Council of the European Union

Brussels, 15 March 2023
(OR. en)

7354/23

Interinstitutional File: 2022/0155(COD)

LIMITE

JAI 300
ENFOPOL 113
CRIMORG 30
IXIM 52
DATAPROTECT 66
CYBER 57
COPEN 72
FREMP 72
TELECOM 67
COMPET 194
MI 185
CONSOM 76
DIGIT 38
CODEC 358

NOTE

From:	General Secretariat of the Council
To:	Law Enforcement Working Party (Police)
No. prev. doc.:	14143/22; 6276/23; CM 1840/23
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – comments from delegations on Articles 1 to 39

Delegations will find attached the compilation of comments received from Members States on the abovementioned proposal following the meeting of the LEWP (Police) on 24 February 2023.

ANNEX

Table of Contents

CROATIA

Article 13 (1)

In points c) in addition to the term "content data" and d) in addition to the term "all available data", we suggest adding "including metadata".

It is extremely important to place a clear **obligation on accommodation service providers to provide metadata** that is part of images and video records when delivering information about the content of sexual abuse of children. In the current text, the proposed obligation is not explicitly stated. **Metadata is an important and often crucial source of information in criminal investigations**, which enables law enforcement agencies to identify victims, locations where victims are located, and identify perpetrators and the exact locations where the crime occurred. Almost all OTT Internet service providers exclude metadata when transferring images and videos via their platforms. For the stated reason, metadata would not be included in the term "all available data" and it is necessary to prescribe a clear and unambiguous obligation to collect and submit metadata.

In point f), instead of the term "associated date and time zone", which is imprecise and does not specify all the data that needs to be collected in that context, we propose the term "date and time stamp", which is also used in several places in Art. 13, 14, 17 and 18.

Article 14

We suggest deleting paragraph 2a and 2b point (b) as unnecessary. The purpose of the removal order is the need for quick and efficient removal of illegal content, thereby preventing additional victimization. The proposed new text contradicts this need.

It is also necessary to state clearly and unambiguously in the text of the Regulation that police services and national law enforcement agencies are authorized to deliver content removal orders. Therefore, we propose to add an article modelled after Art. 36. Introductory statements of the DSA Regulation.

Article 17

We ask SE PRES to further clarify the new provision in paragraph 1 point ea). From this content of the provision, it is not possible to determine the exact content of the blocking order. We suggest that the stated condition be reworded to make it clear or deleted as unnecessary.

CZECH REPUBLIC

1) With regard to Article 13 SE PRES notes that Article 18 of the DSA provides for an obligation for hosting services to report directly to national law enforcement authorities when they are aware of situations involving a threat to life or safety. Article 13 of the draft CSA Regulation provides for a broader reporting obligation through the EU Centres, including interpersonal electronic communications providers. Do Member States think that it should be explored whether and how the risk of double reporting could be avoided?

Reporting in the event of a threat to life and health directly to the LEA is the normal procedure, the filing of a criminal complaint and the initiation of an investigation into suspected criminal offences. When the provider notifies the LEA, it shall notify both the CSA and the EUC. The EUC will be able to filter not only false positive notifications, but it will also have information about the CSAM report, e.g. from several providers. It should therefore be able to combine information on a specific CSAM solution. The LEA can also combine information on the reporting of a specific material from several pages. In our view, there is no conflict between two notifications.

2) With regard to Article 14, SE PRES asks whether Member States understand equally that 'competent authority' within the meaning of Article 14 is the same as 'competent authority' within the meaning of Article 25 (given that Member States are free to designate judicial authorities and administrative authorities as their 'competent authority' under Article 25).

Yes, the competent authorities throughout the text of the Regulation can be any authority competent to implement the Regulation according to the structure of the Member State. They may also include courts or other independent administrative authorities which also perform another function under the Regulation, but also, for example, any law enforcement authorities.

3) With regard to Article 17(1)(a) SE PRES notes that a blocking order can only be issued if the object of the blockage is on the list established by the EU Centre. Do Member States consider that such a requirement should exist? Or should it be sufficient for Member States to share their blocking orders with the EU Centre and other Member States as soon as they become final?

In this case, we agreed with the original proposal – the blocking order is a significant interference with rights and an additional guarantee consisting of the requirement that the specific items are proportionate to the known CSAM. We believe that it is more important for a blocking order to be sure of accuracy than speed – with the addition of an amendment to Article 16(4)(a), the blocking order is better structured than originally, but we do not see a problem in the requirement for a well-known CSAM. The process of converting new CSAM to known CSAM should not be too time-consuming.

4) With regard to Article 18(3) SE PRES notes that this complaint mechanism only applies to blocking orders. Do Member States consider that a horizontal grievance mechanism should be explored, taking also into account Article 20 DSA?

Initially, the scope of authorised users differed for removal orders and blocking orders, if the scope were harmonised, the right to redress could be unified in one article. However, we prefer to be reluctant to introduce a horizontal complaint-handling mechanism in view of the possibility of duplicating this obligation with Article 20 of the DSA for providers of online platforms (i.e. some hosting service providers). (Article 20 of the DSA introduces an obligation to establish a mechanism with similar parameters.) At least, we recommend that any overlapping obligations under Article 20 DSA and the envisaged horizontal mechanism under CSA can be met by establishing one system meeting the criteria of both mechanisms.

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 **giving rise to a suspicion of** ~~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, **in accordance with the following sub-paragraphs** providing information on the main content of the report, ~~on the manner in which the provider has become aware of the potential child sexual abuse concerned, on the follow-up given to the report insofar as such information is available to the provider~~ and on the user's possibilities of redress, including on the right to submit complaints to the Coordinating Authority in accordance with Article 34.

Commented [U1]: CZ recommends the original text, so that the providers can add other information that is subsequently learned, to facilitate further identification.

The provider shall inform the user concerned without undue delay, either after having received a communication from the EU Centre indicating that it considers the report to be manifestly unfounded as referred to in Article 48(2), or after the expiry of a time period of **six** ~~three~~ months from the date of the report without having received a communication from the EU Centre indicating that the information is not to be provided as referred to in Article 48(6), point (a), whichever occurs first. **The time period of six months refered to in this subparagraph shall be extended by up to 6 months where so requested by the competent authority referred to in Article 48(6)**, ~~point a~~.

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

3. The provider shall establish and operate an **easy to access** ~~accessible, effective,~~ age-appropriate and user-friendly mechanism that allows users to **notify** ~~flag~~ to the provider potential online child sexual abuse on the service. **Those mechanisms shall allow for the submission of notices anonymously and exclusively by electronic means.**

4. **The mechanisms referred to in paragraph 3 ~~shall be such as to~~ may facilitate the submission of sufficiently precise and adequately substantiated notices. To that end, the providers shall take the necessary measures to enable and to facilitate the submission of notices containing all of the following elements:**

Commented [U2]: CZ: "May" gives the possibility, not obligation to report all of the listed facts.

(a) **a sufficiently substantiated explanation of the reasons why the user alleges the information in question to be online child sexual abuse;**

(b) **a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the online child sexual abuse adapted to the specific type of service.**

Article 13

Specific requirements for reporting[4]

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;

(ba) manner in which the provider became aware of the potential child sexual abuse;

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

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

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

(f) information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address **of upload, with associated date and time zone, and port number**;

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

[4] PCY comment: Article 18 DSA provides for an obligation for hosting services to report directly to national law enforcement services when they are aware of situations concerning a threat to life or security. This Article provides for a broader obligation to report via the EU Centre including also providers of interpersonal electronic communications. Do Member States think it should be explored if and how the risk for double reporting could be avoided?

2. The provider shall execute the removal order as soon as possible and in any event within 24 hours of receipt thereof. **The provider shall take the necessary measures to ensure that it is capable to reinstate the material or access thereto in accordance with Article 15(1a).**

2a. Before issuing a removal order, the issuing authority shall inform the provider, if necessary via the Coordinating Authority, of its intention to do so specifying the main elements of the content of the intended removal order and the reasons for its intention. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that authority.

2b. A removal order shall be issued where the following conditions are met:

(a) all investigations and assessments necessary have been carried out;

(b) the reasons for issuing the removal 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, including the exercise of the users' freedom of expression and information and the provider's freedom to conduct a business.

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, including the views of the provider submitted in accordance with paragraph 2a.

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

(a) identification details of the ~~competent 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 **in respect** of ~~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;~~

(da) where applicable, a statement of reasons explaining why the order is issued to a service provider that does not have its main establishment or legal representative in the Member State of the issuing authority according to the procedure provided for in Article 14a;

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

Commented [U3]: CZ: It is a new term, in our point of view it should be competent authority which is issuing the order. (new term must be specified or replaced by the competent authority according to art. 14 par. 1)

Commented [U4]: CZ would like to ask the reason for using expression "if necessary" and why to inform COOA before issuing a removal order. We understand this phrase in case of cross-border removal orders only.

Commented [U5]: CZ would like to return the par. 3a instead of the changes in par. 2 (par. 2a and 2b)

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

(fa) reporting requirements;

(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 competent~~ 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~~ **authority** 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 **shall be transmitted, if necessary via the Coordinating Authority,** to the **the provider's** 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~~ **transmit** the removal order in **any of** the **official** languages declared by the provider pursuant to Article 23(3).

The order may also be transmitted in any of the official languages of the Member State 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 any of the official languages declared by the provider in accordance with article 23(3).

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

The time period set out in paragraph ~~2~~**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 **authority issuing the order, if necessary via the** Coordinating Authority, ~~of establishment,~~ using the template set out in Annex V.

The time period set out in paragraph ~~2~~**1** shall start to run as soon as the provider has received the necessary clarification.

Commented [U6]: CZ: It will be beneficial to unify the text, we are still talking about the competent authority issuing the order.

Commented [U7]: CZ: Please explain why this procedure is used, if it is a procedure according to par. 1 4a, then 1 4a should be mentioned.

Commented [U8]: CZ recommends to return this expression to unify the text.

Commented [U9]: CZ: Please explain why this procedure is used, if it is a procedure according to par. 1 4a, then 1 4a should be mentioned.

Commented [U10]: CZ: Please explain why this procedure is used, if it is a procedure according to par. 1 4a, then 1 4a should be mentioned.

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

Commented [U11]: CZ: Please explain why this procedure is used, if it is a procedure according to par. 14a, then 14a should be mentioned.

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

Article 14a

Procedure for cross-border removal orders

1. Subject to Article 14, where the hosting service provider does not have its main establishment or legal representative in the Member State of the authority that issued the removal order, that authority shall, simultaneously, transmit, if necessary via the Coordinating Authority, a copy of the removal order to the Coordinating Authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established. If the receiving Coordinating Authority is not the competent authority, it shall transmit the order to the competent authority for the purpose of the procedure of this Article.

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

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

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

4. The Coordinating Authority or the competent authority shall, before adopting a decision pursuant to the second subparagraph of paragraph 3, inform the competent authority that issued the removal order, if necessary via the Coordinating Authority, of its intention to adopt the decision and of its reasons for doing so.

5. **Where the Coordinating Authority or the competent authority adopts a reasoned decision in accordance with paragraph 3 of this Article, it shall, without delay, transmit that decision to the authority that issued the removal order, the hosting service provider and the EU Centre, if necessary via the Coordinating Authority.**

Where the decision finds an infringement pursuant to paragraph 3 of this Article, the removal order shall cease to have legal effects.

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

Article 15

Redress and provision of information

1. Providers of hosting services that have received a removal order issued in accordance with Article 14, as well as the users who provided the material, shall have the right to an effective redress. That right shall include the right to challenge such a removal order before the courts of the Member State of the ~~competent judicial authority or independent administrative~~ authority that issued the removal order.

Commented [U12]: CZ recommends to stay with competent authority.

1a. If the order is modified or repealed as a result of a redress procedure, the provider shall ~~immediately~~without undue delay reinstate the material or access thereto or take other necessary measures.

Commented [U13]: CZ would like to unify terminology in the whole text and use: without undue delay.

2. When the removal order becomes final, the ~~competent judicial authority or independent administrative~~ authority that issued the removal order shall, without undue delay, transmit a copy thereof **and copies of the information it has received pursuant to Article 14 (5) to (7) of** to the Coordinating Authority ~~of establishment~~. The Coordinating Authority ~~of establishment~~ shall then, without undue delay, transmit ~~a copy~~ **copies** thereof to all other Coordinating Authorities **and the EU Centre** through the system established in accordance with Article 39(2).

Commented [U14]: CZ recommends to stay with competent authority.

For the purpose of the first subparagraph, a removal 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 removal order following an appeal.

3. Where a provider removes or disables access to child sexual abuse material pursuant to a removal order issued in accordance with Article 14, it shall without undue delay, inform the user who provided the material of the following:

(a) the fact that it removed the material or disabled access thereto;

(b) the reasons for the removal or disabling, providing a copy of the removal order upon the user's request;

(c) the users' rights of judicial redress referred to in paragraph 1 and to submit complaints to the Coordinating Authority in accordance with Article 34.

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

In such a case:

(a) the ~~judicial authority or independent administrative~~ authority issuing the removal order shall **inform, if necessary via the Coordinating Authority, the provider of its decision specifying the applicable time period that shall be** ~~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.~~

The issuing ~~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, **the issuing** ~~that judicial authority or independent administrative~~ authority shall inform, **if necessary via the Coordinating Authority,** the provider of its decision, specifying the applicable time period. ~~Article 14(3) shall apply to that decision.~~

Commented [U15]: CZ recommends to stay with competent authority. Return to the CZ PRES compromise text.

Commented [U16]: CZ recommends to stay with competent authority. Return to the CZ PRES compromise text.

Commented [U17]: CZ recommends to stay with competent authority in whole par. Return to the CZ PRES compromise text.

Commented [U18]: CZ: Please explain why this procedure is used, if it is a procedure according to par. 14a, then 14a should be mentioned.

Section 5
Blocking obligations

Article 16

Blocking orders

1. The **competent authority** ~~Coordinating Authority of establishment~~ shall have the power ~~to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State~~ to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing ~~known~~ child sexual abuse material 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.

Commented [U19]: CZ: Does your change in the text of the proposal mean that only know CSAM can be blocked?

1a. The provider shall execute the blocking order without undue delay or, where applicable, within the reasonable time period set by the issuing authority. The provider shall take the necessary measures to ensure that it is capable of reinstating access in accordance with Article 18(1a).

Commented [U20]: CZ prefers competent authority.

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

~~To that end, it shall, where appropriate:~~

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

~~(b) require the provider to submit, within a reasonable time period set by that Coordinating Authority, the necessary information, in particular regarding the accessing or attempting to access by users of the child sexual abuse material indicated by the uniform resource locators, regarding the provider's policy to address the risk of dissemination of the child sexual abuse material and regarding the provider's financial and technological capabilities and size;~~

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

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

2. Before issuing a blocking order, the issuing authority shall inform the provider, if necessary via the Coordinating Authority, of its intention to do so specifying the main elements of the content of the intended blocking order and the reasons for its intention. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that authority.

Commented [U21]: CZ prefers competent authority to be used in all the compromise text instead of issuing authority.

~~3. The Coordinating Authority of establishment shall, before requesting the issuance of the blocking order, inform the provider of its intention to request the issuance of the blocking order, specifying the main elements of the content of the intended blocking order and the reasons to request the blocking order. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that Coordinating authority.~~

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

(a) **other equally effective and less intrusive measures than blocking cannot be taken to prevent access to child sexual abuse material or it is likely that such measure will fail;** ~~there is evidence of the service having been used during the past 12 months, to an appreciable extent, for accessing or attempting to access child sexual abuse material indicated by the uniform resource locators;~~

(b) the blocking order is necessary to prevent the dissemination of ~~the~~ child sexual abuse material ~~to users~~ in the Union, having regard ~~in particular to the quantity and nature of the material,~~ **to** the need to protect the rights of the victims ~~and the existence and implementation by the provider of a policy to address the risk of such dissemination~~;

(c) all necessary investigations and assessments have been carried out to ensure that the uniform resource locators ~~indicate~~ **correspond,** in a sufficiently reliable manner, **to online locations where** child sexual abuse material **can be found;**

(d) the reasons for issuing the blocking 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, including the exercise of the users' freedom of expression and information and the provider's freedom to conduct a business.

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, including ~~any information obtained pursuant to paragraph 2 and~~ the views of the provider submitted in accordance with paragraph 3~~.~~

5. ~~The Coordinating Authority of establishment when requesting the issuance of blocking orders, and the competent judicial or independent administrative authority when issuing the~~ **A** blocking order~~:~~ shall:

(a) **where necessary,** specify effective and proportionate limits and safeguards necessary to ensure that any negative consequences referred to in paragraph 4, point (d), remain limited to what is strictly necessary;

(b) subject to paragraph 6, ensure that the period of application remains limited to what is strictly necessary.

6. The **issuing** ~~Coordinating~~ authority shall specify in the blocking order the period during which it applies, indicating the start date and the end date.

The period of application of blocking orders shall not exceed five years.

7. ~~In respect of the blocking orders that the competent judicial authority or independent administrative authority issued at its request, t~~**T**he Coordinating Authority ~~or the issuing authority~~ shall, where necessary and at least once every year, assess whether any substantial changes to the grounds for issuing the blocking orders **have** occurred and~~, in particular,~~ whether the conditions of paragraph 4 continue to be met.

Commented [U22]: CZ welcomes these changes and would also like to clarify the relationship to the delisting order.

Commented [U23]: CZ prefers only one authority to be obligated to assess any substantial changes.

~~The Coordinating Authority shall request to the competent judicial authority or independent administrative authority that issued the blocking order the modification or revocation of such order.~~ **W**Where necessary in the light of the outcome of that assessment or ~~to take account of justified requests or~~ **other relevant information, including information obtained through** the reports referred to in Article ~~18~~ 17(5a) ~~and (6), respectively~~ **an order shall be modified or repealed by the issuing authority, where relevant at the request of the Coordinating Authority**. ~~The provisions of this Section shall apply to such requests, *mutatis mutandis*.~~

Commented [U24]: CZ prefers to return previous compromise text.

Article 17

Additional rules regarding blocking orders

1. ~~The Coordinating Authority of establishment shall issue the~~ **A** blocking orders ~~referred to in Article 16~~ **shall be issued** using the template set out in Annex VII. Blocking orders shall include:

   (a) the reference to the list of uniform resource locators, provided by the EU Centre, and the safeguards to be provided for, including the limits and safeguards specified pursuant to Article 16(5) and, where applicable, the reporting requirements set pursuant to Article 18(6)[6];

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

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

   (d) the **child sexual abuse material and its online location** ~~specific service~~ in respect of which the **blocking** ~~detection~~ order is issued;

   (e) the start date and the end date of the blocking order;

   (ea) where applicable, the effective and proportionate limits and necessary safeguards;

[6] PCY comment: PCY observes that the proposal means that a blocking order can only be issued if the subject-matter of the blocking is on the list provided for by the EU Centre. Do Member Sates think that there should be such a requirement? Or should it be sufficient that Member States share their blocking orders with the EU Centre and other Member States once they become final?

(f) a sufficiently detailed statement of reasons explaining why the blocking order is issued;

(fa) where applicable, reporting requirements;

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

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

(i) easily understandable information about the redress available to the addressee of the blocking 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 blocking order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

3. The blocking order shall be transmitted, **if necessary via the Coordinating Authority,** to the provider's 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).

4. The blocking order shall be ~~drafted~~ **transmitted** in **any of** the **official** languages declared by the provider pursuant to Article 23(3).

The order may also be transmitted in any of the official languages of the Member State 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 any of the official languages declared by the provider in accordance with article 23(3).

4a. If the provider cannot execute the blocking 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 authority issuing the order, if necessary via the Coordinating Authority of those grounds, using the template set out in Annex yy.

5. If the provider cannot execute the blocking 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 **authority issuing the order** ~~Coordinating Authority of establishment~~, **if necessary via the Coordinating Authority,** using the template set out in Annex VIII.

Commented [U25]: CZ prefers to unify the term: competent authority. CZ would like to come back to CZ PRES compromise text in all the par. regarding the competent authority.

Commented [U26]: CZ: Please explain why this procedure is used, if it is a procedure according to par. 14a, then 14a should be mentioned. (in all the par.)

DENMARK

General remarks

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

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

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

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

Voluntary agreements to continue alongside the Regulation

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

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

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

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

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

Article 12

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

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

Article 14 and 14 a

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

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

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

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

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

Article 15

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

GERMANY

General remarks

- Combating the sexual abuse of children and young people has the highest priority for Germany's Federal Government. That is why the Federal Government has welcomed the Commission's proposal from the start as a shared European project which will create a clear and lasting legal basis. Establishing a single European regulatory framework with effective reporting channels and a new, independent and decentralised agency (EU Centre on Child Sexual Abuse) are crucial steps in the fight against the sexual abuse of children. As part of this effort, it is important to make the providers of relevant information society services more accountable.

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

- This means that the draft text must be **revised** before Germany can accept it.

  We will submit these and other specific requests for revisions soon. The Federal Government will continue to contribute actively and constructively to the negotiations on the CSA Regulation.

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

Examination of Presidency compromise proposals – 6276/23

- We thank the Presidency for drafting the new compromise texts.

- Unfortunately, the proposed wording we submitted for Article 2 has not yet been adopted. This is specifically in connection with the scope given in the CSA Regulation for Member States to make decisions concerning the age of sexual consent and whether certain conduct and content is punishable. We also see considerable need for amendments to Article 7. We therefore suggest that these points be addressed at a separate meeting of the Working Party.

Article 12:

- We welcome the adoption in paragraph 1 of the wording used in Article 15a (1) of the DSA.

- Paragraph 2: Reports pursuant to Articles 12 and 13 should also state how the provider became aware of a potential CSAM report on its services. We are open to the addition of this requirement in Article 13 (1) (ba).

  However, we would ask the Presidency to explain why the users concerned – especially in view of their possibilities of redress – should not be informed about "the manner in which the provider has become aware of the potential child sex abuse" and why information "on the follow-up given to the report insofar as such information is available to the provider" should no longer be contained in the report.

- Paragraphs 3 and 4: Could the Presidency please explain how anonymous user notices would work in practical terms?

Article 13:

- From the point of view of national law enforcement authorities, double reporting must be avoided in view of the high volume of reporting expected. In any case, there needs to be an automated deconflicting process. Germany would therefore be pleased if the risk of double reporting could be reduced (in line with the CSA and DSA).

- Please explain the deletions in Article 13 (1) (c) and (d). As we have already explained, from the point of view of the competent authorities, it is important to have access to all available information in order to pursue potential avenues of investigation and ensure effective law enforcement.

- Regarding Article 13 (ba): From our point of view, the term "manner" is unclear, as it might refer to the channel or the source of information. We would be grateful if the Presidency could explain this.

Article 14:

- We are pleased that the clarification in paragraph 2 sentence 2 has been adopted in the compromise text.

- Article 14 (2b) and (3): For greater linguistic clarity and easier practical application, we propose that the subject be clearly named: "The (competent) authority shall issue a removal order / The competent authority issuing a removal order shall use the template set out in Annex IV".

- Would the Presidency please explain the additional paragraphs 2a and 2b?

- Regarding paragraph 2b: Which investigations are being referred to? Who is to conduct the investigations and with what (technical) resources?

- As we understand, paragraph 2b only applies if the provider does not remove the content despite having received information in accordance with paragraph 2a. This condition should be clarified in the text of the Regulation – with appropriate time limits specified as required.

- Regarding Article 14 (3) (fa), we would like an explanation and/or addition clarifying what is meant by "reporting requirements" (who reports what to whom?).

- Regarding removal orders, once the competent national authorities have reached a decision with respect to Article 14 (2b), it would be desirable to have a procedure (preferably automated) for communication between competent national authorities and providers when issuing removal orders (in accordance with paragraph 3 in conjunction with Annex IV) and to refer to this procedure in the Regulation.

- As we understand, providers must fulfil their removal/blocking obligations (see Articles 14 and 16) without the use of detection technologies.

Article 15:

- We maintain our scrutiny reservation, especially with regard to the time period specified in Article 15 (4) (a).

Articles 16 and 17:

- We are still sceptical overall regarding the amendments in Articles 16 and 17 because the removal of child sexual abuse material (CSAM) is in our view the most effective and therefore the most preferable measure to stop the spread of CSAM.

- It is therefore important to amend the requirements for issuing blocking orders in Article 16 (4), in particular with regard to weighing the reasons for issuing the blocking order against the negative consequences for the rights and legitimate interests of all parties affected (paragraph (4) (d)). For reasons of proportionality, the text deleted in Article 16 (4) (a) should be restored. We believe that careful weighing-up is necessary in the individual case, particularly in view of the dangers and disadvantages of blocking orders.

- Issuing blocking orders to internet access providers should be allowed as a subsidiary option only if action against the responsible party (located outside of the EU) cannot be taken or would likely fail; if blocking is technically feasible and reasonable; if this does not entail monitoring obligations; and if any HTTPS encryption is respected. For this reason, we object in particular to the deletion of Article 16 (2) (a). (This deletion was already made in 14143/22).

- Could the Presidency please explain the amendments in Articles 17 and 18?

- We welcome the consideration of bringing the text, especially regarding complaint mechanisms, more closely in line with the DSA (Article 20 DSA).

- For greater linguistic clarity, we refer to our comments on Article 14 (2b) and (3) and suggest that the subject be clearly named.

Article 18a:

- If it is not possible to remove CSAM, de-listing can be another suitable option. We believe that joint action at European level would be very helpful, especially in view of the desire for a single regulatory framework, and that it would significantly increase the effectiveness of de-listing. However, we believe de-listing should only be allowed as a subsidiary measure. In other respects too, the requirements given in Article 18a (4) should be further specified, due to the infringement of operators' and users' rights that is associated with de-listing.

- Since de-listing was not part of the Commission's proposal, and therefore not part of the Commission's impact assessment, we suggest asking the the Commission for its appraisal.

- In connection with the discussion of Chapter II, we would also like to address the annexes to the draft Regulation. Given the high volume of reporting expected, the forms referred to in the annex should support the automated processing of reports. Free text fields in the forms should be avoided. The forms should instead contain lists, predetermined values and defined choices, thus facilitating completion and further processing.

- We assume that even after the establishment of the EU Centre, the U.S. organisation NCMEC will remain a key source of reporting to the Centre and/or to Member States. We are therefore in favour of basing the format of the EU Centre's reporting forms on that of the NCMEC's forms. These forms have been used successfully for many years in an international context.

  We would be happy to propose specific amendments to this effect.

- We also refer to our previous comments on Article 2 and Articles 12–18c.

Examination of the proposal as of Article 19 – 14143/22

Articles 25 and 26:

- The way the Coordinating Authority is organised is extremely important to Germany and other Member States. We would therefore like to emphasise once again that the Coordinating Authority must be able to perform its tasks independently. For this reason, we have already called for bringing the CSA Regulation into line with the requirements of the TCO Regulation.

  In any case, we think that Article 25 (9) should clarify that other competent authorities taking over tasks from the Coordinating Authority must carry out these specific tasks independently and without seeking nor taking instructions. This is necessary in particular because law enforcement authorities should continue to be able to carry out evidence processing tasks and to take on tasks related to removal orders.

Article 25 (9) should therefore read as follows:

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

- We understand Article 25 (9) as permitting individual tasks (and not all the powers referred to in Articles 26–31) to be delegated to other authorities.

- The transitional period given in Article 25 (1) should be appropriate for implementation in national law. We therefore believe the period should be one year.

- As for the rest, we stand by our previous comments, most recently from the LEWP meeting on 24 November 2022.

ESTONIA

As we also raised at the last LEWP meeting, there are two principial problem areas:

The first and the more fundamental issue concerns data retention. Several Member States have raised some questions with data retention, mainly Articles 13 and 22. The current version focuses on data retention which applies only after discovering the criminal content. In reality, however, it is often necessary to react later, which means that in order to investigate the crime, it is necessary to obtain data which has been created long before the criminal content has been discovered at all. Including metadata. For example, with the child sexual abuse material, if the service provider starts retaining the data let's say 24 hours or even a week after the material has been posted (at the moment when it's discovered) then there is no data to pinpoint the person who published it. It is already too late. This is what the current regulation does not seem to take into account. This is a much broader problem that would require a solution which is not necessarily field- or sector-specific, but would then apply to all concerned regulations as an umbrella act. We have also submitted proposals in this regard in the COSI format so that the proposed HLEG working group could start take it into account.

Secondly, the issue also brought up at the LEWP meeting on Feb 24th is about the principles of the coordinating and competent authorities. As already handled in the TCO regulation discussions, it is not realistic to state that the coordinating or competent authority is fully independent. Every institution is subordinate to some other. In the very last case, all institutions are subordinate to the government, and the budgeting of all institutions is also done from the state budget. We should take the wording of the TCO regulation as a basis as it is the result of the same discussions. The recitals of the TCO Regulation state that Member States should remain free to choose the competent authorities, allowing them to appoint administrative, law enforcement or judicial authorities to perform this task. Article 12 of TCO Act states that Member States shall ensure that their competent authorities have the necessary capability and sufficient resources to achieve the aims and fulfil their obligations under TCO regulation. Since the coordinating authority can also be a competent authority according to the CSAM proposal, there is no reason to set different rules from the ones set to TCO competent authority.

Article comments:

- Art 2 (x) 'online search engine' – art 3 i. **which one? There is no (i) is Art 3. Also should we specify the name of the online search engine?**
- Art 12 (3) *The provider shall establish and operate an easy to access accessible, effective, age appropriate and user-friendly mechanism that allows users to notify flag to the provider potential online child sexual abuse on the service. Those mechanisms shall allow for the submission of notices anonymously and exclusively by electronic means.* **What are the user-friendly mechanism referred to? Age appropriate?**
- Art 13 –The competent authority- who will it be?
    - (13) h – to which authority in the third country?

- Art 14 (2) – we find 24 hours to be too long.
    - Art 14 a 6 - The procedure for a cross-border removal order - **how to restore content?**
- Art 15 (1) - If the order is modified or repealed as a result of a redress procedure, the provider shall immediately reinstate the material or access thereto or take other necessary measures. **Which kind of necessary measures?**
- Art 16 (3) – a reasonable time period set by that authority - **what is a reasonable time?**
- Art 17 (a) a blocking order can only be issued if the object of the blocking is on the list provided by the EU Centre? What happens if it is outside the EU?
- Art 18 (a) – what in this case is considered as a reasonable measure?
- Art 22 (2) Service providers shall keep the information referred to in (1) for no longer than is necessary for the applicable purpose and in any case for no longer than 12 months from the date of reporting or the date of removal or denial of access, whichever occurs first. **Is 12 months perhaps too long?**
- Art 25 (4) **one week isn't enough.**
- Art 26 **Estonia does not support the established requirements concerning the creation of a separate new Coordinating Authority in each Member State and the complete administrative independence of that authority.**
- Art 29 (2) (b) - **Detection, restraint and blocking - does the coordinating authority need to be able to negotiate with the provider; can the provider voluntarily implement some of it?**

<u>Comments and questions from the Prosecutor's Office:</u>

- A removal order and a blocking order will certainly need to be regulated at national level - who, how? Same for "Delisting orders" - i.e. search exclusion?
- Art 15 too, of course. The six-week time limit (Art 15 § 4(a)) and its extension by 6 weeks may not be sufficient to bring the procedure to the stage where it can go public under national law. This requires very good coordination with the central authority so that information is not delayed. And a very good readiness to deal with the matter immediately at national level. Translation takes time. Could it be 8 weeks?

A walkthrough of a specific case to illustrate Art 15:

- *Information is received that an Estonian host or a user in an accommodation service in Estonia is handling CSAM. (how soon, will become clear when the system is started).*

- *You have to make an assessment of how serious it is, whether it needs an immediate full-scale response, or whether you can start to ram it through a bit by bit - a couple of hours if you have time.*

- *An investigator (a team) must be found who can get down to work immediately. Timeframe difficult to quantify, probably possible within a day.*

- *We need to start identifying who he is. Making enquiries, analysing information - hard to predict, but probably a couple of days. Possibly need to do surveillance to identify the person.*

- *For the court, the materials have to be translated (the PPA knows how long the queues are for quick translations, even into English).*

- *At least two working days to give/receive authorisation for surveillance. One for the prosecutor to examine the material and write a reasoned request, the other for the court to examine the material and write a reasoned order. In Estonia, there is an insanely high substantive standard to even apply for or be granted a warrant to conduct surveillance. The reasons why evidence cannot be obtained by other means must be explained so that the ultima ratio of the measure is clear, sufficient and comprehensible to all higher courts.*

Even in the best of cases, a week or more has gone by.

- *The authorisation for surveillance can be granted for two months at a time, which is essential. Because not all surveillance operations can be carried out immediately. I have had a case where the preparatory activities necessary for the gathering of evidence, which may also only be carried out with the authorisation of the court and are in the nature of intelligence activities, have lasted 5 weeks.*

- *It can take weeks to obtain conclusive evidence/identify the person/associate with CSAM.*

It is too much of a hassle and too risky to deal with 6 weeks of extensions in parallel, hoping that the information will reach the provider in time.

- The reference to "paragraph 7 of this Article" in Art 14a 2 was confusing, because in the version of Art 14a available there were only 6 paragraphs. Since there is also a reference to Article 14, the reference is probably to paragraph 7 of Article 14. Maybe instead "paragraph 7 of this Article" "paragraph 7 of Article 14". Or is this reference unambiguous for others.

- Normative confusion 14a § 6, which refers to § 6. Which Article § 6?

- The last paragraph of Art 16(4) refers to paragraph 3 "in accordance with paragraph 3", but in Article 16, paragraph 3 has been deleted entirely. The so-called hearing or disclosure of the provider's position is in § 2.

- Art 23 and Art 24 Points of contact and legal representative:

  What if providers obey these requirements? Or the fulfilment of the requirement has been formal and no one respond, we can't actually forward the information. We must create measures to compel providers to comply with these requirements. For example threat of punishment, allow to offer services only if obligations are fulfilled: provider have been designate legal representative and established contact point.

Estonian Police and Border Guard

- Art 13, (4) — if there is a threat to life or safety, the first recipient should be the LEA and cc: to the EU Centre

  This article has relation with Digital Service Act Article 18. Notification of suspicions of criminal offences (1) Where a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available).

- Art 13 Subsection 1(c) - what data are considered to be content data in accordance with this paragraph?

  Given that, according to Article 2 (l), the concept of CSAM also includes live performance directed at the audience, including the performance by means of information and communication technology, i.e. Dir 2011/93, Article 2(e), as well as the same Dir Article 6 referred to in (o) and (q), it is clear that Article 13(1)(c) — content data should include videos, images, text and sound.

- Art 14(2) - must provide nationally for the provider to have the capacity to respond (remove) within 24 hours.

- Art 14(2a) - to set up a national process for how the coordinating authority interacts with service providers.

- The last subparagraph of Art 14(2b) is redundant, repeating the previous one. It is not clear what is meant.

- Art 14(3) da - Can we give an order to a service provider established in a third country? You should contact the law enforcement authority of that country. We can block CSAM content within the EU but not in a non-EU country.

- Art 14(4) - the preferred language would be English as the EU's number 1 working language.

- Art 15(1a) - what becomes of erotic material, this should be worded more precisely as it is prohibited in Estonia to depict a child in an erotic situation.

- Art 15(4) - the Regulation consistently talks about time limits in terms of months, here weeks, which is confusing. Would it be more appropriate to set the time limit at 2 months?

- Art 16(1a) - uses the undefined legal term "reasonable time". The time limit must be specific.

- Art 16(1) - could remain the Commission text. If the identification of new material is also moved to resource indicators, how can new material be identified at all? Could there be a risk of blocking new material in the Parliament's proposal? In any case, does the identification of new material have to be accompanied by a resource blocker? If only child pornography is included in the locator database, what about erotic material?

- Art 16(2) - uses the undefined legal concept of reasonable time. This could be explained at the beginning of the Regulation.

- Art 16(4b) - The service provider must have in place general requirements for risk reduction and detection. Where and if so how are these set out? If they were laid down, there would be no need to set them out in the Articles. The foregoing is supported by point (c).

- Art 17(1a) - Blocking orders could be made available to the coordinating authorities of each EU country through a data exchange platform (perhaps in the form of a table). It is too resource-intensive to ask the EU centre for information on URL blocking.

- Art 17(1) fa - what is the need for reporting requirements to be reflected in the blocking order?

- In Article 18a (3) - what does "*reasonable time period*" mean? and within same article 18a (4)(b) — what is meant by the expression "*in a sufficiently reliable manner*"?

In conclusion, minors portrayed in erotic situations are a danger point. If we do not agree on criteria in our own country, there could be a lot of litigation and burdens on the courts.

Enforcement of injunctions in general - while service providers exercise their right to review and challenge an injunction, is the content still available for prohibited consumption? This will result in a commercial benefit for the service provider from the illegal activity (distribution of prohibited content). Access to the prohibited content must be restricted from the moment the order is issued. It is in our interest that commercial interests do not override the rights of the child.

Is an injunction a new concept in Estonian law, is it the same as an injunction?

FINLAND

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* ***giving rise to a suspicion of*** ~~*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,* ***in accordance with the following sub-paragraphs*** *providing information on the main content of the report*~~*, on the manner in which the provider has become aware of the potential child sexual abuse concerned, on the follow-up given to the report insofar as such information is available to the provider*~~ *and on the user's possibilities of redress, including on the right to submit complaints to the Coordinating Authority in accordance with Article 34.*

Is Article 12(2) about the informer or the user whose material is reported to the Centre - and does it apply to both the suspect and the victim? We have previously submitted a written comment on the ambiguity of paragraph 2 in relation to the right of data subjects under data protection law to be informed of the processing of personal data concerning them, including disclosures of personal data. The data protection legislation allows for a postponement of the provision of information, e.g. to secure a preliminary investigation at the request of the police, but it remains unclear here how the paragraph would interact with it.

FI's previous comment on this topic

The relationship between Article 12 and the data protection legislation should be clarified. We draw attention in particular to the reporting obligation in Article 12, paragraph 2. It is unclear what the relationship of this paragraph is with the requirements imposed on the controller under the GDPR to inform the data subject of recipients of personal data. It is further unclear how the reporting obligation would work together with the provisions of Directive (EU) 2016/680 (LED) that apply to the competent authorities, particularly Articles 14 and 15 thereof, as implemented by the Member States. Those Articles concern the right of access of the data subjects and the limitations on that right.

For the time being, we maintain a scrutiny reservation on the appropriate time limits for the reason that the relationship with LED is unclear. LED only applies to the competent authorities, whereas the provisions of the GDPR would apply to the service providers.

It is important that Article 12 take into account both the interests of investigation and the interests of the data subjects, including those of child victims.

We will be happy to propose drafting that takes into account those interests, once we have a clarification from the Commission on the relationship between Article 12, paragraph 2, and the provisions on the right of access of the data subject and the limitations on that right under the data protection legislation. In particular, is Article 12, paragraph 2, meant to adapt the provisions of the GDPR and LED concerning the right of access of the data subject?

Article 14

Removal orders

2. The provider shall execute the removal order as soon as possible and in any event within 24 hours of receipt thereof. ***The provider shall take the necessary measures to ensure that it is capable to reinstate the material or access thereto in accordance with Article 15(1a).***

2a. Before issuing a removal order, the issuing authority shall inform the provider, if necessary via the Coordinating Authority, of its intention to do so specifying the main elements of the content of the intended removal order and the reasons for its intention. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that authority.

On a general level, Finland believes that Article 14 is a step in the right direction, however, we do not believe that Article 14(2) is workable. The proposed addition would mean that the service provider would have to store the material somewhere in order to be able to do this. Isn't this problematic when it comes to CSA material?

Could the new provisions in Article 14(2a) lead to additional requirements for authorities to tackle illegal content, thus affecting the speed and effectiveness of the enforcement effort? If the material has already been identified as illegal CSA material by a public authority decision, why ask for the provider's opinion in the removal order. The same comment applies to the subsequent Article 14(2bb) and fundamental rights considerations. If it is criminalised content, it does not enjoy the protection of freedom of expression. It would also be useful to clarify the relationship of this Article to Article 3 of the TCO Regulation.

Section 5
Blocking obligations

Article 16

Blocking orders

*1. The **competent authority** ~~Coordinating Authority of establishment~~ shall have the power ~~to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State~~ to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing ~~known~~ child sexual abuse material 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.*

General comment:

Experts from the our National Cyber Security Centre and stakeholders in Finland have raised technical problems in implementing URL-based blocking in practice. In particular, the effectiveness of the measures has been questioned, as most of the network traffic is now HTTPS-encrypted. Has the COM considered other possible ways of implementing blocking orders?

Regarding article 16 (1)

What is the reason and meaning of the deletion of the word known? This has previously been the limitation here, but have the content of the article now significantly extended? Can blocking orders be placed on the site to prevent access to "potential" CSAM material (not yet known) or how should the rest of the section be interpreted. In other words, is it now unclear to what extent it has been identified that CSAM material is present on the site before blocking access to it? This measure is significant, for example in terms of freedom of expression, if it is used to block access to a particular site altogether.

In this respect, it should be noted that the CSA draft regulation includes the word "potential" in the concept of CSAM, i.e. measures to find potential (not yet identified) data. It is good in itself that Article 16 has built in application thresholds, but it would be useful to clarify the above-mentioned issue. As such, the measure may be justified to protect children and various blocking provisions are contained in different laws, but the rationale and meaning of the deletion of the word "known" is now unclear.

Article 17

Additional rules regarding blocking orders

1. ~~*The Coordinating Authority of establishment shall issue the*~~ ***A*** *blocking* ~~*orders referred to in Article 16*~~ ***shall be issued*** *using the template set out in Annex VII. Blocking orders shall include:*

(ea) where applicable, the effective and proportionate limits and necessary safeguards;

What are the necessary safeguards in the new (ea) section; are they to be opened up in the text or perhaps in the recitals?

HUNGARY

Comments on doc. 6276/23

Section 2
Detection obligations

Article 7

Issuance of detection orders

Commented [GYM1]: If the terms competent authorities/issuing authorities/Coordinating Authorities are to be used as proposed in case of the rules of removal orders, blocking orders and delisting orders, the same terms should be applied to detection orders as well.

[...]

[No new compromise texts in this Article]

Article 8

Additional rules regarding detection orders

[...]

[No new compromise texts in this Article]

Article 9

Redress, information, reporting and modification of detection orders

[...]

[No new compromise texts in this Article]

Article 10

Technologies and safeguards

[...]

[No new compromise texts in this Article]

Article 11

Guidelines regarding detection obligations

[...]

[No new compromise texts in this Article]

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 **giving rise to a suspicion of** ~~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).

Commented [GYM2]: We would prefer the previous term as this requirement may be too strict with regard to the fact that service providers are expected to apply it. (Usually it is up to criminal authorities to consider what may give rise to a suspicion.)

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

The provider shall inform the user concerned without undue delay, either after having received a communication from the EU Centre indicating that it considers the report to be manifestly unfounded as referred to in Article 48(2), or after the expiry of a time period of **six** ~~three~~ months from the date of the report without having received a communication from the EU Centre indicating that the information is not to be provided as referred to in Article 48(6), point (a), whichever occurs first. **The time period of six months refered to in this subparagraph shall be extended by up to 6 months where so requested by the competent authority referred to in Article 48(6)**~~, point a~~**.**

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

3. The provider shall establish and operate an **easy to access** ~~accessible, effective,~~ age-appropriate and user-friendly mechanism that allows users to **notify** ~~flag~~ to the provider potential online child sexual abuse on the service. **Those mechanisms shall allow for the submission of notices anonymously and exclusively by electronic means.**

4. **The mechanisms referred to in paragraph 3 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices. To that end, the providers shall take the necessary measures to enable and to facilitate the submission of notices containing all of the following elements:**

(a) **a sufficiently substantiated explanation of the reasons why the user alleges the information in question to be online child sexual abuse;**

(b) **a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the online child sexual abuse adapted to the specific type of service.**

Commented [GYM3]: We agree to introduce minimum requirements regarding users' notices, but the procedure needs to be simplified and made more user-friendly.

Article 13

Specific requirements for reporting[4]

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;

(ba) manner in which the provider became aware of the potential child sexual abuse, with special regard to the source of information (from the victim, from another person, as a result of technological detection or from other organisation or authority);

Commented [TZ4]: Identifying the source of the information may significantly support to establishing the likelihood of the abuse.

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

Commented [GYM5]: We thank PRES for amending the text according to our comment.

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

Commented [GYM6]: We would prefer the earlier wording, it provides more clarity when interpreted together with the amended point (c).

Commented [TZ7]: Meta data could be a significant contribution to clarifying the circumstances of the crime and identifying the victim and the perpetrator.

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

(f) information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address **of upload, with associated date and time zone,** time stamp **and port number**;

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

[4] PCY comment: Article 18 DSA provides for an obligation for hosting services to report directly to national law enforcement services when they are aware of situations concerning a threat to life or security. This Article provides for a broader obligation to report via the EU Centre including also providers of interpersonal electronic communications. Do Member States think it should be explored if and how the risk for double reporting could be avoided?

2. The provider shall execute the removal order as soon as possible and in any event within ~~one 24~~ hours of receipt thereof. **The provider shall take the necessary measures to ensure that it is capable to reinstate the material or access thereto in accordance with Article 15(1a).**

2a. ~~**Before issuing a removal order, the issuing authority shall inform the provider, if necessary via the Coordinating Authority, of its intention to do so specifying the main elements of the content of the intended removal order and the reasons for its intention. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that authority.**~~

2b. A removal order shall be issued where the following conditions are met:

(a) all investigations and assessments necessary have been carried out;

(b) the reasons for issuing the removal 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, including the exercise of the users' freedom of expression and information and the provider's freedom to conduct a business.

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, including the views of the provider submitted in accordance with paragraph 2a.

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

(a) identification details of the ~~**competent 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 **in respect** of ~~**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;**~~

(da) where applicable, a statement of reasons explaining why the order is issued to a service provider that does not have its main establishment or legal representative in the Member State of the issuing authority according to the procedure provided for in Article 14a;

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

Commented [TZ8]: It is proposed in accordance with the TCO Regulation in force.

Commented [TZ9]: It is proposed to delete. We do not see the justification for a prior notification procedure, as removal orders are sent to service providers by an authority with the appropriate competence, in a prescribed format and with a statement of reasons. In our view, this additional step in the removal process does not provide any substantive additional safeguards against erroneous removal, but only makes the process more complex and lengthy.

Commented [GYM10]: We support this additional point.

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

In such a case:

(a) the ~~judicial authority or independent administrative~~ authority issuing the removal order shall **inform, if necessary via the Coordinating Authority, the provider of its decision specifying the applicable time period that shall be** ~~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.~~

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

Commented [TZ11]: Under Article 16(1), the competent authority may order the blocking of all URLs on the EU Centre's list. As the list is likely to include URLs of content accessible via an encrypted protocol (HTTPS), which could only be achieved by blocking the entire domain included in the URL, together with a number of other potentially lawful content, it is proposed that it should not only be possible to block the entire list, but also a part of it that is not accessible via an encrypted protocol (HTTPS).

1a. The provider shall execute the blocking order without undue delay or, where applicable, within the reasonable time period set by the issuing authority. The provider shall take the necessary measures to ensure that it is capable of reinstating access in accordance with Article 18(1a).

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

~~To that end, it shall, where appropriate:~~

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

~~(b) require the provider to submit, within a reasonable time period set by that Coordinating Authority, the necessary information, in particular regarding the accessing or attempting to access by users of the child sexual abuse material indicated by the uniform resource locators, regarding the provider's policy to address the risk of dissemination of the child sexual abuse material and regarding the provider's financial and technological capabilities and size;~~

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

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

~~2. Before issuing a blocking order, the issuing authority shall inform the provider, if necessary via the Coordinating Authority, of its intention to do so specifying the main elements of the content of the intended blocking order and the reasons for its intention. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that authority.~~

Commented [TZ12]: It is proposed to delete. We do not see the justification for a prior notification procedure, as removal orders are sent to service providers by an authority with the appropriate competence, in a prescribed format and with a statement of reasons. In our view, this additional step in the removal process does not provide any substantive additional safeguards against erroneous removal, but only makes the process more complex and lengthy.

~~3. The Coordinating Authority of establishment shall, before requesting the issuance of the blocking order, inform the provider of its intention to request the issuance of the blocking order, specifying the main elements of the content of the intended blocking order and the reasons to request the blocking order. It shall afford the provider an opportunity to comment on that information, within a reasonable time period set by that Coordinating authority.~~

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

(a) **other equally effective and less intrusive measures than blocking cannot be taken to prevent access to child sexual abuse material or it is likely that such measure will fail;** ~~there is evidence of the service having been used during the past 12 months, to an appreciable extent, for accessing or attempting to access child sexual abuse material indicated by the uniform resource locators;~~

(b) the blocking order is necessary to prevent the dissemination of ~~the~~ child sexual abuse material ~~to users~~ in the Union, having regard ~~in particular to the quantity and nature of the material,~~ **to** the need to protect the rights of the victims ~~and the existence and implementation by the provider of a policy to address the risk of such dissemination~~;

(c) all necessary investigations and assessments have been carried out to ensure that the uniform resource locators ~~indicate~~ **correspond,** in a sufficiently reliable manner, **to online locations where** child sexual abuse material **can be found;**

(d) the reasons for issuing the blocking 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, including the exercise of the users' freedom of expression and information and the provider's freedom to conduct a business.

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, including ~~any information obtained pursuant to paragraph 2 and~~ the views of the provider submitted in accordance with paragraph 3~~.~~

5. ~~The Coordinating Authority of establishment when requesting the issuance of blocking orders, and the competent judicial or independent administrative authority when issuing the~~ **A** blocking order~~:~~ shall:

(a) **where necessary,** specify effective and proportionate limits and safeguards necessary to ensure that any negative consequences referred to in paragraph 4, point (d), remain limited to what is strictly necessary;

(b) subject to paragraph 6, ensure that the period of application remains limited to what is strictly necessary.

6. The **issuing** ~~Coordinating~~ authority shall specify in the blocking order the period during which it applies, indicating the start date and the end date.

The period of application of blocking orders shall not exceed five years.

7. ~~In respect of the blocking orders that the competent judicial authority or independent administrative authority issued at its request, t~~**The** Coordinating Authority **or the issuing authority** shall, where necessary and at least once every year, assess whether any substantial changes to the grounds for issuing the blocking orders **have** occurred and~~, in particular,~~ whether the conditions of paragraph 4 continue to be met.

Commented [TZ13]: The content of the "less intrusive measures than blocking" referred to in the paragraph should be clarified, at least by way of example, since if the hosting provider does not remove CSAM content, it is questionable what effective method - other than blocking in the internet service provider's network - is sufficiently effective and yet less intrusive.

(f) a sufficiently detailed statement of reasons explaining why the blocking order is issued;

(fa) where applicable, reporting requirements;

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

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

(i) easily understandable information about the redress available to the addressee of the blocking 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 blocking order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

3. The blocking order shall be transmitted, **if necessary via the Coordinating Authority,** to the provider's 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).

4. The blocking order shall be ~~drafted~~ **transmitted** in **any of** the **official** languages declared by the provider pursuant to Article 23(3).

The order may also be transmitted in any of the official languages of the Member State 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 any of the official languages declared by the provider in accordance with article 23(3).

~~**4a. If the provider cannot execute the blocking 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 authority issuing the order, if necessary via the Coordinating Authority of those grounds, using the template set out in Annex xx.**~~

Commented [TZ14]: It is proposed to delete. The exemption given in this point may give service providers too broad a basis for refusing to implement, in particular because of technical problems and organisational inefficiencies.

5. If the provider cannot execute the blocking 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 **authority issuing the order** ~~Coordinating Authority of establishment~~, **if necessary via the Coordinating Authority,** using the template set out in Annex VIII.

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 [TZ1]: If the terms competent authorities/issuing authorities/Coordinating Authorities are to be used as proposed in case of the rules of removal orders, blocking orders and delisting orders, the same terms should be applied to detection orders as well.

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.

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;

   (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 set by that Coordinating Authority;

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

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

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

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

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

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

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

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

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

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

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

Commented [TZ2]: We suggest to keep the original text, the new proposal makes be the regulation circumventable.

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

Article 13

Specific requirements for reporting

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

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

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

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

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

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

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

(f) information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address **of upload, with associated date and time zone,** time stamp **and port number**;

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

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

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

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

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

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

Commented [TZ3]: Identifying the source of the information may significantly support to establishing the likelihood of the abuse.

Commented [TZ4]: It is proposed to delete this section as it may lead to misunderstandings in the application of the Regulation. With the deletion, the definition of "content data" would be used by Article 2(s).

Commented [TZ5]: Meta data could be a significant contribution to clarifying the circumstances of the crime and identifying the victim and the perpetrator.

Section 4
Removal obligations

Article 14

Removal orders

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

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

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

Commented [TZ6]: It is proposed in accordance with the TCO Regulation in force.

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 **competent** ~~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;

Section 5
Blocking obligations

Article 16

Blocking orders

1. The **competent authority** ~~Coordinating Authority of establishment~~ shall have the power ~~to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State~~ to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing ~~known~~ child sexual abuse material.

The competent authority shall also have the power to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing known child sexual abuse material indicated by ~~all~~ uniform resource locators with an unencrypted URI scheme on the list of uniform resource locators included in the database of indicators, in accordance with Article 44(2), point (b) and provided by the EU Centre.

Commented [TZ7]: Under Article 16(1)(2), the designated authority may order the blocking of all URLs on the EU Centre's list. As the list is likely to include URLs of content accessible via an encrypted protocol (HTTPS), which could only be achieved by blocking the entire domain included in the URL, together with a number of other potentially lawful content, it is proposed that it should not only be possible to block the entire list, but also a part of it that is not accessible via an encrypted protocol (HTTPS).

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

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

~~To that end, it shall, where appropriate:~~

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

~~(b) require the provider to submit, within a reasonable time period set by that Coordinating Authority, the necessary information, in particular regarding the accessing or attempting to access by users of the child sexual abuse material indicated by the uniform resource locators, regarding the provider's policy to address the risk of dissemination of the child sexual abuse material and regarding the provider's financial and technological capabilities and size;~~

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

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

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

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

Article 26

Requirements for Coordinating Authorities

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

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

Commented [KSAd8]: The coordinating authority is likely to be a body funded from the state budget, so we would like to avoid any text that would give the opportunity to question its independence on this basis.

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

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

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

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

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

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

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

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

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

Section 2
Powers of Coordinating Authorities

Article 27

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

Commented [KSAd9]: These are not investigative powers in the classical sense, but rather administrative procedure. In our view, the current wording is not acceptable, even though the DSA regualtion contains this wording, as the DSA is not a law enforcement source of law.

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

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

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

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

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

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

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

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

Article 37

Cross-border cooperation among Coordinating Authorities

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

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

   Commented [KSAd10]: What is the legal basis and information that allows the Commission to come to such a conclusion, and where is the background to this in this draft?

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

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

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

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

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

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

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

Article 38

Joint inspections~~investigations~~

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

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

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

Article 39

General cooperation and information-sharing system

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

IRELAND

Compromise Text 6276/23 (Article 1 to Article 18c), issued 16 Feb 2023

Article 12 Reporting obligations

We seek clarification that the provisions set out in 48(7), which relate to 48(6), allows for an LEA to request a maximum of 18 months for non-notification by the service provider to the content provider.

Ireland supports the provision in Article 12(3). We know that making reporting easier can make a real difference. And that it can benefit from co-design with stakeholders, including children. However, the requirements as set out in 12(4), and in particular 12(4) (b) do not appear to be user friendly, let alone child friendly. Therefore as previously requested, can we be more prescriptive here, perhaps by including a process to ensure there is an industry standard, set out by the EU Centre, for service providers?

Article 13 Specific requirements for reporting

PCY comment: Article 18 DSA provides for an obligation for hosting services to report directly to national law enforcement services when they are aware of situations concerning a threat to life or security. This Article provides for a broader obligation to report via the EU Centre including also providers of interpersonal electronic communications. Do Member States think it should be explored if and how the risk for double reporting could be avoided?

Yes - Ireland believes that this should be explored.

Article 14 Removal Orders

Overall Ireland welcomes the revised wording of Article 14 and the use of "authority" instead of "competent judicial or independent administrative authority" within this article.

We seek further clarification on 14(2b) (a) –*"all investigations and assessments necessary have been carried out"*. Is this referring to investigations and assessment carried out by the EU Centre and the Coordinating Authority? Or does it also refer to an investigating LEA? We also suggest clarification on the envisaged timeframe.

Article 14a Procedure for cross-border removal orders

We question the necessity of Article 14a and believe that Articles 14 and 15 cover all the relevant and necessary points. We are of a view that there is sufficient redress and accountability provisions set out in both Articles 14 and 15.

We welcome the deletion of the previous 14a (4) text.

From a draft perspective, the reference to paragraph 7 in sub paragraph 2 is no longer accurate. Similarly, in paragraph 6, the reference to paragraph 6 in no longer accurate.

Article 15 Redress and provision of information

Ireland supports the changes made to Article 15

Article 16 Blocking orders

Ireland welcomes the revised wording in this article.

Article 18 Redress and provision of information

The PCY raises the following question in relation to 18(3): PCY observes that this complaint mechanism applies only to blocking orders. Do Member States think that a horizontal complaint mechanism should be explored, taking into account also Article 20 DSA?

Ireland is open to a horizontal mechanism being explored.

Compromise Text 14143/22 (Articles 19-39), issued 16 Nov 2022

Article 22 Preservation of Information

As previously indicated, our national LEA has concerns relating to the preservation of evidence. We believe it would be worthwhile exploring these concerns in a meeting with the Presidency and the Commission. We will contact the Presidency with a view to arranging same.

Article 25 Coordinating Authorities for child sexual abuse issues and other competent authorities

IE supports the change from 2 to 6 months and will support any further proposals to extend this time period.

Article 26 Requirements for Coordinating Authorities

IE opposes the addition in 26(1) as we are concerned that this language is too open to interpretation, particularly in the context of potential legal challenges. We could accept the insertion of "independent" into the first sub-paragraph as an alternative, describing the manner in which the CA acts, rather than its status. Therefore para 1 would read as follows:

*Member States shall ensure that the Coordinating Authorities that they designated perform their tasks under this Regulation in an **independent**, 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.*

Article 34 Right of users of the service to lodge a complaint

Ireland has a scrutiny reservation on 34(3). The Commission has not provided any detail of the assessment envisaged in this provision, nor of the "appropriate" circumstances in which the Coordinating Authority of the user's residence would transmit the complaint to the Coordinating Authority of establishment. This provision should include details of these matters, to ensure consistent application across the Union and to ensure that the Coordinating Authority of establishment does not become responsible for unsubstantiated complaints.

Article 36 Identification and submission of online child sexual abuse

We welcome the reinsertion of Coordinating Authority into the text.

ITALY

First of all, with regard to the possibility of allowing users to submit anonymous complaints and/or reports, this office expresses a dissenting opinion about this possibility: it often happens that users make anonymous reports regarding the availability of child sexual abuse material with the only purpose of belittling the victim. Therefore, the report should contain identification data of the whistleblower.

Instead, we agree on the need to standardize the terminology used as much as possible, leaving a minimum margin of interpretation. In particular, as regards the definition of URL contained in Article 2, letter y), reference can be made to the official document RFC3986.

Regarding the amendment of article 12 c.1 in the part in which the provider must report any information that raises even the simple suspicion of CSAM material presence, rather than information indicating the (its) potential presence, this office takes note of the intention to expand the reporting obligation on the part of the provider as much as possible. However, caution should be adopted in this regard as the term "potential presence" used previously and deleted was already broad enough to include cases of dubious, processing while information indicating suspicion seems too broad a term in relation to the purpose of the reporting obligation, implying the risk of receiving numerous negative reports, which, however, contribute to congesting the procedure for processing reports, the efficiency of which is proportional to the accuracy of the report received.

For the same reasons, it is believed that article 12 c. 4, can be maintained in its current formulation contained in the latest draft. In fact, detailing the reasons why a user reports the presence of CSAM material raises public awareness of the seriousness of the issue and reduces the risk of receiving reports based on a superficial evaluation

We share the priority need to avoid duplication of reports, therefore providers must look for solutions, even with the use of software and databases to avoid these circumstances

With regard to the possibility suggested by Sweden of providing for two processing channels depending on the urgency, it is suggested to rather have only one template with the possibility of ticking a flag indicating the urgency of the matter

The term metadata that Croatia would like to insert in article 13 appears generic, even if we agree on the need to include all the data held by the provider

Finally, with regard to the obligations to inform a victim, we share the view that they occur subject to the need to maintain investigative secrecy. Hence, the possibility must be left for the police to easily flag the above occurrence.

In addition to the comments on the minutes contained in the annex, these are the answers to the questions posed to this Office.

1) *Article 18 DSA provides for an obligation for hosting services to report directly to national law enforcement services when they are aware of situations concerning a threat to life or security. This Article provides for a broader obligation to report via the EU Centre including also providers of interpersonal electronic communications. Do Member States think it should be explored if and how the risk for double reporting could be avoided?*

The risk of duplication of reporting increases proportionally to the number of reporting and receiving authorities, therefore in the opinion of this office the only way to reduce the risk is to limit the number of interlocutors, and to establish clear reporting procedures with marked timescales in order to ensure timely completion

2) *The proposal means that a blocking order can only be issued if the subject-matter of the blocking is on the list provided for by the EU Centre. Do Member Sates think that there should be such a requirement? Or should it be sufficient that Member States share their blocking orders with the EU Centre and other Member States once they become final?*

To answer this question it is necessary to know the contents of the aforementioned list, in the absence of such indication we agree with the need to leave the Member States a wider margin for manoeuvre in the formulation of the blocking orders which, therefore, once final, can also simply be shared with the EU rather than being subordinated to the additional requirement of compliance with the object provided for in the aforementioned list.

MALTA

Malta firstly wishes to thank the Presidency for a number of amendments in the latest compromise text which further aligns the Proposal with the Digital Services Act. However, following other Member States' interventions in the meeting, some amendments may have led to the text becoming more complicated than necessary.

Document 6276/23 (Articles 1-18c)

– **Article 12 paragraph 2**

It seems that there is a missing link in the process since the provider will report to the Centre while the user can submit complaints to the coordinating authority which might not be aware of this reporting. Can you please clarify at what stage will the coordinating authority be made aware of this report?

– **Article 12 paragraph 3**

Whereas anonymous reporting should be given as an option, in view that not all users would wish to ascertain their identity, service providers should implement safeguards which would stop the mechanism from being misused.

– **Article 12 paragraph 4 sub clauses (a) and (b) (new)**

Malta agrees that the addition of these provisions could overburden the reporting mechanism established in paragraph 3, to the extent that its effectiveness will be lost. On point (a) the wording 'sufficiently substantiated' could be removed. Furthermore, if clause (b) is retained, the wording should be more generic so as not to limit the type and amount of information which the user may send.

– **Article 13 paragraph 1 clause (ba) (new)**

Following the explanation by the Commission that it is the manner and not the source of information by which the provider became aware of the potential child sexual abuse material, a separate requirement for the source of information to be given is suggested for inclusion in the list and accompanying Annex III template (in view that the source of information could be helpful for investigations).

– **Article 13 paragraph 1 clause (d)**

Malta supports the inclusion of metadata in the list. This would oblige service providers to store this type of data.

– **Footnote 4**

Double reporting is envisaged if a similar mechanism as to that established under Article 18 of the Digital Services Act is created here. Following clarifications during the meeting, there appears to be no need for another mechanism.

– **Article 14 paragraph 2**

Malta supports other Member States' suggestion to reduce the time to takedown child sexual abuse material to one hour. Reducing the time of the material propagating across the internet increases the likelihood of containing the spread.

– **Article 14 paragraph 2a (new)**

While Malta values the Presidency's standardisation of the text, in particular in view of the reference to the CJEU ruling on prior consultation, it is concerned that this would in practice increase the administrative burden on national authorities which would have already carried out a diligent assessment on the material. By comparison, the detection order is to our understanding a more sensitive and elaborate process which would necessitate the contribution of the service provider following the implementation plan under article 7 paragraph 3. There appears to be no added value in allowing service providers the possibility to provide input on the removal order and by extension to other orders (except the detection order) as a suitable redress mechanism is available for the reinstatement of the material should this be considered. Should the need be felt to retain this new provision, specific timeframes should be set for service providers to adhere to.

– **Article 15 paragraph 4**

Malta supports the increase in timeframe in paragraph 4 to twelve weeks.

– **Article 16 paragraph 2**

The rationale for article 14 paragraph 2a (new) applies here.

Document 14143/22 (Articles 19-39)

– **Article 25(9)**

Malta wishes to raise a scrutiny reservation on this provision. Applying the requirements of the Coordinating Authority to other competent authorities is not feasible in the Maltese system. Malta supports other Member States' intervention that this would effectively remove law enforcement authorities from the equation.

– **Article 26**

Malta reiterates its written comment following the meeting of 6 September 2022. The provisions on requirements for Coordinating Authorities remain overly restrictive, disallowing for established national structures to be designated without requiring comprehensive restructuring. Malta raises a scrutiny reservation on article 26 paragraph 1 and supports the deletion of the new provision while aligning the original text with the equivalent provision in the Terrorist Content Online Regulation.

THE NETHERLANDS

Art. 2 (j)

For Article 2(j), an earlier amendment to the text in the definition of 'child user' changed the age from 17 to 18 years. As we have previously noted, the inclusion of ages 17 and 18 causes problems with our national legislation. In the Netherlands, sexual majority is set at the age of 16. The Dutch criminalisation of grooming is also based on that age limit.

A solution would be to include 'the age of sexual consent' instead of an age in the definition of 'çhild user':

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

Could the presidency please elaborate on why this is not considered a desirable solution?

Art. 2 (s)

Article 2(s) of the CSAM Regulation refers to another regulation for the definition of 'content data'.

This definition of 'content data' includes voice and text. There is nothing in the regulation or the impact assessment about the mandatory detection of voice communication, but it refers to 'images', 'videos' and 'photographs'. The technical meetings also did not discuss technologies for detecting voice communication. The Netherlands is highly critical of the voice communication detection, because we have concerns about proportionality. The Netherlands would like to specify the definition of content data in this regulation instead of referring to another regulation. The Netherlands believes that voice communication and text should remain outside the scope of the regulation.

Art. 14

14.1

First of all, thanks to the Presidency for the proposed text of Article 14. We have indicated that the proposed process in Article 14.1 is legally impossible and contrary to the Dutch Constitution. We appreciate that the Presidency is seeking solutions.

The Netherlands believes that this provision is heading in the right direction. Nevertheless, we would like to ask a question for further clarification. In the current wording, we are uncertain whether it is also possible for the Coordinating Authority to seek judicial authorization, while the Coordinating Authority itself remains the issuing authority. Does the current wording leave enough flexibility for the administrative authority to ask a judge for authorization. Could the Presidency please elaborate on this?

14.2

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

14.2a

The Netherlands does not see much added value to this text. However, it does seem relevant to make an exception to Article 2a for justified emergencies. In those cases, we want to skip this step in the context of urgency.

Art. 14a

We are still studying this article in respect of our constitution. At this moment we would like to uphold a general scrutiny reservation for article 14(a).

Art. 15

(4)

It is not clear what is meant by the addendum 'if necessary'. The addition of ‘if necessary’ makes it arbitrary and makes it unclear when relevant public authorities should be consulted. The Netherlands suggests removing the text ‘if necessary’.

The Netherlands wants to emphasise that in the case of new material from CSAM law enforcement should always be informed, because this could be acute abuse but also so that ongoing cases are not disrupted. According to the Netherlands, this may be reflected more specifically in the text.

What should we consider by "or related offences"? This regulation only concerns CSA.

Art. 20

(1)

This article may raise expectations among victims. Can those expectations be met? In practice, the police see that there are images that, since they appeared, have been reported more than 2 million times. Is it then intended that the victim should be notified in every incident? And isn't the constant confrontation of this actually harmful to the victim?

It is a far-reaching obligation and also requires a lot of administration. We can discuss whether victims are entitled to proactive information sharing on this point, if this constant confrontation isn’t actually harmful to the victim and also whether expectations can be met.

Art. 25

(1)

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

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

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

Art. 26

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

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

Art. 27

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

Art. 38

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

Art. 39

(2)

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

POLAND

Art. 12 para 3 and 4 - in general, PL is positive about the direction in which we are heading towards clarifying the process of notifying CSAM by the user. Do we understand correctly that the provider is to establish and operate the notification system for users in such a way that they have the possibility (not the obligation) to justify why they consider the content to be CSAM? In other words, it seems that such a possibility should be created, but it should also be possible to notify without justification. Users will not always have the will, time or sufficient knowledge to justify a report, especially if the user is a child. The mechanism must be effective, easy and simple for everyone.

Art. 13 - support for the changes made, especially point (c) and "all content data" in accordance with submitted written comments PL

Art. 14 (removal orders) -

- with regard to the new sentence in para. 2 "The provider shall take the necessary measures to ensure that it is capable of reinstate the material or access thereto in accordance with Article 15(1a)." In PL's opinion, we should focus on ensuring that the removed content and all information necessary to identify the user and the victim have been secured for the purposes of the investigation by law enforcement authorities, so that it is possible to effectively detect the perpetrator and identify the victim and bring the perpetrator to justice. We need to be consistent with Art. 22, which is crucial for us - we propose to refer to this article in Art. 14 para 2.

- with regard to the new para. 2a - PL opposes the introduction of an obligation to inform the provider about the intention to issue an order and to wait for his comment. We do not know the aim of this consultation process and what its effect would be. It may interfere with the purpose of the regulation because it will prolong the removal process. The process of issuing the orders should be quick, simple and efficient, as time is of the essence in cybercrime, and the price is the safety of children. If the supplier does not agree with the content of the order, he will have the right under Art. 15 to redress and to challenge the order before the court which will independently assess its legitimacy. It is the best possible mechanism to protect the interests of the provider. We oppose the proposal of para. 2a in art. 14. From the perspective of law enforcement and combating child sexual abuse, this is a red line for PL.

- with regard to the new para. 2b - similarly, we have significant doubts concerning the justification of the added part. Letter a): What does "all investigations and assessments necessary have been carried out". An investigation will certainly be launched when there is a suspicion of a crime, but definitely not finished. An investigation cannot be a condition for issuing n order. Letter b): already in para. 1 we have the wording that the competent authority may issue an order after a diligent assessment. Perhaps "proportionality" or "fair balance" should be added here. However, similarly to the case 2a, we do not support the wording of the second paragraph in sec. 2b, in which it is mentioned of taking into account the view of the supplier as to the intention to issue the order. In this context, it is worth noting that orders to remove terrorist content under TCOs can already be removed without such conditions (such as the need to consult with the provider before issuing) and it is not clear why CSAM would require a different procedure.

Art. 14 para 4 - what does it mean that "a removal order should be given if necessary via the Coordinating Authority(…))? will the competent authority (not the coordinating authority) then be able to address the order directly to the provider? In our opinion, such a procedure is the shortest and most desirable when the authority competent to issue the order is an entity other than the coordinating authority. It is not clear whether this provision gives MS such flexibility?

Art.16 para 2 – see comments to removal orders. The proposed addition complicates and extends the procedure, it is not clear what is the purpose of "consultations" with the provider in this case. The supplier has the right to redress to the court. Designated Competent Authorities will have knowledge and experience in CSAM identification and orders are to be issued after careful assessment of the material.

Art. 17 para 3 – PL would like to thank the Presidency for taking into account PL comment and deleting "where relevant", but the question regarding "if necessary via CA" should be repeated - it is not fully clear when the intermediation of the coordinating authority will be necessary.

According to the analysis of meaning and context, "if necessary" may just be used here as: suggests that it may never be necessary at all. If so, then we would have many circumstances that would be allowed to eliminate Child Protection Preventive Action (CSE). This is a serious gap that the modification of Art. 17 made with the previous changes.

By analogy to paras 5 and 5a - there is the same problem with the interpretation of "if necessary". We could propose replacing words "if necessary" with "where" or „when necessary". We also propose to consider other provisions, where "if necessary" is used (e.g. Article 18) with a strong emphasis on the need to modify them, for the reasons stated above. Please kindly note that both doc. 14143/22 and 6276/23 also use the phrase "where necessary", hence both for unifying the mechanism, as well as greater clarity, it is justified to make the aforementioned change in favor of resigning from "if (...)".

Art. 19 (Liability of providers), we suggest including "if"; related to the need to show good will. Exclusion of liability as referred to in art. 19 (Providers of relevant information society services shall not be liable for child sexual abuse offenses solely because they carry out) should depend on the "good will of the service provider", and not only on the "mere fact of the actions taken", as they may be façade. In this case, the regulation will be ineffective and its implementation will be entirely dependent on individual providers, so it is proposed to modify the wording e.g. as follows: "Providers of relevant information society services shall not be liable for child sexual abuse offenses if they carry out, in good faith, the necessary activities to comply with the requirements of this Regulation (...).

Art. 26 - it should be noted that the provision requiring the coordinating authority to be free from all external influences and not to take instructions from other public authorities will greatly limit the possibility of assigning these tasks to already existing bodies. In particular none of the ministers or any of the police authorities will be able to play this role. Establishing a new body might be necessary to fulfil this role. For this reason, we propose to delete the provision "The Coordinating Authorities shall be free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party."

In our opinion, the priority is to limit the list of requirements for the Coordinating Authority – so that the authorities that are already dealing with the issue of counteracting to some extent and combat exploitation could fulfil this role. There must be more flexibility in this regard for MS.

Art. 39 - We support strengthening the role of hotlines and references to them in the draft. In Art. 39 para 2 and 3, we propose to add references to hotlines as follows:

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

The Coordinating Authorities, hotlines, 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."

ROMANIA

Art. 14 Referring to doc 6276/23 regarding the compromise proposals, RO agrees with the proposals, with the exception of the issue of the 24 hour deadline under art. 14, paragraph 2. We consider this term to be far too long for content removal. While a 24-hour period for executing a removal order may be reasonable in some cases, there are strong reasons to argue that a one-hour time limit would be more appropriate. If content is deemed harmful or illegal, then every hour it remains online could potentially cause further harm. By reducing the time period to 1 hour, illegal content could be removed more quickly, reducing the potential for harm it causes.

If the proposal to set a one-hour time limit would not be generally accepted, perhaps consideration should be given to having more time limits for the provider to remove illegal material on a case-by-case basis. For example, in the cases of easy-to-remove material such as text-based content or small image files, a 1-hour time frame for executing a takedown order would be appropriate, and a longer or 24 hours for storage-intensive materials such as long-form videos. Content types based on text, images and short videos can often be easily identified and removed from a provider's platform, especially if the provider has a strong content moderation system.

Art. 15 Regarding article 15 paragraph 1a, the addition of seeking the user's consent before reinstating the material subjected to the CSA investigation is a sensible measure to ensure that the user's rights and interests are respected. It is possible that the user may not wish for the material to be reinstated due to personal reasons or safety concerns. Therefore, seeking the user's consent is a respectful and responsible approach.

Additionally, some material that is subjected to CSA investigations may involve sensitive content, but not actual CSA material, for example a nude 1-2 years old child at a beach, which in many cases is habitual. In such cases, it is crucial to ensure that the material is not reinstated without proper consideration. Seeking the user's consent before reinstating such material would allow for a more nuanced and careful decision-making process.

Therefore, by seeking the user's consent before reinstating the material subjected to the CSA investigation, the provider can demonstrate a commitment to protecting the user's rights and safety, and ensure that the reinstatement decision is made in a responsible and ethical manner.

SLOVAKIA

Comments on Presidency's compromise text (doc. 6276/23)

The Slovak Republic thanks SE PRES for submitting the compromise text. In general, we appreciate the constructive and pragmatic work of the PRES, which has brought about significant amendments to the draft proposal, which are, in our opinion, clearly moving in the right direction.

In particular, the Slovak Republic thanks SE PRES for incorporating our proposed amendment in Art. 12 para. 2 (scope of reporting obligations).

Art. 14 para. 2a (new)

SR welcomes the inclusion of additional safeguards for service providers by allowing them to comment on the content of the proposed removal order, but we believe that **a maximum time period for comment should be set here**. (i.e. "within a reasonable time period set by that authority. **That time period shall not be longer than [xx]**". It is important that the material is removed as soon as possible and without undue delay, which may be caused by the addition of additional procedural steps. The need for quick removal is also emphasized by the removal deadline set in para. 2: within 24 hours of receiving the removal order. We believe that this article applies a different logic to the one relating to detection orders as in the case of removal orders, the material in question has already been confirmed to contain child sexual abuse.

The same comment also applies to Art. 16(2) (new) (blocking orders).

Art. 15 1a (new)

The Slovak Republic agrees with the inclusion of the provision, but suggests softening the text by replacing the text "shall immediately reinstate" with the text "**shall, without undue delay, reinstate**" considering that the immediate reinstating of the content does not appear to be sufficiently justified from the point of view of the users' rights.

The same comment **also applies to Art. 18(1a) (new)** (blocking orders) as well as **Art. 14a(6)** (procedure for cross-border removal orders) and **Art. 18c(2)** (redress and provision of information relating to delisting orders)

Art. 15 para. 4 letter a)

In accordance with our previously voiced position, the Slovak Republic requests an extension of the period for not informing the user from 6 to **12 weeks** in order to prevent the potential interference with a possible investigation by law enforcement authorities.

Art. 17 para. 5a (new)

The Slovak Republic would like to see strengthening of the provision on **mandatory reporting** on the implementation of the blocking order to the competent authority, also when with regard to **reporting at regular intervals** pursuant to the second indent of the paragraph. This information is in any case important to the competent authority.

Comments on doc. 14143/22 (Articles 19-39)

Art. 22 para. 2

The Slovak Republic would like to suggest an examination of the appropriateness of **setting also a minimum time period for data retention (e.g. 6 months)**, in addition to the maximum time period. This would be to ensure in any case the retention of data in the period from the notification of potential child sexual abuse to the EU Centre pursuant to Article 12 until the point when law enforcement authorities may request information relating to moment when the possible requests from relevant for data relating to the report in question.

Art. 25 para. 1

The Slovak Republic requests an extension of the time limit for designating one or more competent authorities as responsible for the application and enforcement of the proposed Regulation from 6 to **12 months**. It is clear that potentially establishing a new authority, endowing an existing authority with the powers necessary for the application of this Regulation or establishing a network of cooperating national authorities requires considerable legislative work, preparation of agreements at national level, preparation in terms of material, financial, personnel, etc. by Member States. This is the case even when taking into account the overlapping roles and powers of the proposed Coordinating Authority and the Digital Services Coordinator to be established pursuant to the Digital Services Act. At the same time, we suggest that a clarification be included in the recitals that the Coordinating Authority under this proposal and the Digital Services Coordinator may be the same authority.

SPAIN

Article 13: Specific reporting requirements: Do Member States consider that consideration should be given to whether and how to avoid the risk of double reporting of these facts?

Article 13 of the CSAM Regulation refers to specific requirements for the reporting of suspected child sexual abuse, which is related to Article 18 of the DSA. While there is some overlap, there are also differences: the DSA article applies only to hosting, while CSAM applies to hosting and interpersonal communications; DSA refers to suspicions of crimes involving threat to life and safety, while CSAM refers to suspicions of sexual abuse of children in its service; in DSA suspicions are reported to law enforcement or judicial authorities, while in CSAM they are reported to CSAM's EU Center agency (without prejudice to subsequent referral to national law enforcement authorities).

Finally, Article 13 CSAM develops Article 12 in detail, establishing a series of requirements that the DSA lacks in this specific aspect, and which are key for police investigation, notably point f) on the identification of the IP address and TCP port in question.

In short, in order to ensure that communication is made with respect to CSAM content, it is considered that the horizontal provision of Article 18 DSA is enabling but not sufficient with respect to the sectoral CSAM requirement; and consequently, it seems appropriate that Articles 12 and 13 CSAM are maintained and developed in detail in their specific scope.

Article 18: Recourse and provision of information: The Chair notes that this complaint mechanism only applies to blocking orders. Do Member States consider that a horizontal complaint mechanism should be considered, also taking into account Article 20 of the Digital Services Act?

Section 5 regulates blocking orders, which can be sent by competent authorities to providers of internet access services, with the provider having to remove the content as indicated in the articles. Article 18.3 stipulates that these providers must provide a system to enable users to complain about alleged breaches of the obligations in this section.

Other sections of the CSAM Regulation regulate content removal orders from hosting providers and de-indexing orders from search engines. However, these sections do not provide for providers to offer users complaint systems. It is not clear why only Internet access service providers, and not hosting providers and search engines, are considered to be able to lodge complaints.

As regards the possibility of applying the internal complaints management system of Article 20 of the DSA, it should be borne in mind that this Article only applies to content moderation decisions by the provider (both voluntary content moderation systems and following Notice&Action mechanisms), but not to content removal following orders from competent authorities. On the other hand, in any event, Article 20 of the DSA Regulation only applies to online platform providers, which are only a subset of the total number of hosting service providers.