Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 15 November 2022

WK 10235/2022 ADD 8

LIMITE

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

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

WORKING DOCUMENT

From: To:	General Secretariat of the Council Law Enforcement Working Party (Police)
N° prev. doc.:	9068/22, 14008/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations on Articles 83 to 89 (Chapters V and VI) and Articles 1 and 2 (Chapter I)

Delegations will find attached the compilation of comments received from Members States on the abovementioned proposal following the meeting of the LEWP (Police) on 3 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

Written comments on doc. 14008/22 (Proposal for a Regulation laying down rules to prevent and combat child sexual abuse):

Doc. 14008/22 (revised version of Art. 1 and 2):

Austria has a scrutiny reservation. Austria suggests a comprehensive discussion and analysis of the question of proportionality before further changes/amendments in the text are discussed. In this context it is important to address the legal opinion of the Council Legal Service. Essentially a change in the text was made only concerning the age of the "child user" in Article 2 ("Definitions"). Such changes are incomprehensible as long as the overall concept is not clear. This also applies for changes concerning the authorities. Before tackling such detailed questions it has to be clear to what extent changes are necessary to guarantee the proportionality of proposed measures.

Written comments on Chapters V and VI of doc. 9068/22 (Proposal for a Regulation laying down rules to prevent and combat child sexual abuse):

From a data protection perspective Austria has a scrutiny reservation concerning Chapters V and VI.

The processing of personal data relating to criminal convictions and offences according to Article 10 of the General Data Protection Regulation, as stipulated in Article 84, shall be carried out only under the control of official authority and by providing appropriate safeguards for the rights and freedoms of data subjects.

Article 83:

Para. 2: Austria has a scrutiny reservation concerning the reporting obligations. Austria rejects especially lit. a, second bullet point because it goes too far. According to Article 84 para. 2 the Coordinating Authority has to draw up an annual report compiling the information referred to in Article 83 para. 2 and make it available by 31 March of the next year. It is not clear where the information is obtained from because the information in the police crime statistics and in the statistics on convictions of the judiciary cannot be assigned to a concrete report. A comment of the police to every single report, especially concerning the state of play of the investigation, whether any suspects were arrested, identification of victims, etc. is a disproportionate effort and is therefore rejected. The number of reports, also containing increasing amounts of data, is steadily rising. A high amount of personnel is needed to cope with the work. An additional workload for the police in form of a feedback obligation concerning reports und new obligations to report to the Coordinating Authority is counterproductive from an operational point of view. An automatically assignment of a report to a judicial decision is not possible. Therefore the relation would have to be established in every single case manually. The data collection should be based on already existing information in the police crime statistics and in the statistics on convictions of the judiciary. An enormous bureaucratic extra effort for the law enforcement authorities has absolutely to be avoided. This would be detrimental for the operative police work.

Article 89:

The six month period is with a view to the necessary national legal procedures far too short. The national legal process, especially the parliamentary procedure, requires a minimum period of 18 month.

BELGIUM

In relation to the proposal for a CSA Regulation we would like to share with you the following remarks:

- We have no further comments related to the two amended definitions at this moment. The change towards 18 years for 'child user' in relation to grooming is welcomed.
- We want to confirm that for reasons of consistency it would probably be useful in article 2(x) to refer to the DSA for the definition of 'online search engines' (article 3(j) of the published DSA 2022/2065). Is there a reason for not doing so yet?
- Our previous written comments of course remain valid, such as for example our hesitations concerning the inclusion of private audio communications and the risk this poses towards proportionality and, linked to this, the acceptability of the proposal by the co-legislators.

Written comments of Belgium related to Chapters V and VI of the proposal for a CSA Regulation

Reference: doc. 9068/22

While Belgium acknowledges and supports the importance of gathering data to determine the effectiveness of the Regulation as well as the importance of transparency, it seems that the Article 83 should be still studied further as regards its impact and the additional workload. To this end, Belgium already shares the following preliminary comments:

- Namely paragraph 2(a) would bring a substantial workload if those detailed consequences should be provided for every single report. We are not convinced that this is all necessary in light of evaluating and proving the effectiveness. We advise to look into other wording and/or less specific wording. Some of the data will only be able to be transmitted after the investigation has been concluded and involves the judiciary.
- A specific questions concerns the mentioning of a differentiation in the statistics related to gender in Article 83(2)(a). We wonder what the added value is of such a differentiation, based on gender or biological sex. In our cases this does not seem to matter in a way that justifies this data collection for the purpose of Article 83.
- A user-friendly way of reporting would be advisable, for example through a template
- What is the reason for including both for providers and the coordinating authorities the obligation to gather data on the time needed to execute removal orders?

We support including the words *"That report shall compile the information referred to in Article 83(3)."* as an additional sentence, after the current first sentence, in Article 84(4) to streamline the wording with Article 84(1) and (2).

Article 85(7) states that, where appropriate, the evaluation reports will be accompanied by legislative proposals. This seems logical, but we wonder about whether this should be included in the text. It seems evident, unnecessary and restrictive with regard to the timing. Is this a customary or standard addition? Could we leave it out?

Timing the end of the interim Regulation 2021/1232 at the moment of application of the CSA Regulation will create a gap for the use of detection technologies that is unwanted and disproportionate. A lot of the providers that are currently voluntarily using detection technologies would indeed probably be subject to detection orders, but those will only be issued after a lengthy process. Not only the procedure for issuing a detection order will be lengthy but it will also be dependent on the procedure for risk analysis and risk mitigation that comes before. We strongly recommend transitional provisions that limit the loss of reporting during the transitional period. A phased procedure could be considered to this end.

Lastly, we support extending the six months period in Article 89 to at least twelve months and will study further the impact thereof.

FINLAND

Written comments on Chapter I & II. (doc. 12354/22)

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

(Text with EEA relevance)

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Regulation lays down uniform rules to **prevent and** address in a targeted, carefully balanced and proportionate manner the ~~mis~~use of relevant information society services for online child sexual abuse in the internal market.

   It establishes, in particular:

   (a) obligations on providers of relevant information society services to minimise the risk that their services are ~~mis~~used for online child sexual abuse;

   (b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

   (c) obligations on providers of hosting services to remove or disable access to child sexual abuse material on their services;

   (d) obligations on providers of internet access services to disable access to child sexual abuse material;

   (da) obligations on providers of online search engines to delist websites indicating specific items of child sexual abuse;

   (e) rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member States, the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre') and cooperation and transparency.

2. This Regulation shall apply to providers of relevant information society services offering such services in the Union, irrespective of their place of main establishment.

Commented [KT1]: General remark 1

To address the concerns regarding the protection of personal data, the confidentiality of communications, **legal protection** and the freedom of speech, we would propose highlighting from the very start and throughout the text that the co-legislators have defined the scope of limitations. (See C-401/19 paras 63-68. In the case, the Court did not annul the new Copyright Directive, as the reasons to limiting fundamental rights were clearly addressed in the Directive (see paras 77-97).)

Pursuant to the established case law of the European Court of Human Rights (ECtHR) the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (Liberty and Others v. the United Kingdom, 1 July 2008, § 56 and Weber and Saravia v. Germany, 29 June 2006, § 78)

To this end, we propose several additions to the text.

Commented [KT2]: We see that some reassurance to worries regarding the limitations to fundamental rights can be attained by including text form the Interim CSAM Regulation and the DSA stating that no *general* derogations will follow, but the measures are targeted, balanced and proportionate.

Commented [KT3]: From recital 2.

3. This Regulation shall not affect the rules laid down by the following legal acts:

(a) Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA;

(b) Directive 2000/31/EC and Regulation (EU) …/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC];

(ba) Regulation (EU) 2022/... of ... on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act);

(c) Directive 2010/13/EU;

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725, and, subject to paragraph 4 of this Article, Directive 2002/58/EC;

(e) Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

4. This Regulation lays down strictly limited rules derogating from ~~limits~~ the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC to the extent strictly necessary ~~insofar as necessary~~ for the execution of the detection orders issued in accordance with Section 2 of Chapter ~~I~~ II of this Regulation. Therefore, no general obligation to monitor the information which the relevant information society services transmit or store shall be imposed.

5. This Regulation should be applied so that it does not cause any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law.

Commented [KT4]: From the Interim Regulation art. 1(1).

Commented [KT5]: From the Interim Regulation art. 1(1).

Commented [KT6]: Shortened from DSA 8 article.

Commented [TM(7]: From recital 2.

Article 2

Definitions

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

(a) 'hosting service' means an information society service as defined in Article 2, point (f), third indent, of Regulation (EU) …/… *[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*;

(b) 'interpersonal communications service' means a publicly available service as defined in Article 2, point 5, of Directive (EU) 2018/1972, including services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service;

(c) 'software application' means a digital product or service as defined in Article 2, point 13, of Regulation (EU) …/… [*on contestable and fair markets in the digital sector (Digital Markets Act)*];

CHAPTER II

OBLIGATIONS OF PROVIDERS OF RELEVANT INFORMATION SOCIETY SERVICES TO PREVENT AND COMBAT ONLINE CHILD SEXUAL ABUSE

Section 1
Risk assessment and mitigation obligations

Article 3

Risk assessment

1. Providers of hosting services and providers of interpersonal communications services shall diligently identify, analyse and assess, for each such service that they offer, the risk of use of the service for the purpose of online child sexual abuse.

2. When carrying out a risk assessment, the provider shall take into account, in particular:

   (a) any previously identified instances of use of its services for the purpose of online child sexual abuse;

   (b) the existence and implementation by the provider of a policy and the availability of functionalities to address the risk referred to in paragraph 1, including through the following:

   – prohibitions and restrictions laid down in the terms and conditions;

   – measures taken to enforce such prohibitions and restrictions;

   – functionalities enabling age verification;

   – functionalities enabling users to flag online child sexual abuse to the provider through tools that are easily accessible and age-appropriate;

   (c) the manner in which users use the service and the impact thereof on that risk;

   (d) the manner in which the provider designed and operates the service, including the business model, governance and relevant systems and processes, and the impact thereof on that risk;

Commented [TM(8]: We endorse measures which aim to prevent the risks of online child sexual abuse, such as Articles 3 and 4. However, the scope and the binding nature of these preventive obligations should be clarified. The obligations to assess and mitigate risks are defined broadly and it remains unclear how comprehensive analysis are required from the provider and which kind of measures are considered to be adequate before adhering to stricter restrictions, such as a detection order. For instance, it is not entirely clear whether the providers have rather wide discretion, or in some cases also incentives, to conclude that the risk exists and cannot be mitigated and thereby argue that the detection order is necessary (see also recital 17).

Pursuant to Article 5, the providers should report to the Coordinating Authority and EU centre their process and results as for risk assessment as well as any mitigation measures taken. Article 5 paragraph 4 also includes the power of the Coordinating Authority to require the provider to re-conduct or update the risk assessment or to introduce, review, discontinue or expand, as applicable, the mitigation measures.

We have following questions and remarks relating to Articles 3, 4 and 5.

1) If the detection order should be used as a last resort, the coordinating authority firstly and primarily require the providers firstly to supplement and enhance measures taken e.g. under Articles 3 and 4 of this Regulation before adhering to Article 7 and this should be indicated more clearly in Article 7 (see below modification suggestion to Article 7(2)).

This could prevent the possibility that the providers undermine their obligations under Articles 3 and 4 due to their willingness of being issued a detection order. Naturally, the fundamental rights of the providers should also be respected, notably their freedom to conduct a business (Article 16 of the EU Charter).

2) Should this obligation to re-conduct, update, introduce review, discontinue or expand the measures under Articles 3 and 4 (Article 5 paragraph 4) primarily precede the imposition of penalties under Article 35 of this Regulation considering that it might be difficult also for the providers to understand the content and parameters of their obligations under Articles 3 and 4, as defined broadly?

Commented [TM(9]: From recital 18. There should be some criteria also for the quality and breadth of the risk assessment. This is essential especially consider that risk assessment (and mitigation measures) form the basis of the analysis of a detection order.

See EDPB-EDPS Joint Opinion 04/2022, paragraph 28, page 14.

(b) the Coordinating Authority of establishment may require the provider to update the risk assessment at a reasonable earlier date than the date referred to in the second subparagraph, where there is evidence indicating a possible substantial change in the risk that the service is used for the purpose of online child sexual abuse.

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

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

Commented [TM(10]: The power to issue guidelines is broad and it should specified what is the legal effect of these guidelines and to what extent the obligations defined in law maybe be specified in these guidelines. Similar comment about Article 4(5).

Article 4

Risk mitigation

1. If pProviders of hosting services and providers of interpersonal communications services have identified risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they shall take reasonable mitigation measures, tailored to the risk identified pursuant to Article 3, to minimise that risk. Such measures shall include some or all of the following:

Commented [TM(11]: At the moment, Article 4 does not clearly inform when the provider should take the mitigations measures. This is clearly noted only in recital 18 ("When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures"). This should also be indicated in the provision of the Regulation.

(a) adapting, through appropriate technical and operational measures and staffing, the provider's content moderation or recommender systems, its decision-making processes, the operation or functionalities of the service, or the content or enforcement of its terms and conditions;

(b) reinforcing the provider's internal processes or the internal supervision of the functioning of the service;

(c) initiating or adjusting cooperation, in accordance with competition law, with other providers of hosting services or providers of interpersonal communication services, public authorities, civil society organisations or, where applicable, entities awarded the status of trusted flaggers in accordance with Article 19 of Regulation (EU) …/… [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*] .

2. The mitigation measures shall be:

Commented [TM(12]: This paragraph in fact imposes obligation on the providers to perform a kind of proportionality analysis. Pursuant to subparagraph (c) it includes "the potential consequences of the mitigation measures for the exercise of fundamental rights of all parties affected". These kinds of general remarks may include challenges for this kind of analysis as the provider itself is a party whose rights are affected. Thus, the provider is analysing the fundamental rights of others against its own fundamental rights, namely right to conduct a business. Thus, it might be necessary to subject this analysis to the control of public authorities (see modification suggestion Article 5 (1) point (b)).

(a) effective in mitigating the identified risk;

(b) targeted and proportionate in relation to that risk, taking into account, in particular, the seriousness of the risk as well as the provider's financial and technological capabilities and the number of users;

(c) applied in a diligent and non-discriminatory manner, having due regard, in all circumstances, to the potential consequences of the mitigation measures for the exercise of fundamental rights of all parties affected;

(d) introduced, reviewed, discontinued or expanded, as appropriate, each time the risk assessment is conducted or updated pursuant to Article 3(4), within three months from the date referred to therein.

3. Providers of interpersonal communications services that have identified, pursuant to the risk assessment conducted or updated in accordance with Article 3, a risk of use of their services for the purpose of the solicitation of children, shall take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the mitigation measures.

4. Providers of hosting services and providers of interpersonal communications services shall clearly describe in their terms and conditions the mitigation measures that they have taken. That description shall not include information that may reduce the effectiveness of the mitigation measures.

5. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1, 2, 3 and 4, having due regard in particular to relevant technological developments and in the manners in which the services covered by those provisions are offered and used.

Article 5

Risk reporting

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

(a) the process and the results of the risk assessment conducted or updated pursuant to Article 3, including the assessment of any potential remaining risk referred to in Article 3(5);

(b) any mitigation measures taken pursuant to Article 4 and how these measures comply with the requirements of Article 4 (2).

2. Within three months after receiving the report, the Coordinating Authority of establishment shall assess it and determine, on that basis and taking into account any other relevant information available to it, whether the risk assessment has been carried out or updated and the mitigation measures have been taken in accordance with the requirements of Articles 3 and 4.

3. Where necessary for that assessment, that Coordinating Authority may require further information from the provider, within a reasonable time period set by that Coordinating Authority. That time period shall not be longer than two weeks.

The time period referred to in the first subparagraph shall be suspended until that additional information is provided.

4. Without prejudice to Articles 7 and 27 to 29, where the requirements of Articles 3 and 4 have not been met, that Coordinating Authority shall require the provider to re-conduct or update the risk assessment or to introduce, review, discontinue or expand, as applicable, the mitigation measures, within a reasonable time period set by that Coordinating Authority. That time period shall not be longer than one month.

Commented [TM(13]: This obligation to re-conduct, update, introduce, review, discontinue or expand should be primary before resorting to Article 7. The expression "without prejudice to Article 7" seems to suggest otherwise. What is the meaning of this reference to Article 7?

5. Providers shall, when transmitting the report to the Coordinating Authority of establishment in accordance with paragraph 1, transmit the report also to the EU Centre.

6. Providers shall, upon request, transmit the report to the providers of software application stores, insofar as necessary for the assessment referred to in Article 6(2). Where necessary, they may remove confidential information from the reports.

Article 6

Obligations for software application stores

1. Providers of software application stores shall:

(a) make reasonable efforts to assess, where possible together with the providers of software applications, whether each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children;

(b) take reasonable measures to prevent child users from accessing the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children;

(c) take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b).

2. In assessing the risk referred to in paragraph 1, the provider shall take into account all the available information, including the results of the risk assessment conducted or updated pursuant to Article 3.

3. Providers of software application stores shall make publicly available information describing the process and criteria used to assess the risk and describing the measures referred to in paragraph 1. That description shall not include information that may reduce the effectiveness of the assessment of those measures.

4. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1, 2 and 3, having due regard in particular to relevant technological developments and to the manners in which the services covered by those provisions are offered and used.

Section 2
Detection obligations

Article 7

Issuance of detection orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative ~~authority~~body whose decision is binding of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect online child sexual abuse on a specific service.

2. The Coordinating Authority of establishment shall, before requesting the issuance of a detection order, carry out the investigations and assessments necessary to determine whether the conditions of paragraph 4 have been met. The issuance of a detection order is only possible if the measures taken pursuant to Articles 3 and 4 are considered inadequate, including also the requirement of Article 5 (4) to re-conduct, update, introduce, review, discontinue and expand them.

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

3. Where the Coordinating Authority of establishment takes the preliminary view that the conditions of paragraph 4 have been met, it shall:

(a) establish a draft request for the issuance of a detection order, specifying the main elements of the content of the detection order it intends to request and the reasons for requesting it including the necessity of the issuance of a detection order;

(b) submit the draft request to the provider and the EU Centre;

(c) afford the provider an opportunity to comment on the draft request, within a reasonable time period of no less than four weeks set by that Coordinating Authority;

Commented [TM(14]: We have still concerns and questions, notably relation to technology solutions and legal issues (concerning fundamental rights), that needs to be further addressed.

Firstly, it is of great importance for us that the solutions of this obligation meet the requirements of proportionality principle and are acceptable taking into consideration also the essence of different fundamental rights, in particular the secrecy of confidential communication and data protection.

Recently, the Finnish Constitutional Law Committee of the Parliament, which is the most authoritative constitutional organ in legislative affairs, concluded in its statement concerning this Regulation that, based on the information currently available, the regulation does not seem unproblematic from the perspective of the Finnish Constitution (section 10 (4) of the Constitution).

In addition, the relationship of the Regulation, notably its Article 7, with fundamental rights, including also the ECHR and EU Charter, should be further specified that this Regulation is in line with them.

The compliance of this article with the principle of proportionality requires that at least the following three aspects are diligently answered and analysed:

1) The necessity criterion as a part of proportionality analysis means that a restriction on the secrecy of a confidential message or data protection is only permitted if the objective cannot be achieved with less interference with these rights and that a restriction to secrecy to confidential communication is as targeted and restricted as possible.

2) The proportionality principle also requires that a restriction cannot go beyond what is justified, considering the weighty nature of the interest underlying the restriction in relation to the legal interest to be restricted. Herein, one should not ... [1]

Commented [KT15]: We see it necessary that the power to issue a detection order remains within judicial control.

Commented [KT16]: We would like to note that the ECJ has set conditions that an authority must fulfil when it is not a court. It would be beneficial to address that in recitals. See C-746/18 paras 51-54.

(x) It is essential that the issuance of detection orders be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request. Th ... [2]

Commented [KT17]: From the ECJ's jurisprudence in data retention cases, see for example C-793/19 para 72.

Commented [TM(18]: The obligation to submit information is very broad and it is linked to the possibility of issuance of a detection order. The threshold for submitting information seems to be rather open "where appropriate" regardless of the fact that this information may include very sensitive information. Moreover, it is not entirely clear what is meant by "relevant experts" or "entities".

Commented [KT19]: To ensure the necessity of the measure and its assessment

Commented [KT20]: As four weeks is given to the EU Centre as well.

Page 11: [1] Commented [TM(14] **31/10/2022 12:17:00**

We have still concerns and questions, notably relation to technology solutions and legal issues (concerning fundamental rights), that needs to be further addressed.

Firstly, it is of great importance for us that the solutions of this obligation meet the requirements of proportionality principle and are acceptable taking into consideration also the essence of different fundamental rights, in particular the secrecy of confidential communication and data protection.

Recently, the Finnish Constitutional Law Committee of the Parliament, which is the most authoritative constitutional organ in legislative affairs, concluded in its statement concerning this Regulation that, based on the information currently available, the regulation does not seem unproblematic from the perspective of the Finnish Constitution (section 10 (4) of the Constitution).

In addition, the relationship of the Regulation, notably its Article 7, with fundamental rights, including also the ECHR and EU Charter, should be further specified that this Regulation is in line with them.

The compliance of this article with the principle of proportionality requires that at least the following three aspects are diligently answered and analysed:

1) The necessity criterion as a part of proportionality analysis means that a restriction on the secrecy of a confidential message or data protection is only permitted if the objective cannot be achieved with less interference with these rights and that a restriction to secrecy to confidential communication is as targeted and restricted as possible.

2) The proportionality principle also requires that a restriction cannot go beyond what is justified, considering the weighty nature of the interest underlying the restriction in relation to the legal interest to be restricted. Herein, one should not only consider the impact on this article to privacy rights or freedom of speech at individual cases but also how this article might negatively impact on the collective nature and values of those rights which are highly important also to many basic functions in a democratic society, in particular consider the role of confidential communications.

3) The measures taken should be such that the aim pursued can de facto be achieved through them. This also includes that the measures taken cannot be easily circumvented.

As for data protection the ECJ concluded that derogations or limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (C-293/12 and C-594/12, paragraph 52). Moreover, in Schrems, the ECJ concluded that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (C-362/14, paragraph).

The essential question to be specified is how it is ensured that a detection order is targeted and restricted not only in the provision but also in practice and does not result in a generalised basis of supervision of the confidential content of electronic communications.

As noted in EDPB/S opinion, paragraph 30, page 15, procedural safeguards can never fully replace substantive safeguards, which also needs to be addressed, including the clarification of key concepts, such as "significant risk".

One of the challenge of Article 7 is that the proportionality analysis and requirements might vary significantly depending on the content that is being detected, whether it is (un)known CSAM-material or solicitation of children.

Thus, it might be useful to consider whether it would be beneficial to divide Article 7 into two or more articles considering that Article 7 invokes very different considerations (including proportionality analysis) as well as technological solutions depending on the actual content being detected (e.g known CSAM-material or solicitation of children). This could help to analyse more precisely which parts of Article 7 might be more easily acceptable taking into consideration also the technology already available and which parts of Article 7 include more reservations with regard to fundamental rights, such as privacy rights and freedom of speech.

Page 11: [2] Commented [KT16] 19/10/2022 15:57:00

We would like to note that the ECJ has set conditions that an authority must fulfil when it is not a court. It would be beneficial to address that in recitals. See C-746/18 paras 51-54.

(x) It is essential that the issuance of detection orders be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request. The court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. It follows from the foregoing considerations that the authority must be a third party in relation to the authority which requests the issuance of the detection order.

(d) invite the EU Centre to provide its opinion on the draft request, within a time period of four weeks from the date of receiving the draft request.

Where, having regard to the comments of the provider and the opinion of the EU Centre, that Coordinating Authority continues to be of the view that the conditions of paragraph 4 have met, it shall re-submit the draft request, adjusted where appropriate, to the provider. In that case, the provider shall do all of the following, within a reasonable time period set by that Coordinating Authority:

(a) draft an implementation plan setting out the measures it envisages taking to execute the intended detection order, including detailed information regarding the envisaged technologies and safeguards;

(b) where the draft implementation plan concerns an intended detection order concerning the solicitation of children other than the renewal of a previously issued detection order without any substantive changes, conduct a data protection impact assessment and a prior consultation procedure as referred to in Articles 35 and 36 of Regulation (EU) 2016/679, respectively, in relation to the measures set out in the implementation plan;

(c) where point (b) applies, or where the conditions of Articles 35 and 36 of Regulation (EU) 2016/679 are met, adjust the draft implementation plan, where necessary in view of the outcome of the data protection impact assessment and in order to take into account the opinion of the data protection authority provided in response to the prior consultation;

(c bis) where the draft implementation plan is likely to be detrimental to the protection of privacy in the electronic communications sector, consult the national regulatory authority responsible for the supervision of Directive 2002/58/EC;

(c ter) where the draft implementation plan is likely to be detrimental to the security of networks and services, consult the national regulatory authority responsible for the supervision of Directive (EU) 2018/1972.

(d) submit to that Coordinating Authority the implementation plan, where applicable attaching the opinion of the competent data protection authority and specifying how the implementation plan has been adjusted in view of the outcome of the data protection impact assessment and of that opinion.

Where, having regard to the implementation plan of the provider and the received opinions ~~of the data protection authority~~, that Coordinating Authority continues to be of the view that the conditions of paragraph 4 have met, it shall submit the request for the issuance of the detection, adjusted where appropriate, to the competent judicial authority or independent administrative ~~authority~~body whose decision is binding. It shall attach the implementation plan of the provider and the opinions of the EU Centre and the data protection authority to that request and, when appropriate, the reasons for diverging from the opinions received.

Commented [KT21]: In some countries, as in Finland, the data protection authority is not responsible for all privacy questions of electronic communications.

Commented [KT22]: Typically, the data protection authority is not responsible for the supervision of security questions under the electronic communications code.

Commented [KT23]:
The obligations imposed on service providers cannot become excessive taking into consideration the principle of proportionality. Therefore, these prior obligations and their scope before issuance of a detection order should be reviewed having due regard also to the right to property and right to conduct a business.

Herein one could refer to recitals 2 and 22 in which it is noted that the Regulation should not impose any excessive burdens on the providers of services and that the assessment should also take account of the financial and technological capabilities and size of the provider concerned.

Commented [KT24]: The Court/body must know this in order to properly assess the matter.

The Court/body should also be informed why measures taken pursuant Articles 3 and 4 are not enough.

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

(a) there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5, 6 and 7, as applicable;

(b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties;.

(c) issuing the detection order is constitutes a necessary, appropriate and proportionate measure within a democratic society to detect online child sexual abuse material [and solicitation of children], ~~since~~and ~~less restrictive~~no measures pursuant to Article 4 ~~have not or~~ would ~~not~~ be effective.

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

(a) the risk assessment conducted or updated and any mitigation measures taken by the provider pursuant to Articles 3 and 4, including any mitigation measures introduced, reviewed, discontinued or expanded pursuant to Article 5(4) where applicable;

(b) any additional information obtained pursuant to paragraph 2 or any other relevant information available to it, in particular regarding the use, design and operation of the service, regarding the provider's financial and technological capabilities and size and regarding the potential consequences of the measures to be taken to execute the detection order for all other parties affected;

(c) the views and the implementation plan of the provider submitted in accordance with paragraph 3;

(d) the opinions of the EU Centre and of the data protection authority submitted in accordance with paragraph 3.

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

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

(a) ~~it is likely,~~ despite any mitigation measures that the provider ~~may have~~has taken or will take, ~~that~~ there is a genuine and present or foreseeable, risk that the service is used, to an appreciable extent for the dissemination of known child sexual abuse material;

Commented [TM(25]: The competent judicial authority must have discretion to decide whether or not to issue a detection order based on an independent analysis of the requirements specified in Article 7 (4). In order to guarantee high level of legal protection, the judicial control must not be illusory but genuine which means that that judicial authority has all the necessary information and reasoning to reach its decision.

Commented [KT26]: These are the general requirements of measures restricting fundamental rights.

Commented [KT27]: Clarification that other measures should be used first.

Commented [KT28]: What role does the Commission play here?

Commented [KT29]: To highlight the necessity of the measure.

Commented [KT30]: From ECJ's data retention rulings.

Commented [KT31]: As EDPB/S have noted, this is too broad and vague term, and not precise enough to justify an interference with the fundamental rights.

In recital 21, it is also noted that "appreciable extext" means something else than "isolated and relatively rare instances" which seems to indicate that the threshold is de facto lower than "appreciable".

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

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~~has taken or will take, there is a genuine and present or foreseeable, risk that 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 on interpersonal communication services, 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~~has taken or will take, there is a genuine and present or foreseeable, risk that service is used, to an appreciable extent, for the solicitation of children;

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

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

Commented [TM(32]: This criterion is challenging because it expresses that risk assessment is not linked to a concrete risk in a certain service but rather to a more general risk assessment that certain kinds of services already includes the idea of significant risk.

Commented [KT33]: A factor in the assessment of the risk cannot be that one is in the scope of the measure.

Commented [PP34]: Detection of solicitation is clearly different measure than detection of CSA material. Therefore, detection of solicitation should be moved to a separate article focusing solely on the conditions and safeguards for this particular measure.

Detecting solicitation also limits the rights of the children, and therefore, the justification for these measures must be assessed separately from the detection of CSA material.

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

To that aim, they shall take into account all relevant parameters, including the availability of sufficiently reliable detection technologies in that they limit to the maximum extent possible the rate of errors regarding the detection and their suitability and effectiveness for achieving the objectives of this Regulation, as well as the impact of the measures on the rights of the users affected, and require the taking of the least intrusive measures, in accordance with Article 10, from among several equally effective measures.

In particular, they shall ensure that:

(a) ~~where that risk is limited to an identifiable part or component of a service,~~ the required measures are not general and indiscriminate, but only applied on the basis of objective and non-discriminatory factors, for example, in respect of ~~that~~ a limited part or component of a service; type, frequency or format of a communication; categories of persons concerned; or a geographical criterion;

(b) where necessary, in particular to limit such negative consequences, effective and proportionate safeguards additional to those listed in Article 10(4), (5) and (6) are provided for;

(c) subject to paragraph 9, the period of application remains limited to what is strictly necessary.

9. The competent judicial authority or independent administrative authority shall specify in the detection order the period during which it applies, indicating the start date and the end date.

The start date shall be set taking into account the time reasonably required for the provider to take the necessary measures to prepare the execution of the detection order. It shall not be earlier than three months from the date at which the provider received the detection order and not be later than 12 months from that date.

The period of application of detection orders concerning the dissemination of known or new child sexual abuse material shall not exceed 24 months and that of detection orders concerning the solicitation of children shall not exceed 12 months.

Commented [TM(35]: According to the Finnish Constitutional Law Committee when analysing surveillance and its interference with fundamental rights the focus is on the existence of legislation but also it is essential to analyse how the system in practise function. Thus, it is not enough to note that a detection order should be targeted and specified if it remains unclear how this is in fact possible taking into consideration the technology available. This question is particularly relevant as regard to detecting solicitation of children and how the detection order can be targeted to a specific users or specific groups of users (recital 23) and broad are these groups of users. Could this also mean all communication with a child user?

Secondly, it should be clarified what is the geographical application and scope of a detection order if the parties to the communication reside in different countries.

Commented [KT36]: As mentioned above, the scope must be narrowed down and not be general and indiscriminate. Inspired by the ECJ rulings in the data retention cases.

The Finnish Constitution Article 10(4) does not also allow general, indiscriminate and overall supervision of communications.

Commented [TM(37]: What are these "additional safeguards"?

In recital 23 it is stated that "the specification of the safeguards additional to the ones already expressly specified in this Regulation, such as independent auditing, the provision of additional information or access to data, or reinforced human oversight and review, and the further limitation of the duration of application of the detection order that the Coordinating Authority deems necessary."

Does this means that member states have margin of appreciation to regulate more precisely on issues mentioned e.g. in recital 23 based on Article 7 (8) point (b)?

Commented [PP38]: These are too long. It is very hard to set a proper length so it might be best to leave this to the courts to decide case per case.

Article 8

Additional rules regarding detection orders

1. The competent judicial authority or independent administrative ~~authority~~body whose decision is binding shall issue the detection orders referred to in Article 7 using the template set out in Annex I. Detection orders shall include:

(a) information regarding the measures to be taken to execute the detection order, including the indicators to be used and the safeguards to be provided for, including the reporting requirements set pursuant to Article 9(3) and, where applicable, any additional safeguards as referred to in Article 7(8);

(b) identification details of the competent judicial authority or the independent administrative authority issuing the detection order and authentication of the detection order by that judicial or independent administrative authority;

(c) the name of the provider and, where applicable, its legal representative;

(d) the specific service in respect of which the detection order is issued and, where applicable, the part or component of the service affected as referred to in Article 7(8);

(e) whether the detection order issued concerns the dissemination of known or new child sexual abuse material or the solicitation of children;

(f) the start date and the end date of the detection order;

(g) a sufficiently detailed statement of reasons explaining why the detection order is issued and the conditions set out in article 7, paragraph 4 met;

Commented [KT39]: This is needed so that one can assess the need to appeal and for the appellate court to rule on the matter.

(h) a reference to this Regulation as the legal basis for the detection order;

(i) the date, time stamp and electronic signature of the judicial or independent administrative authority issuing the detection order;

(j) easily understandable information about the redress available to the addressee of the detection order, including information about redress to a court and about the time periods applicable to such redress.

2. The competent judicial authority or independent administrative ~~authority~~ body whose decision is binding issuing the detection order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

The detection order shall be transmitted to the provider's point of contact referred to in Article 23(1), to the Coordinating Authority of establishment and to the EU Centre, through the system established in accordance with Article 39(2).

The detection order shall be ~~drafted~~ **transmitted** in the language declared by the provider pursuant to Article 23(3).

The order may also be transmitted in the language of the authority issuing the order, provided that it is accompanied by a translation of at least the most important elements necessary for the execution of the order into the language declared by the provider in accordance with article 23(3).

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

Commented [KT40]: This paragraph should be removed due to its problematic nature from the perspective of rule of law. With regard to possible errors in a court judgment, the legal remedy is to appeal. Moreover, other authorities cannot clarify a judgment made by a court. The Court's judgment should entail adequate information for its enforcement and legal provision must be precise enough to guarantee this.

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

Article 9

Redress, information, reporting and modification of detection orders

1. Providers of hosting services and providers of interpersonal communications services that have received a detection order, as well as users affected by the measures taken to execute it, shall have a right to effective redress. That right shall include the right to challenge the detection order before the courts of the Member State of the competent judicial authority or independent administrative authority that issued the detection order.

Commented [KT41]: We have reservations to what extent it is possible to provide (all?) users affected by the measures taken to execute it the right to challenge the detection order before a court. Nevertheless, a strong legal protection is essential and a prerequisite for this kind of regulation. We will examine this issue further together with the supervision system of this Regulation in follow up negotiations.

2. When the detection order becomes final, the competent judicial authority or independent administrative authority that issued the detection order shall, without undue delay, ~~transmit a copy thereof to~~ **inform** the Coordinating Authority of establishment. The Coordinating Authority of establishment shall then, without undue delay, transmit a copy ~~thereof~~ **of the detection order** to all other Coordinating Authorities through the system established in accordance with Article 39(2).

For the purpose of the first subparagraph, a detection order shall become final upon the expiry of the time period for appeal where no appeal has been lodged in accordance with national law or upon confirmation of the detection order following an appeal.

3. Where the period of application of the detection order exceeds 12 months, or six months in the case of a detection order concerning the solicitation of children, the Coordinating Authority of establishment shall require the provider to report to it the necessary information on the execution of the detection order at least once, halfway through the period of application.

Those reports shall include a detailed description of the measures taken to execute the detection order, including the safeguards provided, and information on the functioning in practice of those measures, in particular on their effectiveness in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, and on the consequences of those measures for the rights and legitimate interests of all parties affected.

4. ~~In respect of the detection orders that the competent judicial authority or independent administrative authority issued at its request,~~ the Coordinating Authority of establishment shall, where necessary and in any event following reception of the reports referred to in paragraph 3, assess whether any substantial changes to the grounds for issuing the detection orders occurred and, in particular, whether the conditions of Article 7(4) continue to be met. In that regard, it shall take account of additional mitigation measures that the provider may take to address the significant risk identified at the time of the issuance of the detection order.

That Coordinating Authority shall request to the competent judicial authority or independent administrative authority that issued the detection order the modification or revocation of such order, where necessary in the light of the outcome of that assessment. The provisions of this Section shall apply to such requests, *mutatis mutandis*.

Article 10

Technologies and safeguards

1. Providers of hosting services and providers of interpersonal communication services that have received a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46.

2. The provider shall be entitled to acquire, install and operate, free of charge, technologies made available by the EU Centre in accordance with Article 50(1), for the sole purpose of executing the detection order. The provider shall not be required to use any specific technology, including those made available by the EU Centre, as long as the requirements set out in this Article are met. ~~The use of the technologies made available by the EU Centre shall not affect the responsibility of the provider to comply with those requirements and for any decisions it may take in connection to or as a result of the use of the technologies.~~

Commented [KT42]: Since this is a general power, it needs to be limited to necessary.

Commented [TM(43]: This is rather broad and it is difficult to analyse what should be in fact reported: does it include false positives or complaints against the service provider?

Commented [TM(44]: What is the additional value of this as all detection orders are given by the competent judicial authority or independent administrative authority?

Commented [KT45]: The providers should be able to trust the technologies that are made available to them.

At least it should be: "..shall not fully exempt them from the responsibility…"

3. The technologies shall ~~be~~:

(a) be effective, suitable and not easily circumvented in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;

(b) not be able to extract or deduce any other information from the relevant communications than the information strictly necessary to detect, using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;

(c) be in accordance with the state of the art in the industry and the least intrusive in terms of the impact on the users' rights to private and family life, including the confidentiality of communication, and to protection of personal data;

(d) be sufficiently reliable, in that they limit to the maximum extent possible the rate of errors regarding the detection;

4. The provider shall:

(a) take all the necessary measures to ensure that the technologies and indicators, as well as the processing of personal data and other data in connection thereto, are used for the sole purpose of detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, insofar as strictly necessary to execute the detection orders addressed to them;

(b) establish effective internal procedures to prevent and, where necessary, detect and remedy any misuse of the technologies, indicators and personal data and other data referred to in point (a), including unauthorized access to, and unauthorised transfers of, such personal data and other data;

(c) ensure regular human oversight as necessary to ensure that the technologies operate in a sufficiently reliable manner ~~and, where necessary, in particular when potential errors and potential solicitation of children are detected, human intervention~~[3];

(d) establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it, within a reasonable timeframe, complaints about alleged infringements of its obligations under this Section, as well as any decisions that the provider may have taken in relation to the use of the technologies, including the removal or disabling of access to material provided by users, blocking the users' accounts or suspending or terminating the provision of the service to the users, and process such complaints in an objective, effective and timely manner;

Commented [TM(46]: In line with the opinion EDPB/S (pages 24-25) we also consider that the requirements that apply to the technologies to be deployed for the detection of CSAM and solicitation of children do not appear to be sufficiently stringent. In general, as the opinion concludes, also private services providers enjoy a very broad margin of appreciation which might to legal uncertainty on how to balance the rights at stake in each individual case.

The services providers have a very wide margin to decide on the technologies to be used. As this choice of technology is directly connected with the interference of fundamental rights, including the scope and breadth of this interference, the requirements for the technology are unsatisfactorily broad and open in this respect.

In particular, it should be clarified what is the legal protection of users in the case of misuse of these technologies, including the unauthorised use of information obtained through these technologies. Additionally, what is the possibility of public authority to supervise the possible misuse of technologies for other purposes than those prescribed in this Regulation.

Commented [TM(47]: If the used technologies may be easily circumvented and thus not suitable for effectively reaching the aim pursued, they are inconsistent with the principle of proportionality. For instance, if the end-to-end-encryption is undermined but the users can themselves easily re-encrypt their actions, then a detection order may disproportionally affect the users in general without effectively detecting the criminal behaviour.

Commented [TM(48]: See EDPB/S opinion (pages 24-25).

Commented [TM(49]: The meaning of the concept "regular human oversight" should be explained as well as indicated what it would mean in practice? Does it mean that service providers could assess the material and its (criminal) nature before submitting it to the EU Centre?

Commented [KT50]: How service providers are to become aware of false positives?

Are service providers required to keep records for the information about the used technologies, in order to later verification and control of the level of intrusiveness?

[3] Will be included in a recital.

(e) inform the Coordinating Authority, at the latest one month before the start date specified in the detection order, on the implementation of the envisaged measures set out in the implementation plan referred to in Article 7(3);

(f) regularly review the functioning of the measures referred to in points (a), (b), (c) and (d) of this paragraph and adjust them where necessary to ensure that the requirements set out therein are met, as well as document the review process and the outcomes thereof and include that information in the report referred to in Article 9(3).

Commented [TM(51]: Does this and Article 7(3) mean that service providers have to resort to the technologies and implementation plan already reported before a detection order is given considering that they also form the basis and vital information on a Court's decision? Or more like the requirement to update the technologies regularly?

What is the reason for submitting the implementation plan beforehand "including detailed information regarding the envisaged technologies and safeguards" pursuant to Article 7 (3) unless they also play a role in deciding about the detection order?

In other words, how is the wide margin of appreciation of services providers concerning the technologies combined with the process of deciding under which conditions may a detection order be issued?

5. The provider shall inform users in a clear, prominent and comprehensible way of the following:

(a) the fact that it operates technologies to detect online child sexual abuse to execute the detection order, the ways in which it operates those technologies and the impact on the confidentiality of users' communications;

(b) the fact that it is required to report potential online child sexual abuse to the EU Centre in accordance with Article 12;

(c) the users' right of judicial redress referred to in Article 9(1) and their rights to submit complaints to the provider through the mechanism referred to in paragraph 4, point (d) and to the Coordinating Authority in accordance with Article 34.

The provider shall not provide information to users ~~that may reduce the effectiveness of the measures to execute the detection order~~on how to circumvent the detection.

Commented [KT52]: The original text can be read in a way that would make the point a quite void of meaning. This reflects the intention better and is clearer.

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

GERMANY

Meeting of the Law Enforcement Working Party, 3 November 2022

AGENDA ITEM 3: Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

General

- Germany thanks the Presidency for the opportunity to address articles 83–89 in further detail.
- Germany welcomes the possibility to discuss the articles of Chapter I based on the Presidency's compromise text (14008/22).
- As the Federal Government has not yet completed its examination, we would like to enter a general **scrutiny reservation**.

Article 83

- In Germany's view, it is important to receive standardised information about CSA reports and further action taken. This applies in particular to the question of whether investigations were initiated and if not, the reasons why they were not initiated, as well as the results of any subsequent criminal proceedings. Monitoring the orders set out in the Commission's proposal seems important as well.
- We believe that it is necessary to ensure appropriate processes at the same time. As far as Article 83 refers to follow-up measures, it is not clear to us at what point in time information from the national law enforcement agencies or courts concerned is to be submitted. Even if a report were only to be submitted after the conclusion of proceedings, this would likely require a great deal of (new) effort, especially in view of the fact that a report in accordance with Article 12 of the Commission's proposal may contain a large amount of CSAM. With this in mind, Article 83 (2) (a) to (i) appears in some cases to be very extensive. Germany believes that the collection of data should be reduced to a reasonable amount.
- We kindly ask the Commission to explain for which purposes the EU Centre is to be able to request data in accordance with Article 83 (1) and (2) (beyond the need to produce transparency reports).

Article 84

- Germany is generally in favour of transparency reports, especially reports from providers on measures they have taken to combat CSAM. The template to be drawn up in accordance with Article 84 (6) should ensure that reports are as streamlined and as fully automated as possible.
- We kindly ask the Commission to explain why the EU Centre's transparency report (Article 84 (4)) does not contain information in accordance with Article 83 (3) (analogous to Article 84 (1) and (2)).

Article 85

Articles 86 and 87

- We kindly ask the Commission to explain the extent to which privacy rights experts (including EDPS/EDPD) are to be involved in the procedures pursuant to Article 86 and Article 87.

Article 88

Article 89

- The Commission's proposal requires extensive adaptation at national level; this includes in particular establishing or expanding a national authority to serve as Coordinating Authority. To ensure the proper implementation at national level, Germany believes the period for entry into force should ideally be increased to 18 months, but should be at least 12 months.

Chapter I

- Germany thanks the Presidency for its second compromise text on Chapter I.
- Germany is open to the proposal to include online search engines in the scope of the Regulation. This would cover all possible service providers, just as the Digital Services Act (DSA) does. The resulting obligations for online search engine providers (including delisting obligations) are subject to further examination. With this in mind, the revisions in Article 1 (1) (da) and Article 2 (f), (v) and (x) are consistent with the proposal to include online search engines in the scope of the Regulation.
- The Interim Regulation excludes audio communications from its scope (Article 1 (2) of the Interim Regulation). According to the Commission's impact assessment for the proposed Regulation, telephone calls present neither a specific risk nor one that has newly arisen since the Interim Regulation. Technical possibilities for detecting grooming in voice communications are not examined either. We are interested in hearing the views of the other member states on including audio communications in the scope of the Commission's proposal.
- We kindly ask the Presidency to explain why the age of child users has been changed to below 18 in Article 2 (j). We also request an explanation of why the word "potential" has been deleted from the definition of known child sexual abuse material in Article 2 (m) and what effects this deletion is intended to have.

Our proposed wording for taking the decisions of national legislators into account in the definitions has unfortunately not yet found its way into the compromise text. This applies to the age of sexual consent and whether certain content and conduct is punishable. We will be happy to suggest wording related to this issue as well as other aspects of Chapter I, and we are available to discuss this further

HUNGARY

Please find the general and specific comments of Hungary on the discussed document (ST 9068/22).

(i) 'child' means any natural person below the age of 18 years;

(j) 'child user' means a natural person who uses a relevant information society service and who is a natural person below the age of 18~~7~~ years;

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

(k) 'micro, small or medium-sized enterprise' means an enterprise as defined in Commission Recommendation 2003/361 concerning the definition of micro, small and medium-sized enterprises[50];

(l) 'child sexual abuse material' means material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU;

(m) 'known child sexual abuse material' means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (a);

(n) 'new child sexual abuse material' means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (b);

(o) 'solicitation of children' means the solicitation of children for sexual purposes as referred to in Article 6 of Directive 2011/93/EU;

(p) 'online child sexual abuse' means the online dissemination of child sexual abuse material and the solicitation of children;

(q) 'child sexual abuse offences' means offences as defined in Articles 3 to 7 of Directive 2011/93/EU;

(r) 'recommender system' means the system as defined in Article 2, point (o), of Regulation (EU) …/… *[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*;

(s) 'content data' means data as defined in Article 2, point 10, of Regulation (EU) … [on European Production and Preservation Orders for electronic evidence in criminal matters (…/… e-evidence Regulation)];

(t) 'content moderation' means the activities as defined in Article 2, point (p), of Regulation (EU) …/… *[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*;

(u) 'Coordinating Authority of establishment' means the Coordinating Authority for child sexual abuse issues designated in accordance with Article 25 by the Member State where the provider of information society services has its main establishment or, where applicable, where its legal representative resides or is established;

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

EN 42 EN

– enabling users to search for other users and, in particular, for adult users to search for child users;

– enabling users to establish contact with other users directly, in particular through private communications;

– enabling users to share images or videos with other users, in particular through private communications.

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

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

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

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

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

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

(a) for a service which is subject to a detection order issued in accordance with Article 7, the provider shall update the risk assessment at the latest two months before the expiry of the period of application of the detection order;

(b) the Coordinating Authority of establishment may require the provider to update the risk assessment at a reasonable earlier date than the date referred to in the second subparagraph, where there is evidence indicating a possible substantial change in the risk that the service is used for the purpose of online child sexual abuse.

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

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

(a) make reasonable efforts to assess, where possible together with the providers of software applications, whether each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children;

(b) take reasonable measures to prevent child users from accessing the software applications in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children;

(c) take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b).

2. In assessing the risk referred to in paragraph 1, the provider shall take into account all the available information, including the results of the risk assessment conducted or updated pursuant to Article 3.

3. Providers of software application stores shall make publicly available information describing the process and criteria used to assess the risk and describing the measures referred to in paragraph 1. That description shall not include information that may reduce the effectiveness of the assessment of those measures.

4. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1, 2 and 3, having due regard in particular to relevant technological developments and to the manners in which the services covered by those provisions are offered and used.

Section 2
Detection obligations

Article 7

Issuance of detection orders

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

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect online child sexual abuse on a specific service.

2. The Coordinating Authority of establishment shall, before requesting the issuance of a detection order, carry out the investigations and assessments necessary to determine whether the conditions of paragraph 4 have been met.

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

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

Commented [HU4]: badly worded, as if it had no discretion on emissions at all

(a) there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5, 6 and 7, as applicable;

(b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties.

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

(a) the risk assessment conducted or updated and any mitigation measures taken by the provider pursuant to Articles 3 and 4, including any mitigation measures introduced, reviewed, discontinued or expanded pursuant to Article 5(4) where applicable;

(b) any additional information obtained pursuant to paragraph 2 or any other relevant information available to it, in particular regarding the use, design and operation of the service, regarding the provider's financial and technological capabilities and size and regarding the potential consequences of the measures to be taken to execute the detection order for all other parties affected;

(c) the views and the implementation plan of the provider submitted in accordance with paragraph 3;

(d) the opinions of the EU Centre and of the data protection authority submitted in accordance with paragraph 3.

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

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

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

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

(e) whether the detection order issued concerns the dissemination of known or new child sexual abuse material or the solicitation of children;

(f) the start date and the end date of the detection order;

(g) a sufficiently detailed statement of reasons explaining why the detection order is issued;

(h) a reference to this Regulation as the legal basis for the detection order;

(i) the date, time stamp and electronic signature of the judicial or independent administrative authority issuing the detection order;

(j) easily understandable information about the redress available to the addressee of the detection order, including information about redress to a court and about the time periods applicable to such redress.

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

The detection order shall be transmitted to the provider's point of contact referred to in Article 23(1), to the Coordinating Authority of establishment and to the EU Centre, through the system established in accordance with Article 39(2).

The detection order shall be drafted in the language declared by the provider pursuant to Article 23(3).

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

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

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

Article 9

Redress, information, reporting and modification of detection orders

1. Providers of hosting services and providers of interpersonal communications services that have received a detection order, as well as users affected by the measures taken to execute it, shall have a right to effective redress. That right shall include the right to challenge the detection order before the courts of the Member State of the competent judicial authority or independent administrative authority that issued the detection order.

2. When the detection order becomes final, the competent judicial authority or independent administrative authority that issued the detection order shall, without undue delay, transmit a copy thereof to the Coordinating Authority of establishment.

Section 3

Reporting obligations

Article 12

Reporting obligations

1. Where a provider of hosting services or a provider of interpersonal communications services becomes aware in any manner other than through a removal order issued in accordance with this Regulation of any information indicating potential online child sexual abuse on its services, it shall promptly submit a report thereon to the EU Centre in accordance with Article 13. It shall do so through the system established in accordance with Article 39(2).

2. Where the provider submits a report pursuant to paragraph 1, it shall inform the user concerned, providing information on the main content of the report, on the manner in which the provider has become aware of the potential child sexual abuse concerned, on the follow-up given to the report insofar as such information is available to the provider and on the user's possibilities of redress, including on the right to submit complaints to the Coordinating Authority in accordance with Article 34.

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

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

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

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

Article 13

Specific requirements for reporting

1. Providers of hosting services and providers of interpersonal communications services shall submit the report referred to in Article 12 using the template set out in Annex III. The report shall include:

   (a) identification details of the provider and, where applicable, its legal representative;

   (b) the date, time stamp and electronic signature of the provider;

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

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

(e) whether the potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material or the solicitation of children;

(f) information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address;

(g) information concerning the identity of any user involved in the potential online child sexual abuse;

(h) whether the provider has also reported, or will also report, the potential online child sexual abuse to a public authority or other entity competent to receive such reports of a third country and if so, which authority or entity;

(i) where the potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material, whether the provider has removed or disabled access to the material;

(j) whether the provider considers that the report requires urgent action;

(k) a reference to this Regulation as the legal basis for reporting.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annex III to improve the template where necessary in view of relevant technological developments or practical experiences gained.

Section 4
Removal obligations

Article 14

Removal orders

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

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

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

3. The competent judicial authority or the independent administrative authority shall issue a removal order using the template set out in Annex IV. Removal orders shall include:

(a) identification details of the judicial or independent administrative authority issuing the removal order and authentication of the removal order by that authority;

(b) the name of the provider and, where applicable, of its legal representative;

(c) the specific service for which the removal order is issued;

(d) a sufficiently detailed statement of reasons explaining why the removal order is issued and in particular why the material constitutes child sexual abuse material;

(e) an exact uniform resource locator and, where necessary, additional information for the identification of the child sexual abuse material;

(f) where applicable, the information about non-disclosure during a specified time period, in accordance with Article 15(4), point (c);

(g) a reference to this Regulation as the legal basis for the removal order;

(h) the date, time stamp and electronic signature of the judicial or independent administrative authority issuing the removal order;

(i) easily understandable information about the redress available to the addressee of the removal order, including information about redress to a court and about the time periods applicable to such redress.

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

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

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

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

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

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

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

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

In such a case:

(a) the judicial authority or independent administrative authority issuing the removal order shall set the time period not longer than necessary and not exceeding six weeks, during which the provider is not to disclose such information;

(b) the obligations set out in paragraph 3 shall not apply during that time period;

(c) that judicial authority or independent administrative authority shall inform the provider of its decision, specifying the applicable time period.

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

Section 5
Blocking obligations

Article 16

Blocking orders

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

2. The Coordinating Authority of establishment shall, before requesting the issuance of a blocking order, carry out all investigations and assessments necessary to determine whether the conditions of paragraph 4 have been met.

To that end, it shall, where appropriate:

(a) verify that, in respect of all or a representative sample of the uniform resource locators on the list referred to in paragraph 1, the conditions of Article 36(1), point (b), are met, including by carrying out checks to verify in cooperation with the EU Centre that the list is complete, accurate and up-to-date;

(b) require the provider to submit, within a reasonable time period set by that Coordinating Authority, the necessary information, in particular regarding the accessing or attempting to access by users of the child sexual abuse material

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

Article 20

Victims' right to information

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

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

2. The request referred to in paragraph 1 shall indicate:

   (a) the relevant item or items of known child sexual abuse material;

   (b) where applicable, the individual or entity that is to receive the information on behalf of the person making the request;

   (c) sufficient elements to demonstrate the identity of the person making the request.

3. The information referred to in paragraph 1 shall include:

   (a) the identification of the provider that submitted the report;

   (b) the date of the report;

   (c) whether the EU Centre forwarded the report in accordance with Article 48(3) and, if so, to which authorities;

   (d) whether the provider reported having removed or disabled access to the material, in accordance with Article 13(1), point (i).

Article 21

Victims' right of assistance and support for removal

1. Providers of hosting services shall provide reasonable assistance, on request, to persons residing in the Union that seek to have one or more specific items of known child sexual abuse material depicting them removed or to have access thereto disabled by the provider.

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

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

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

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

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

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

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

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

Article 23

Points of contact

1. Providers of relevant information society services shall establish a single point of contact allowing for direct communication, by electronic means, with the Coordinating Authorities, other competent authorities of the Member States, the Commission and the EU Centre, for the application of this Regulation.

2. The providers shall communicate to the EU Centre and make public the information necessary to easily identify and communicate with their single points of contact, including their names, addresses, the electronic mail addresses and telephone numbers.

3. The providers shall specify in the information referred to in paragraph 2 the official language or languages of the Union, which can be used to communicate with their points of contact.

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

Article 24

Legal representative

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

CHAPTER III

SUPERVISION, ENFORCEMENT AND COOPERATION

Section 1
Coordinating Authorities for child sexual abuse issues

Article 25

Coordinating Authorities for child sexual abuse issues and other competent authorities

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

2. Member States shall, by the date referred to in paragraph 1, designate one of the competent authorities as their Coordinating Authority for child sexual abuse issues ('Coordinating Authority').

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

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

3. Where a Member State designates more than one competent authority in addition to the Coordinating Authority, it shall ensure that the respective tasks of those authorities and of the Coordinating Authority are clearly defined and that they cooperate closely and effectively when performing their tasks. The Member State concerned shall communicate the name of the other competent authorities as well as their respective tasks to the EU Centre and the Commission.

4. Within one week after the designation of the Coordinating Authorities and any other competent authorities pursuant to paragraph 1, Member States shall make publicly available, and communicate to the Commission and the EU Centre, the name of their Coordinating Authority. They shall keep that information updated.

5. Each Member State shall ensure that a contact point is designated or established within the Coordinating Authority's office to handle requests for clarification, feedback and other communications in relation to all matters related to the application and enforcement of this Regulation in that Member State. Member States shall make the information on the contact point publicly available and communicate it to the EU Centre. They shall keep that information updated.

6. Within two weeks after the designation of the Coordinating Authorities pursuant to paragraph 2, the EU Centre shall set up an online register listing the Coordinating

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

Authorities and their contact points. The EU Centre shall regularly publish any modification thereto.

7. Coordinating Authorities may, where necessary for the performance of their tasks under this Regulation, request the assistance of the EU Centre in carrying out those tasks, in particular by requesting the EU Centre to:

   (a) provide certain information or technical expertise on matters covered by this Regulation;

   (b) assist in assessing, in accordance with Article 5(2), the risk assessment conducted or updated or the mitigation measures taken by a provider of hosting or interpersonal communication services under the jurisdiction of the Member State that designated the requesting Coordinating Authority;

   (c) verify the possible need to request competent national authorities to issue a detection order, a removal order or a blocking order in respect of a service under the jurisdiction of the Member State that designated that Coordinating Authority;

   (d) verify the effectiveness of a detection order or a removal order issued upon the request of the requesting Coordinating Authority.

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

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

Article 26

Requirements for Coordinating Authorities

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

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

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

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

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

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

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

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

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

(a) the provider has failed to take the necessary measures to terminate the infringement;

(b) the temporary restriction does not unduly restrict access to lawful information by users of the service, having regard to the number of users affected and whether any adequate and readily accessible alternatives exist.

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

Article 30

Common provisions on investigatory and enforcement powers

1. The measures taken by the Coordinating Authorities in the exercise of their investigatory and enforcement powers referred to in Articles 27, 28 and 29 shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement of this Regulation or suspected infringement to which those measures relate, as well as the economic, technical and operational capacity of the provider of relevant information society services concerned, where applicable.

2. Member States shall ensure that any exercise of the investigatory and enforcement powers referred to in Articles 27, 28 and 29 is subject to adequate safeguards laid down in the applicable national law to respect the fundamental rights of all parties affected. In particular, those measures shall only be taken in accordance with the right to respect for private life and the rights of defence, including the rights to be heard and of access to the file, and subject to the right to an effective judicial remedy of all parties affected.

Article 31

Searches to verify compliance

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

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

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

Article 32

Notification of known child sexual abuse material

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

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

Section 3

Other provisions on enforcement

Article 33

Jurisdiction

1. The Member State in which the main establishment of the provider of relevant information society services is located shall have jurisdiction for the purposes of this Regulation.

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

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

Article 34

Right of users of the service to lodge a complaint

1. Users shall have the right to lodge a complaint alleging an infringement of this Regulation affecting them against providers of relevant information society services with the Coordinating Authority designated by the Member State where the user resides or is established.

2. Coordinating Authorities shall provide child-friendly mechanisms to submit a complaint under this Article and adopt a child-sensitive approach when handling

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

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

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

Article 35

Penalties

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

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

2. Member States shall ensure that the maximum amount of penalties imposed for an infringement of this Regulation shall not exceed 6 % of the annual income or global turnover of the preceding business year of the provider.

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

3. Penalties for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information or to submit to an on-site inspection shall not exceed 1% of the annual income or global turnover of the preceding business year of the provider or the other person referred to in Article 27.

4. Member States shall ensure that the maximum amount of a periodic penalty payment shall not exceed 5 % of the average daily global turnover of the provider or the other person referred to in Article 27 in the preceding financial year per day, calculated from the date specified in the decision concerned.

5. Member States shall ensure that, when deciding whether to impose a penalty and when determining the type and level of penalty, account is taken of all relevant circumstances, including:

(a) the nature, gravity and duration of the infringement;

(b) whether the infringement was intentional or negligent;

(c) any previous infringements by the provider or the other person;

(d) the financial strength of the provider or the other person;

(e) the level of cooperation of the provider or the other person;

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

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

Article 37

Cross-border cooperation among Coordinating Authorities

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

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

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

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

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

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

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

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

   Where it considers that it has insufficient information to 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 investigations

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

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

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

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

Article 39

General cooperation and information-sharing system

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

2. The EU Centre shall establish and maintain one or more reliable and secure information sharing systems supporting communications between Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services.

3. The Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services shall use the information-sharing systems referred to in paragraph 2 for all relevant communications pursuant to this Regulation.

4. The Commission shall adopt implementing acts laying down the practical and operational arrangements for the functioning of the information-sharing systems referred to in paragraph 2 and their interoperability with other relevant systems. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 87.

CHAPTER IV

EU CENTRE TO PREVENT AND COMBAT CHILD SEXUAL ABUSE

Section 1

Principles

Article 40

Establishment and scope of action of the EU Centre

1. A European Union Agency to prevent and combat child sexual abuse, the EU Centre on Child Sexual Abuse, is established.

2. The EU Centre shall contribute to the achievement of the objective of this Regulation by supporting and facilitating the implementation of its provisions concerning the detection, reporting, removal or disabling of access to, and blocking of online child sexual abuse and gather and share information and expertise and facilitate cooperation between relevant public and private parties in connection to the prevention and combating of child sexual abuse, in particular online.

Article 41

Legal status

1. The EU Centre shall be a body of the Union with legal personality.

2. In each of the Member States the EU Centre shall enjoy the most extensive legal capacity accorded to legal persons under their laws. It may, in particular, acquire and dispose of movable and immovable property and be party to legal proceedings.

3. The EU Centre shall be represented by its Executive Director.

Article 42

Seat

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

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

Section 2

Tasks

Article 43

Tasks of the EU Centre

The EU Centre shall:

Article 53

Cooperation with Europol

Commented [HU20]: More detailed rules are needed on the relationship with Europol.

1. Where necessary for the performance of its tasks under this Regulation, within their respective mandates, the EU Centre shall cooperate with Europol.

2. Europol and the EU Centre shall provide each other with the fullest possible access to relevant information and information systems, where necessary for the performance of their respective tasks and in accordance with the acts of Union law regulating such access.

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

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

Article 54

Cooperation with partner organisations

1. Where necessary for the performance of its tasks under this Regulation, the EU Centre may cooperate with organisations and networks with information and expertise on matters related to the prevention and combating of online child sexual abuse, including civil society organisations and semi-public organisations.

2. The EU Centre may conclude memoranda of understanding with organisations referred to in paragraph 1, laying down the terms of cooperation.

Section 5

Organisation

Article 55

Administrative and management structure

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

(a) a Management Board, which shall exercise the functions set out in Article 57;

(b) an Executive Board which shall perform the tasks set out in Article 62;

(c) an Executive Director of the EU Centre, who shall exercise the responsibilities set out in Article 64;

(d) a Technology Committee as an advisory group, which shall exercise the tasks set out in Article 66.

CHAPTER V

DATA COLLECTION AND TRANSPARENCY REPORTING

Article 83

Data collection

1. Providers of hosting services, providers of interpersonal communications services and providers of internet access services shall collect data on the following topics and make that information available to the EU Centre upon request:

   (a) where the provider has been subject to a detection order issued in accordance with Article 7:

   – the measures taken to comply with the order, including the technologies used for that purpose and the safeguards provided;

   – the error rates of the technologies deployed to detect online child sexual abuse and measures taken to prevent or remedy any errors;

   – in relation to complaints and cases submitted by users in connection to the measures taken to comply with the order, the number of complaints submitted directly to the provider, the number of cases brought before a judicial authority, the basis for those complaints and cases, the decisions taken in respect of those complaints and in those cases, the average time needed for taking those decisions and the number of instances where those decisions were subsequently reversed;

   (b) the number of removal orders issued to the provider in accordance with Article 14 and the average time needed for removing or disabling access to the item or items of child sexual abuse material in question;

   (c) the total number of items of child sexual abuse material that the provider removed or to which it disabled access, broken down by whether the items were removed or access thereto was disabled pursuant to a removal order or to a notice submitted by a Competent Authority, the EU Centre or a third party or at the provider's own initiative;

   (d) the number of blocking orders issued to the provider in accordance with Article 16;

   (e) the number of instances in which the provider invoked Article 8(3), Article 14(5) or (6) or Article 17(5), together with the grounds therefor;

2. The Coordinating Authorities shall collect data on the following topics and make that information available to the EU Centre upon request:

   (a) the follow-up given to reports of potential online child sexual abuse that the EU Centre forwarded in accordance with Article 48(3), specifying for each report:

Commented [KSAd21]: HU would like to see more conceret ruling here.

– whether the report led to the launch of a criminal investigation, contributed to an ongoing investigation, led to taking any other action or led to no action;

~~– where the report led to the launch of a criminal investigation or contributed to an ongoing investigation, the state of play or outcome of the investigation, including whether the case was closed at pre-trial stage, whether the case led to the imposition of penalties, whether victims were identified and rescued and if so their numbers differentiating by gender and age, and whether any suspects were arrested and any perpetrators were convicted and if so their numbers;~~

Commented [KSAd22]: HU do not want to share concrete information on ongoing investigations or trials. Reporting on the administrative aspects should be enough for the EU Centre.

– where the report led to any ~~other~~ action, the type of action, the state of play or outcome of that action and the reasons for taking it;

– where no action was taken, the reasons for not taking any action;

(b) the most important and recurrent risks of online child sexual abuse, as reported by providers of hosting services and providers of interpersonal communications services in accordance with Article 3 or identified through other information available to the Coordinating Authority;

(c) a list of the providers of hosting services and providers of interpersonal communications services to which the Coordinating Authority addressed a detection order in accordance with Article 7;

(d) the number of detection orders issued in accordance with Article 7, broken down by provider and by type of online child sexual abuse, and the number of instances in which the provider invoked Article 8(3);

(e) a list of providers of hosting services to which the Coordinating Authority issued a removal order in accordance with Article 14;

(f) the number of removal orders issued in accordance with Article 14, broken down by provider, the time needed to remove or disable access to the item or items of child sexual abuse material concerned, and the number of instances in which the provider invoked Article 14(5) and (6);

(g) the number of blocking orders issued in accordance with Article 16, broken down by provider, and the number of instances in which the provider invoked Article 17(5);

(h) ~~a list of relevant information society services to which the Coordinating Authority addressed a decision taken pursuant to Articles 27, 28 or 29, the type of decision taken, and the reasons for taking it;~~

Commented [KSAd23]: Which services can be detected as relevant?

(i) the instances in which the opinion of the EU Centre pursuant to Article 7(4)(d) substantially deviated from the opinion of the Coordinating Authority, specifying the points at which it deviated and the main reasons for the deviation.

Centre shall ensure that the data referred to in paragraphs 1, 2 and 3, respectively, is stored ~~no longer than is necessary~~ for the transparency reporting referred to in Article 84. The data stored shall not contain any personal data.

5. They shall ensure that the data is stored in a secure manner and that the storage is subject to appropriate technical and organisational safeguards. Those safeguards shall ensure, in particular, that the data can be accessed and processed only for the purpose for which it is stored, that a high level of security is achieved and that the information is deleted when no longer necessary for that purpose. They shall regularly review those safeguards and adjust them where necessary.

Article 84

Transparency reporting

1. Each provider of relevant information society services shall draw up an annual report on its activities under this Regulation. That report shall compile the information referred to in Article 83(1). The providers shall, by 31 January of every year subsequent to the year to which the report relates, make the report available to the public and communicate it to the Coordinating Authority of establishment, the Commission and the EU Centre.

2. Each Coordinating Authority shall draw up an annual report on its activities under this Regulation. That report shall compile the information referred to in Article 83(2). It shall, by 31 March of every year subsequent to the year to which the report relates, make the report available to the public and communicate it to the Commission and the EU Centre.

3. Where a Member State has designated several competent authorities pursuant to Article 25, it shall ensure that the Coordinating Authority draws up a single report covering the activities of all competent authorities under this Regulation and that the Coordinating Authority receives all relevant information and support needed to that effect from the other competent authorities concerned.

4. The EU Centre, working in close cooperation with the Coordinating Authorities, shall draw up an annual report on its activities under this Regulation. That report shall also compile and analyse the information contained in the reports referred to in paragraphs 2 and 3. The EU Centre shall, by 30 June of every year subsequent to the year to which the report relates, make the report available to the public and communicate it to the Commission.

5. The annual transparency reports referred to in paragraphs 1, 2 and 3 shall not include any information that may prejudice ongoing activities for the assistance to victims or the prevention, detection, investigation or prosecution of child sexual abuse offences. They shall also not contain any personal data.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to supplement this Regulation with the necessary templates and detailed rules concerning the form, precise content and other details of the reports and the reporting process pursuant to paragraphs 1, 2 and 3.

Written comments from Hungary regarding the Commission's Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (9068/22) – Chapter V and VI.

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

On behalf of Hungary, we thank the Presidency for the work it has invested. The compromise text of Chapter I is acceptable for us.

Our position on Chapter V is that regarding the data collection and transparency reporting more detailed analysis is needed, as it seems to be a bit too detailed, since not just statistics, but detailed activity reports from Member States is required. For coordinating authorities, this detailed data provision will be a significant burden.

As regards the phrase *"upon request"* in Article 83 (2), we would like to see more clarity on the underlying meaning of this, so we would like to see more specific wording on this.

As regards the Article 83 (2), since Hungary does not wish to share specific information on ongoing investigations or judicial proceedings and reporting on administrative aspects should be sufficient for the EU Centre, we propose to delete the second paragraph of Article 83 (2) (a) and the word *"other"* in the third paragraph.

With regard to the second paragraph of Article 83 (2) (a), we would like to note in general that collecting data on the basis of *"gender"* is unacceptable to us.

According to the horizontal Hungarian position, we reject the concept of gender, and for us the collection of data based on *"sex"* is appropriate. Therefore, Article 83 (2) (a), the collection of data based on *"gender"* should be replaced by the word "sex". For the Hungarian side, we reject the concept of gender as such, in our view there is only sex. **Furthermore, in practice, the authorities collect data only on the basis of sex, not on gender, so the mandate cannot be fulfilled in this way.**

We propose the deletion of Article 83 (2) (h), as it is not clear from Hungary which service providers are covered and which are considered relevant.

In Article 83(4), we propose to delete the part *"no longer than it necessary"*, as we are of the opinion that this is also not sufficiently specified.

Please find our specific comments included in the attached document "HU incorporated comments on Draft CSA st9068.en22".

Budapest, 11 November 2022.

IRELAND

Chapter VI – IE Response

FINAL PROVISIONS

Given the complexity of the proposed regulation, we believe that a minimum period of twenty-four months should be given for the application of the Regulation (article 90), following entry into force, rather than the six-month timeframe that is currently proposed.

Furthermore consideration needs to be given to ensure that there is no gap in detection of known or new CSAM, as we transition from the existing legal frameworks to the provisions contained within this proposal, once it enters into force.

ITALY

The remarks of the Italian delegation are the following:

- - regarding Article 83, we have to consider the fact that it is hard to force the coordination authorithy to give up many information related to ongoing investigations. it would be better to water down the mandatory obligation, and use the word 'should' instead;
- - regarding Art 89, should be foreseen at least 1 year the coming into effect

LATVIA

Written comments on the proposed CSA Regulation (doc. 9068/22)[1] as a follow-up to the LEWP-P meeting held on 3 November 2022

LV maintains **a general scrutiny reservation**

Article 85 "Evaluation"

Para 2:

- LV would favour that evaluation of the EU Centre referred to in paragraph 2 of this Article **would be carried out by COM** (it is currently foreseen that "COM shall ensure that an evaluation (…) is carried out").

  In this regard, Europol Regulation[2] (Article 68(1)), for instance, clearly states that "by 29 June 2027 and every five years thereafter, the Commission shall carry out an evaluation, in particular, of the impact, effectiveness and efficiency of Europol and of its working practices. That evaluation may, in particular, address the possible need to modify the structure, operation, field of action and tasks of Europol, and the financial implications of any such modification".

- LV would like to clarify whether the findings of evaluation, carried out in accordance with paragraph 2, will be reported **to anyone**; in LV view, it is not entirely clear from the current wording (in accordance with paragraph 4, COM reports to the European Parliament (hereinafter – EP) and the Council the findings of the evaluation referred to in paragraph 3

[1] Proposal for a Regulation of the European Parliament and of the Council laying down the rules to prevent and combat child sexual abuse (COM (2022) 209 final).

[2] **Regulation (EU) 2016/794** of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

of this Article, namely, findings of every second evaluation referred to in paragraph 2 of this Article). LV considers that **all findings** of the evaluation referred to in paragraph 2 of this Article should be reported to the relevant stakeholders.

In addition, LV would like to see **the Management Board of the EU Centre** (hereinafter – MB) being involved in the evaluation of the EU Centre. LV **is opened to** further discuss the exact model of the MB involvement, for instance, the current ones in the context of JHA agencies:

- eu-LISA Regulation[3] (Article 39(1)) specifies that COM shall carry out an evaluation of eu-LISA after consulting the Management Board of eu-LISA;
- Europol Regulation (Article 68(2)) specifies that COM shall submit the evaluation report the Management Board of Europol which shall provide its observations on the evaluation report within three months from the date of receipt; then COM shall submit the final evaluation report, together with the COM's conclusions, and the Management Board's observations in an annex thereto, to the EP, the Council, the national parliaments and the Management Board.

In any case, LV believes that the findings of the evaluation shall be reported not only to the EP and the Council, **but also to the MB**.

LV also considers that the reference to "the Coordinating Authorities" in paragraph 5 of this Article should be deleted. In LV view, the **reference to "Member States"** in this paragraph is sufficient (this reference covers also Coordinating Authorities).

Article 88 "Repeal"

In accordance with this Article, Regulation (EU) 2021/1232[4] is repealed from the date of application of the proposed CSA Regulation. Bearing in mind that the process of issuing the first detection orders will be lengthy (according to COM, it may take approximately one year), LV sees that there will be a legal gap – namely, approximately one year after the date of application of the proposed CSA Regulation, providers of interpersonal communications services will neither be allowed to voluntarily detect child sexual abuse material (hereinafter – CSAM), nor they (some of them) will be obliged to detect CSAM, based on the issued detection order.

Bearing this in mind, LV finds it crucial to remedy this deficiency in the transition phase by **revising the repeal deadline** of Regulation (EU) 2021/1232 (for instance, it could be determined that Regulation (EU) 2021/1232 is repealed one year after the proposed CSA Regulation becomes applicable).

Article 89 "Entry into force and application"

LV finds it important to have sufficient time to prepare for the application of the proposed CSA Regulation that would allow to establish a well-functioning system for a more effective fight against child sexual abuse online.

LV therefore considers that **a longer period (at least 12 months)** should be foreseen for the start of the application of the proposed CSA Regulation provided that this **does not result in a legal gap in**

---

3 **Regulation (EU) 2018/1726** of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

4 **Regulation (EU) 2021/1232** of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (OJ L 274, 30.7.2021, p. 41).

application of Regulation (EU) 2021/1232 and the proposed CSA Regulation (in this context, the available options for the possible extension of the application of Regulation (EU) 2021/1232 should be duly considered).

MALTA

Malta's Comments on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (ST 14008/22)

Following the Law Enforcement Working Party meeting held on 3 November 2022, below please find Malta's comments on Chapter V and VI as follows:

Article 83 'Data Collection'

Malta joins other Member States in calling for data collection to be only limited to necessary collection, in order to avoid adding administrative burdens on the envisaged Coordinating Authorities and competent authorities.

Paragraph 3

Malta supports an ensuing recommendation EDPB-EDPS Joint Opinion 4/2022 in line 136 regarding statistics relating to Europol.

Article 89 'Entry into force and application'

Malta joins other Member States in calling for a longer period of application over and above six months.

POLAND

PL remarks to Chapter V and VI

Art. 83 (1) – it is worth to consider that the data, collected according to art. 83 para 1, should be available also to the Coordinating Authorities upon request.

Art. 83 (2) - with regard to the obligation to collect data by the Coordinating Authorities, it should be emphasized that providing information on follow-up given to the reports by law enforcement authorities, cannot in any way violate the secrecy of the investigation and classified nature of operational activities. It should not go beyond sharing the statistical information, without giving any personal details of the perpetrators and victims, the modus operandi of the case, information on how to identify the perpetrators or victims. Only the numbers are acceptable for PL, without entering in the details of the cases. Therefore we do support the art 83 para 4., stating that the collected data cannot contain personal data.

However, taking into account the anticipated overwhelming quantity of the reports and constant overload of the law enforcement agencies, especially in the cybercrime area nowadays, PL shares the view of the majority of the Member States as regards the necessity to avoid additional, unproportional administrative burden to the law enforcement. Having said that, we suggest that the Coordinating Authorities should provide EU Centre once a year an information on the number of launched and closed criminal investigations, with no personal data. The rational behind this approach is as follows:

- this solution safeguards both transparency and proportionality;
- in order conduct an accurate statistical research and assess the effectiveness of the regulation, EU Centre needs a representative amount of data. Requests of information and answers in particular cases, will not allow fulfilling these tasks. For example, it is unclear,

what will the EU Centre do with an information on a single investigation that is ongoing. Firstly, it does not have statistical value and secondly, it shouldn't be the EU Centre's role to assess the performance of the law enforcement tasks.

- providing and updating information on every investigation by law enforcement might be significantly challenging, if not impossible; we cannot cause the situation that law enforcement will be obliged to spend more time on reporting back on the follow-up than on investigation itself.

Art. 83 (2) (e) – the authority entitled to issues an order has to be updated, in accordance with changes foreseen in art. 14 – "Competent authority" instead of "Coordinating Authority"

Art. 88 – PL supports the position of other Member States that some transition period between the repeal of the temporary regulation and application of CSA is required. We suggest 12 months.

Art. 89 – The regulation shall apply from 12 months after its entry into force.

PORTUGAL

COMMENTS OF THE PORTUGUESE DELEGATION

The Portuguese delegation wishes to thank the Presidency for the possibility to comment these two texts.

Doc 14008/22

Regarding the compromise text, PT wishes to make the following comments:

Article 1 – as mentioned previously, the dimension to assistance is still lacking. Portugal would like to have it introduced here, unless this dimension is not an objective of the Regulation. In that case, we should further discuss this issue.

Article 1 no. 1 da) - it would be worth to include also in this new *alínea* the internet addresses that promote or disseminate CSAM materials or images.

Doc 9068/22

As for chapters V and VI of the document, Portugal delegations wishes to make the following comments:

Article 83 - data collection

This is a very long article on data collection obligations and affects. It summarizes all the activities of these entities, but again, it mentions very briefly prevention and assistance. Nothing is mentioned on the intervention of victims which we deem very necessary.

In addition to this general consideration, the following appears:

In relation to paragraph 1, reference should be made to the scope of application of the obligation. We should clarify the space to which these data refer, maybe data relating to the scope of jurisdiction of the state that issued the detention order. But it could also, for example, be data relating to the state of the main establishment (where the main financial functions and operational control of the service provider are carried out) or any other criteria. So therefore it should be explained.

A lot of information with a high degree of disaggregation is also requested, which will only be useful if it can in fact be filled in a consistent and updated way. It is information that should be collected in a network and with common indicators. This has to be taken into account on the transposition articles.

The information requested also has to do with data that the entity - on whom the obli9gation falls- does not have (this is specially concerning in relation to n. 1 a) but will also affect n.2 j) . This collection will be difficult and emphasizes the need for a very extensive network collection of information.

Sometimes the requested information needs to be more concrete: who and how will define the elements referred to in article 83, n. 1 c), and n.2 d)?

In n. 2 d) are we referring to the communication of risks carried out under the terms of article 5 (risk report) or is it something else.

We would also like to understand the scope of the "potential" referred to in paragraph 3 of indents d), f), h) and f).

Article 86 – delegated acts

As for the delegated acts provided for in article 86, PT delegation believes that this article should only be debated after discussion of the annexes document (doc 9068/22 ADD 4).

In any case, delegated acts are defined by the Treaties as non-legislative acts of general scope, which can only be adopted if the delegation of powers is delimited in a legislative act, being able to *supplement or amend certain non-essential elements thereof.*

Thus, it has been very difficult to perceive a delegation of competence meant to "*improve the model*", as in the case of article 13, n. 2, 14, n. 8 and 17 n. 6. This specially applies to some of the interventions of article 47: for example, to decide on detailed rules on the precise content, the creation and operation of the indicators databases referred to in paragraph 1 of article 44, or paragraph 1 of article 45 . Those elements could be considered essential elements, and therefore should not be included in article 86 .

The same reflection applies to indent d) of the same article 47 or even indent e) and to point 6 of article 84 regarding the "exact content and other details".

Eventually, a reference in article 86 to changes caused by *reported developments in the technologies and procedures involved* (otherwise we run the risk that in a few years the text will become outdated), may resolve the situation.

SLOVENIA

With reference to the LEWEP Police meeting on 3 November 2002 and the Presidency follow-up message, please find bellow written comments of Slovenia on document **ST 9068/22** (Chapter V and VI):

Article 83/2/a – We share the opinion of other states. This will place a heavy burden on the police, which is already at the edge of its capacity. If we take a look at NCMEC, the police cannot handle all the investigations because there are so many. It takes the police a lot of time to prioritise the cases. If we must report on investigations, it will put a disproportionate burden on the police, the prosecution and the court. In addition, we will also have to report on cases that we will not investigate. It is clear from what has been written that the police will have to report the case several times, because investigations are complex and can lead to the discovery of a network of perpetrators and to the further identification of new victims. All of this may also lead to the need to create new records, which is again a new burden. If we are already reporting statistics, this should be regulated as it is now in the provisional regulation, once a year or once a period.

Article 88 – It will be necessary to adjust the time of entry into force of this Regulation and the repeal of the provisional Regulation.

Article 89 – Slovenia also agrees with the others that the deadline of 6 months for the application of the Regulation is too short. It should be at least 12 months.

We also reiterate that Slovenia has a general scrutiny reservation on the proposal.

SPAIN

Follow-up comments to the last LEWP meeting (11/11 /2022)

As regards to the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (Chapters I and II of the CSA proposal): Spain supports all measures to strengthen the detection and surveillance of child pornography and other sexual abuse of minors on the Internet and the idea of encouraging the cooperation of companies that offer services on the web in order to develop prevention strategies. However, this legislative development is very complicated and involves several actors, which is why Spain has a scrutiny reservation on this issue. Having said that, Spain has a general comment to share:

Comments chapters V y VI: art. 89 with respect to Article 89, it is considered appropriate to extend the 6-month period to 12 months.

SWEDEN

Swedish proposal regarding Article 1 on the scope of the Regulation

To be included in Article 1 (from Article 1.4 of the TCO Regulation):

This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to freedom of expression and information [, including freedom and pluralism of the media].

Rationale:

1. Sweden has in the context of the present legal developments such as on the TCO and DSA regulations on counteracting illegal content online taken the position in principle that any legislation establishing new powers for our authorities to act and directing demands on service providers to implement measures must be concerned with content that is defined as illegal in national or EU law. Otherwise, the legislation will cover also legal expressions and there will be an infringement of the freedoms of expression and information.

2. Even if the CSAM-proposal is built on definitions of Directive 2011/93 on child sexual exploitation, there are differences between Member States as regards the scope of the criminalisation. This is true for instance when it comes to solicitation for which different age spans applies. It can also be assumed (quite safely) that there are differences as regards

pornographic performances, for instance for the age group 15-17 years of age, and the child pornography offence, for instance as regards the scope on non-real, but realistic depictions.

3. The very complex and detailed CSAM-proposal contains many provisions that depends on the definitions of the material scope, ranging from reporting requirements for service providers to the issuing of orders and investigative measures, measures that a Member State also can request another Member State to take. Indeed, the complexity of the proposal also makes it difficult to completely identify and fully understand all the possible cases under the Regulation that may involve content that after scrutiny is not considered illegal. In other words, there may occur cases, albeit exceptionally, that is concerned with content that is not illegal.

4. Furthermore, at the meeting of LEWP CSAM on 3 November, a number of Member States expressed support for the proposal of the Presidency to define a child user as a natural person below the age of 18 years. The EC did not object to this proposal. Consequently, the scope of the draft regulation is on its way to formally cover non-illegal or non-criminalised acts and situations.

5. For these reasons, Sweden is of the view that a clarification regarding the relation to freedom of expression and information should be included in Article 1. To that end, it seems appropriate to build on agreed language and Article 1.4 of the TCO Regulation provides such language. A clarification will help MS in the implementation and application of the Regulation to exclude cases for further action that is concerned with content that is not illegal.