the European Union law – only criminal-law and non-criminal-law penalties are known in this context. In the case of the latter, where the legal act does not refer to the type of sanctions, the Member States can apply these in any proceedings at their discretion. We therefore oppose references to administrative penalties. There is no uniform understanding in the EU law of what the term means. The Member States must be ensured the maximum flexibility to use the sanction system and type which is the most suitable in their legal system. Consideration should also be given to establishing penalties only for certain more serious violations. Because there are monetary fines with a high upper limit, in the cases of which the impact the effect of such sanctions will have of the fundamental rights for a person is not clear, sanctioning should only be limited to legal persons. The Member States should be ensured flexibility to only sanction certain more serious violations (*ultima ratio* principle), i.e., not every violation must be mandatorily punishable. If necessary, sanctions should be established only for more serious violations, ensuring the maximum flexibility with regard to sanction rate, type and proceedings for the member states.

**5.18 We support maintaining limited accountability with regard to the providers of intermediary services included in the scope of application of the Regulation, and compliance with the principle of country of origin.**

The requirements established in the draft Regulation for the providers of intermediary services, must take into account the special role of the providers of intermediary services and their actual knowledge of the content mediated via them and their capability to change that information or intervene in the sharing of that information with the public or other users. The activities of a provider of intermediary services are generally limited to transmitting or storing of information provided by third parties, which is technical and automatic by nature. In such a case, the provider of intermediary services generally does not have any knowledge of the transmitted or stored information, or control over illegal information reaching the Internet. The principle of limited accountability should therefore apply to the providers of intermediary services, including digital platforms. We support the preservation of the principle of limited accountability, pursuant to which the providers of intermediary services should not be prosecuted under criminal law for making child sexual abuse content available if the undertaking promptly removes or blocks access to child sexual abuse information upon learning of it.

The providers of intermediary services should also not be held accountable for making child sexual abuse information available when they have been issued a detection order, but they have not been able to detect and remove or block access to all the child sexual abuse information with the help of additional technical measures. Article 19 of the draft Regulation excludes the accountability of the providers of intermediary services and the providers of interpersonal communication services only if they fulfil, in good faith, the obligations established in this Regulation. A violation of this Regulation should not entail the prosecution of the providers of intermediary services and the

providers of interpersonal communication services under criminal law for the dissemination of child pornography, as even with the best efforts and the highest-end technical solutions, it is not possible for the providers to ensure, without exception, that the users of their services do not misuse their services for child sexual abuse. Liability for child sexual abuse should fall upon the users who upload child pornography or solicit children, and upon the providers of intermediary services who knowingly allow such persons to disseminate such content in their environment.

The cross-border free movement of digital services is a principle driving factor in their development. It must be ensured that in the course of the negotiations that this Regulation is in conformity with the internal market principle or the principle of country of origin, deriving from the E-Commerce Directive and confirmed in the DSA, which ensures that supervision over information society services should take place at the place of origin. It is important to ensure that in the course of the negotiations the supervision mechanism of the draft Regulation is in conformity with the principle of country of origin, i.e. the supervision competence over the requirements arising from the Regulation should be vested in the country of location.

**5.19 We support the extension of the term established for the implementation of the Regulation from six months to at least 12 months.**

According to the draft act, the Regulation is immediately applicable in the EU Member States within six months after its entry into force. This may be insufficient for the establishment of such an extensive new system. If a new national system must be created upon the implementation of the draft Regulation and the development of capabilities in accordance with requirements must be ensured, an implantation period of 12 months or more must be provided.

# FINLAND

**Finland's comments on CSAM proposal after the LEWP meeting on 24 November.**

General comments:

- As we know, the proposed regulation contains provisions that extensively restrict various fundamental rights. Legislation of this kind is in itself an interference with fundamental rights, regardless of how it is to be applied. Therefore, the legislation itself must be sufficiently precise and the aspects relating to the various fundamental rights must be taken into account from the beginning of the text of the regulation and throughout. Doubts have been raised among experts in Finland as to whether this is currently being adequately achieved. We have already submitted written proposals for clarifications to Articles 1-10 of the Regulation, and we are working to submit more. With these proposals for clarification, Finland aims to address the concerns about the proportionality and necessity of the regulation.
- One way of ensuring proportionality would be, for example, to narrow the scope in a controlled and precise way that preserves the tools for identification, but would make the obligations more acceptable. We do not have a concrete proposal for this at the moment, nor have we sought to do so in our previous comments. Taking into account the concerns raised by Member States in LEWP, and also, for example, the EDPS & EDPB joint statement and its concerns, a considered narrowing of the scope may at some point come on the table. With this in mind, it would be interesting to hear more in detail the thoughts of Member States on, for example, voice messages, how is this perceived?

Articles 3 & 4:

- Finland supports the obligations under Articles 3 and 4 of the proposal. However, the obligations remain open, both in terms of their content and their binding nature. In addition, the relationship between Articles 3 and 4 and Article 7 should be clarified and it should be ensured, especially at legislative level, that measures under Article 7 are only taken when the measures under Articles 3 and 4 and their supplementation by the authority have been found to be insufficient.

Article 7

- Finland still has several reservations regarding Article 7 of the proposal, and as far as we know, the regulation does not seem to be without problems under the Finnish Constitution, especially with regard to restrictions on confidential communications. Concerns relate in particular to the impact of the regulation on the encryption of communications and the extent to which control would be exercised, taking into account in particular the principle of proportionality. The key concepts and practical focus of the regulation need to be clarified. Procedural safeguards and procedures are not yet a substitute for substantive issues if the latter remain unclear.
- In addition, particular attention should also be paid to the legal protection of users in case of possible abuse and to the supervision of service providers and the adequacy of such supervision. Service providers have a wide freedom of choice as to the technology to be used and the proposal's minimum criteria for the technology to be used are now too open-ended. This can be problematic, as it is the choice of technology that will determine how and to what extent fundamental rights are interfered with through regulation. The identification of grooming, for example, differs significantly from the identification of known visual material. The fundamental rights assessment and the technologies used may also differ greatly. In Helsinki, our experts have considered whether it would be appropriate to split and fragment Article 7 more in terms of the content that can be identified, as the article as a whole is now very challenging to assess.

Article 18 (5)

- Article 18(5) of the compromise text requires further clarification: ”*The provider and the users referred to in paragraph 1 shall be entitled to request the Coordinating Authority* ***in consultation if necessary with the competent authority that issued the blocking order*** *...”*
- The former is, in our view, problematic because the blocking order would be issued by the competent authority, which may therefore be different from the coordinating authority. In general, it is the authority that has issued the decision that also provides further information and advice on its decision and assesses compliance, and not another authority. This is a natural starting point, since the issuing authority is of course the best expert on its own administrative decision. At the moment, the second authority may comment on the decision of the other authority and "if necessary" consult the authority that actually issued the decision in the first place. We find this situation odd.

# GERMANY

- Second revision of Chapters I, II and III - 14143/22
- Next steps and conclusions from Workshop on Age Verification Techniques and Detection of Child Sexual Abuse Material in Encrypted Environments

General

- Germany thanks the Presidency for preparing the second compromise text on chapters 1-3 of the draft regulation (14143/22).
- Some of our proposed wording has unfortunately not yet found its way into the compromise text. This applies, among other things, to taking into account the decisions of national legislators concerning the age of sexual consent and the impunity of certain content and conduct. In our view, increasing the age of child users to below eighteen is problematic because this age of consent is not in line with our national legislation. For this reason, we would like to ask you to examine a national opening clause on the impunity of certain content and conduct under national law.
- As the Federal Government has not yet completed its examination, we would like to enter a general **scrutiny reservation**.

Second revision of Chapters I, II and III - 14143/22

Chapter I

- We maintain our previous comments, in particular from the LEWP meeting on 3 November 2022.

Chapter II

- Article 3: Please explain why the time limit in Article 3 (4) (a) has been extended to four months. Providers to whom a detection order is addressed should submit a new risk assessment which allows the competent authorities to re-evaluate the situation before the order expires. Germany is generally open to granting providers a reasonable period of time to repeat the risk assessment.
- Article 8: We agree with the clarifying amendments to Article 8 (2) on the language regime.
- Article 14: In our view, the amendments to Article 14 (5) and (6) are consistent.
- Article 14a: Germany welcomes the possibility to order the removal of CSAM across national borders. Cross-border removal orders can help to significantly reduce the availability of CSAM. It is important to be able to order removals quickly. The proposed provision involves the authorities in the member state in which the businesses have their registered office. The provisions in Article 4 of the TCO Regulation seem to be an appropriate example.
- Article 16: In paragraph 4, certain factual requirements for issuing a blocking order have been deleted, namely evidence that the service was used to disseminate CSAM in the last 12 months and a balancing of the rights and legitimate interests of all parties concerned. Please explain why these requirements have been deleted.
- Article 17: Issuing blocking orders to internet access providers should be allowed only if action against the responsible party cannot be taken or would likely fail; if blocking is technically feasible and reasonable; if this does not entail monitoring obligations; and if any HTTPS encryption is respected. The amendments to paragraph 5 seem to be practical and consistent. Any further necessary information is to be requested by the responsible authority which issued the order.

- The amendments to Article 18 (6) and Article 18b (5) seem to be both consistent and practical.
- Article 18a: Excluding web pages from search engine results affects both operators and users. Given the current practices of providers, we are pleased that the draft regulation creates a legal basis. However, requirements for delisting under Article 3 should be further specified.
- We also maintain our comments on the providers' obligations, in particular the comments we made at the LEWP meetings of 19 October 2022 and 22 September 2022.
- Article 21: Germany welcomes the fact that paragraph 3 strengthens the rights of the individuals affected. Many times, they cannot know all the services which store and disseminate material about them.

Chapter III

- The new title of Chapter 3 Section 1 helps achieve a common understanding.
- Article 26: In Germany's view, the coordinating authority should act independently. For this reason, we have expressed our support for bringing the CSA Regulation into line with the requirements of the TCO Regulation.
  In any case, we think that Article 25 (9) should clarify that other competent authorities taking over tasks from the coordinating authority must carry out these specific tasks independently and without seeking nor taking instructions. This is necessary in particular because law enforcement authorities should continue to be able to carry out evidence processing tasks and take over tasks related to removal orders.

  Therefore, Article 25 (9) should read as follows:

  *The requirements applicable to Coordinating Authorities set out in Articles 26, 27, 28, 29, and 30 and 31 shall also apply to any other competent authorities that the Member States designate pursuant to paragraph 1 in relation to the carrying out of their respective tasks.*

- We maintain our comments, in particular from the LEWP meeting on 17 October 2022.

Next steps and conclusions from Workshop on Age Verification Techniques and Detection of Child Sexual Abuse Material in Encrypted Environments

- Germany thanks the Presidency for conducting the second technology workshop.
- The workshop showed that there are already a wide range of possible age verification technologies. Technologies for age assessment based on faces or voices have already been certified at national level by the Voluntary Self-Regulation Body of Multi-Media Service Providers (FSM) and the Commission for the Protection of Minors in the Media (KJM). Using such technologies requires higher data protection standards because sensitive data, which may include biometric data, are involved. Germany welcomes the fact that the BIK+ strategy aims at uniform certification of age verification technologies. This is also relevant for the purposes of the CSA Regulation. However, regarding mandatory age verification – especially through document identifiers – it is important for Germany that this does not lead to an identification obligation. Anonymous or pseudonymous use of the services must still be possible.

- The workshop also showed that there are already different approaches to detecting CSAM in encrypted services, some of which providers are currently testing or even already using.
- In Germany's view, the Regulation must not lead to general interference with private, in particular encrypted, communication where there is no suspicion of wrongdoing, or to the weakening or circumvention of seamless and secure end-to-end encryption. 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 examining the use of suitable technical solutions.
- Due to time constraints, it was unfortunately not possible to address all the questions that Germany had submitted in advance. We therefore suggest a follow-up, possibly in writing.

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

(a) → it is likely that, despite any mitigation measures that the provider may have taken or will take, the service is used, to an appreciable extent, for the dissemination of new child sexual abuse material;¶

(b) → there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent, for the dissemination of new child sexual abuse material;¶

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

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

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

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

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

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

(c) → there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent, for the solicitation of children.¶

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

Page Break

TZ **Tóth Zoltán**
We suggest to keep the original text, the new proposal makes be the regulation circumventable.¶

8. → The EU Centre shall provide such assistance free of charge and in accordance with its tasks and obligations under this Regulation and insofar as its resources and priorities allow. ¶

9. → The requirements applicable to Coordinating Authorities set out in Articles 26, 27, 28, 29, ~~and~~ 30 **and 31** shall also apply to any other competent authorities that the Member States designate pursuant to paragraph 1. ¶

*Article 26*¶

*Requirements for Coordinating Authorities*¶

1. → Member States shall ensure that the Coordinating Authorities that they designated perform their tasks under this Regulation in an objective, impartial, transparent and timely manner, while fully respecting the fundamental rights of all parties affected. Member States shall ensure that their Coordinating Authorities have adequate technical, financial and human resources to carry out their tasks.¶

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

KS **Kisné Szabó Adrienn dr.**
The coordinating authority is likely to be a body funded from the state budget, so we would like to avoid any text that would give the opportunity to question its independence on this basis.¶

~~2. → When carrying out their tasks and exercising their powers in accordance with this Regulation, the Coordinating Authorities shall act with complete independence. To that aim, Member States shall ensure, in particular, that they:~~ ¶

~~(a) → are legally and functionally independent from any other public authority;~~¶

~~(b) → have a status enabling them to act objectively and impartially when carrying out their tasks under this Regulation;~~¶

~~(c) → are free from any external influence, whether direct or indirect;~~¶

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

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

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

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

Page Break

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

**Section 2**
**Powers of Coordinating Authorities**¶

*Article 27*¶

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

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

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

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

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

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

2. → Member States may grant additional ~~investigative~~inspective powers to the Coordinating Authorities.¶

Page Break

KS **Kisné Szabó Adrienn dr.**
These are not investigative powers in the classical sense, but rather administrative procedure. In our view, the current wording is not acceptable, even though the DSA regualtion contains this wording, as the DSA is not a law enforcement source of law.¶

3. → Member States shall ensure that, where their law enforcement authorities receive a report of the dissemination of new child sexual abuse material or of the solicitation of children forwarded to them by the EU Centre in accordance with Article 48(3), a diligent assessment is conducted in accordance with paragraph 1 and, if the material or conversation is identified as constituting child sexual abuse material or as the solicitation of children, the Coordinating Authority submits the material to the EU Centre, in accordance with that paragraph, within one month from the date of reception of the report or, where the assessment is particularly complex, two months from that date. ¶

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

*Article 37* ¶

*Cross-border cooperation among Coordinating Authorities* ¶

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

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

KS **Kisné Szabó Adrienn dr.** novembre 21, 2022
What is the legal basis and information that allows the Commission to come to such a conclusion, and where is the background to this in this draft? ¶
Reply Resolve

2. → The request or recommendation referred to in paragraph 1 shall at least indicate: ¶

(a) → the point of contact of the provider as set out in Article 23; ¶

(b) → a description of the relevant facts, the provisions of this Regulation concerned and the reasons why the Coordinating Authority that sent the request, or the Commission suspects, that the provider infringed this Regulation; ¶

(c) → any other information that the Coordinating Authority that sent the request, or the Commission, considers relevant, including, where appropriate, information gathered on its own initiative and suggestions for specific investigatory or enforcement measures to be taken. ¶

Page Break

3. → The Coordinating Authority of establishment shall assess the suspected infringement, taking into utmost account the request or recommendation referred to in paragraph 1.¶

Where it considers that it has insufficient information to asses the suspected infringement or to act upon the request or recommendation and has reasons to consider that the Coordinating Authority that sent the request, or the Commission, could provide additional information, it may request such information. The time period laid down in paragraph 4 shall be suspended until that additional information is provided.¶

4. → The Coordinating Authority of establishment shall, without undue delay and in any event not later than two months following receipt of the request or recommendation referred to in paragraph 1, communicate to the Coordinating Authority that sent the request, or the Commission, the outcome of its assessment of the suspected infringement, or that of any other competent authority pursuant to national law where relevant, and, where applicable, an explanation of the investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation.¶

*Article 38*¶

*Joint inspections~~investigations~~*¶

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

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

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

*Article 39*¶

*General cooperation and information-sharing system*¶

1. → Coordinating Authorities shall cooperate with each other, any other competent authorities of the Member State that designated the Coordinating Authority, the Commission, the EU Centre and other relevant Union agencies, including Europol, to facilitate the performance of their respective tasks under this Regulation and ensure its effective, efficient and consistent application and enforcement.¶

Page Break

# IRELAND

**Article 14/14a**

Ireland can support the addition of cross-border removal orders. The words "**under the jurisdiction of that Member State**" should therefore be deleted from 14(1).

It is not clear to us that 14(3a) is necessary, given the opportunities for redress in Article 15. But we can accept this provision if that is the consensus view.

We can accept Article 14(a), with the exception of 14a(4).

The Presidency has inserted the mechanism for cross-border removal orders set out in the TCO Regulation. However, the CSA Regulation is quite different from the TCOR, and CSAM is different to terrorist content.

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

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

There are several other reasons in support of our position:

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

We propose therefore amending Article 14a as below:

***Article 14a***

***Procedure for cross-border removal orders***

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

**order to the Coordinating Authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established.**

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

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

**Where it finds an infringement, it shall, within the same period, adopt a reasoned decision to that effect.**

~~**4. Hosting service providers and content providers shall have the right to submit, within 48 hours of receiving either a removal order or information pursuant to Article 15(3), a reasoned request to the Coordinating Authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established to scrutinise the removal order as referred to in the first subparagraph of paragraph 3 of this Article.**~~

~~**The competent authority shall, within 72 hours of receiving the request, adopt a reasoned decision following its scrutiny of the removal order, setting out its findings as to whether there is an infringement.**~~

**5. The Coordinating Authority shall, before adopting a decision pursuant to the second subparagraph of paragraph 3 ~~or a decision finding an infringement pursuant to the second subparagraph of paragraph 4~~, inform the competent authority that issued the removal order of its intention to adopt the decision and of its reasons for doing so.**

**6. Where the Coordinating Authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established adopts a reasoned decision in accordance with paragraph 3 ~~or 4~~ of this Article, it shall, without delay, communicate that decision to the competent authority that issued the removal order, the hosting service provider~~, the content provider who requested the scrutiny pursuant to paragraph 4 of this Article~~ and, in accordance with Article 14, Europol. Where the decision finds an infringement pursuant to paragraph 3 ~~or 4~~ of this Article, the removal order shall cease to have legal effects.**

**Upon receiving a decision finding an infringement communicated in accordance with paragraph 6, the hosting service provider concerned shall immediately reinstate the content or access thereto, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.**

**Article 26**

We oppose the addition in 26(1). We could accept the insertion of "independent" into the first sub-paragraph as an alternative, describing the manner in which the CA acts, rather than its status.

**Article 36**

We welcome the reinsertion of Coordinating Authority into the text.

# ITALY

Italy presents this comment on the following artcles:

- in the Article 14 is  indicated  the competent authority . does this term encompass the judicial authority, as written in the paragraph 3 letter a) and h or in the paragraph 4 of the same article?

- in the Article 14 par 4 appears the competent authority to be in charge of issuing the order (and not the coordinating authority which appears in art 14 paragr 1  3  and 5). Why?

- What is the role in the Art 16 par of the competent authority (par 1 3  nd 4 ) ?why in the paragr 3 is the coordinating authority the one in charge ?

- The same problem in art 17 par 1 and art 18 a) and in art 20.

# THE NETHERLANDS

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. The Netherlands would like to thank the Czech Presidency for all the work done on the proposal so far.

The Netherlands appreciates the opportunity to ask questions about Chapter I, II and III of the proposal and looks forward to continue the meetings in 2023.

**Chapter I**

**Article 2 (j)**

In Article 2(j), the Presidency has changed the age in the definition of 'child user' from 17 years to 18 years.

Earlier, the Commission explained the choice of 17 years. Our understanding is that this choice was made because of consistency with the 2011/93 directive, which defines all offences covered by the CSA Regulation. The definition of grooming refers to an adult and a child under the age of sexual consent. The 2011/93 directive leaves the determination of that age to the member states. So the age of sexual consent varies between EU member states.

The Commission chose the age of 17 because that would be the highest age of sexual consent in the EU. However, the age of sexual consent in the Netherlands is set at 16. The Dutch criminalisation of grooming is also linked with that age limit. For the Netherlands, the inclusion of ages 17 and 18 creates problems with our legislation.

A solution would be to include 'the age of sexual consent' in the definition The Netherlands proposes the following amendment:

> *'child user' means a natural person who uses a relevant information society service and who is a natural person below the age of ~~17 years~~* ***of sexual consent****.*

**Chapter II**

**Article 8**

**1(e)**

whether the detection order issued concerns the dissemination of known **child sexual abuse material,** ~~or~~ new child sexual abuse material **and/**or the solicitation of children

**1(f)**

the start date and the end date of the detection order; **as specified also in article 7(9)**;

**Article 10 (3)**

First of all, The Netherland would like to thank the Presidency for the summary of the workshop on technologies. We are studying this with great interest. At this moment we would like to uphold a general scrutiny reservation for chapter II.

The Netherlands retains questions about the detection order. The questions mainly focus on how such an order fits into a proportionate and efficient approach to preventing the storage and dissemination of online child sexual abuse material, and the security implications for communications and other data.

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

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

**Article 14 (1)**

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

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

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

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

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

**Article 14 (a)**

In article 14 (a) the Presidency introduces a possibility to issue cross-border removal orders. At this moment we would like to uphold a general scrutiny reservation for article 14(a).

Could the Presidency please clarify on why this article has been added to the proposal?
The Netherlands is also curious about the Commissions view on this article.

**Article 16**

**(4)(d)**

The Netherlands suggests to retain Article 16 (4)(d) because it requires considering the interests of all parties involved. The Netherlands deems this important.

**Chapter III**

**Article 25**

**(1)**

According to our information, the amendment to 6 months deviates from TCO regulation. We would like to do a proposal to include: 'from the date of application' instead of six months:

1. Member States shall, ~~by [*Date –* *two* **six** *months from the date of entry into force*~~ **from the date of application** *of this Regulation*~~]~~, designate one or more competent authorities as responsible for the application and enforcement of this Regulation ('competent authorities')

This does also mean a minor amendment to paragraphs **(4)** and **(6)**.

**Article 26**

The Netherlands is positive about adding this paragraph to article 26, but it is important for the Netherlands that it is about the Authority's performance of its tasks under this regultions.

We would like to suggest to add this to the text:

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

**Article 27**

**(1)(c)**
These are extensive special investigative powers which are subject to strong safeguards. As far as the Netherlands is concerned, this is a task for the enforcement authorities.

**Article 38**

**(2)**
The participating Coordinating Authorities shall make the results of the joint investigations available to other Coordinating Authorities, the Commission and the EU Centre, through the system established in accordance with Article 39(2), for the fulfillment of their respective tasks under this Regulation. Can the Commission please clarify on why 'the Commission' is included in this list?

**Article 39**

**(2)**

Why is the Commission included in this list? Could the sharing of information with the Commission be more efficient (e.g. the obligation to report to the Commission once a year on certain relevant aspects) instead of including it in all information management and information sharing?

## SPAIN

Art. 7 The detection orders concerning the solicitation of children shall apply only to interpersonal communications **between** ~~where one of the users is~~ a child user **and an adult**.

The previous wording is considered more appropriate, as it covers certain cases where the victim is a minor and the potential adult perpetrator may be using another minor (probably close to the age of majority) as an intermediary.