European Parliament
2019-2024

Committee on the Internal Market and Consumer Protection

2022/0155(COD)

27.6.2023

COMPROMISE AMENDMENT 1 - 8

Draft opinion
Alex Agius Saliba
(PE740.727v01-00)

Laying down rules to prevent and combat child sexual abuse

Proposal for a regulation
(COM(2022)0209 – C9-0174/2022 – 2022/0155(COD))

AM_Com_LegCompr

Batch 1

Compromise amendment on Chapter I
Compromise amendment replacing all relevant amendments, including AM (235, 236, 237, 33, 238, 239, 240, 241, 34, 242, 35, 36, 243, 244, 245, 37, 246, 247, 248, 249, 250, 38, 251, 252, 253, 254, 255, 256, 39, 40, 257, 41, 258, 42, 259, 260, 261, 43, 262, 263, 264, 265, 266, 267, 44, 268, 269, 270, 271, 45, 272, 46, 273, 47, 274, 275, 159, 1, 160, 161, 162, 2, 163, 164, 165, 166, 3, 167, 168, 169, 4, 170, 5, 171, 6, 172, 7, 173, 174, 8, 175, 9, 176, 177 and 184)

Article 1

Subject matter and scope

1. This Regulation lays down uniform rules to address the ~~mis-~~use of relevant information society services for online child sexual abuse in ***order to contribute to the proper functioning of*** the internal market ***and to create a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter are effectively protected***.

   It establishes, in particular:

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

   [(b) "obligations on ***relevant*** providers of ***information society services that allow the dissemination, exchange and sharing of images, video and audio material*** ~~hosting services and providers of interpersonal communication services to detect and~~ ***to identify and*** report online child sexual abuse;" tbd political]

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

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

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

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

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

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

   (b) Directive 2000/31/EC and Regulation (EU) ***2022/2065*** ~~…/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC];~~

   (ba) Regulation (EU) .../... [laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts;

   (c) Directive 2010/13/EU;

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

(e) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

4. This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC insofar as necessary for the execution of the detection orders issued in accordance with Section 2 of Chapter 1 of this Regulation.

Article 2

Definitions

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

(a) 'hosting service' means an information society service as defined in Article 3 ~~2~~, point (~~f~~ g), third indent, of Regulation (EU) ***2022/2065*** ~~*…/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*~~;

(aa) 'cloud computing service' means a service as defined in Article 6, point (30), of Directive (EU) 2022/2555.

(b) 'interpersonal communications service' means a publicly available service as defined in Article 2, point 5, of Directive (EU) 2018/1972, including services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service ***in so far as they allow the dissemination and sharing of images, video and audio material***;

(ba) 'number-independent interpersonal communications service' means a publicly available service as defined in Article 2, point 7, of Directive (EU) 2018/1972;

(c) 'software application' means a digital product or service as defined in Article 2, point ***15*** ~~13~~, of Regulation (EU) ***2022/1925*** ~~*…/…* [*on contestable and fair markets in the digital sector (Digital Markets Act)*]~~;

(d) 'software application store' means a service as defined in Article 2, point ***14*** 12, of Regulation (EU) ***2022/1925*** ~~*…/…* [*on contestable and fair markets in the digital sector (Digital Markets Act)*]~~;

(e) 'internet access service' means a service as defined in Article 2(2), point 2, of Regulation (EU) 2015/2120 of the European Parliament and of the Council[1];

(f) 'relevant information society services' means all of the following services:

(i) a hosting service;

(ii) a ***'number-independent'*** interpersonal communications service;

[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

(iii) a software applications store;

(iv) an internet access service.

(g) 'to offer services in the Union' means to offer services in the Union as defined in Article ***3*** ~~2,~~ point (***g*** ~~d~~), of Regulation (EU) ***2022/2065*** ~~…/…~~ [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~];

(h) 'user' means any natural or legal person who uses a relevant information society service;

(h a) 'hotline' means a service provided by an entity, other than the reporting channels provided by law enforcement agencies, under which victims or other members of the public are able to anonymously report alleged child sexual abuse to that entity, and which is officially recognised by the Member State of establishment of that entity for the purpose of combating child sexual abuse;

(h b) 'help-line' means a service provided by an entity, which is officially recognised by the Member State of establishment of that entity, consisting in providing information and support to children in need;

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

(j) 'child user' means a natural person who uses a relevant information society service and who is a natural person below the age of 17 years;

(k) 'micro, small or medium-sized enterprise' means an enterprise as defined in Commission Recommendation 2003/361 concerning the definition of micro, small and medium-sized enterprises[2];

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

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

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

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

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

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

(r) 'recommender system' means the system as defined in Article **3**, point (***s*** ~~o~~), of Regulation (EU) ***2022/2065*** ~~*…/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*~~;

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

---

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

(t) 'content moderation' means the activities as defined in Article **3**, point (***t*** ~~p~~), of Regulation (EU) ***2022/2065*** ~~*…/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*~~;

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

(v) 'terms and conditions' means terms and conditions as defined in Article **3**, point (***u*** ~~q~~), of Regulation (EU) ***2022/2065*** ~~*…/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*~~;

(w) 'main establishment' means the head office or registered office of the provider of relevant information society services within which the principal financial functions and operational control are exercised.

Relevant Recitals (1- 13, 16a)

(1) Information society services have become very important for communication, expression, gathering of information and many other aspects of present-day life, including for children. ***However, these services are also used by*** ~~but also for~~ perpetrators of child sexual abuse offences. Such offences, which are subject to minimum rules set at Union level, are very serious criminal offences that need to be prevented and combated effectively in order to protect children's rights and well-being, as is required under the Charter of Fundamental Rights of the European Union ('Charter'), and to protect society at large. Users of such services offered in the Union should be able to trust that the services concerned can be used safely ***in a trusted online environment***, especially by children.

(2) Given the central importance of relevant information society services, ***for the digital single market and the fact that those services might be abused by third parties to carry out illigal activities related to child sexual abuse online, it is important to ensure*** ~~aims can only be achieved by ensuring~~ that providers offering such services in the Union behave responsibly and take reasonable measures to minimise the risk of their services being ~~mis~~used for the purpose of child sexual abuse, those providers often being ~~the only ones~~ in a position to prevent and ***to help*** combat such abuse. The measures taken should be targeted, carefully balanced, ***effective, necessary*** and proportionate, ***and subject to constant review***, so as to avoid any undue negative consequences for those who use the services for lawful purposes, in particular for the exercise of their fundamental rights protected under Union law, that is, those enshrined in the Charter and recognised as general principles of Union law, and so as to avoid imposing any excessive burdens on the providers of the services.

(3) Member States ***are aware of the existing problem and are*** increasingly introducing, or are considering introducing, national laws to prevent and combat online child sexual abuse, in particular by imposing requirements on providers of relevant information society services. ***On the other hand,*** ~~In the light of~~ the inherently cross-border nature of the internet and the service provision concerned, ***and the diverging*** ~~those~~ national laws, ~~which diverge~~, ***may*** have a direct negative effect on the internal market. To increase legal certainty, eliminate the resulting obstacles to the provision of the services and

ensure a level playing field in the internal market, the necessary harmonised requirements should be laid down at Union level.

(4) Therefore, this Regulation should contribute to the proper functioning of the internal market by setting out clear, uniform ***effective, proprotionate and carefully*** balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights of all parties concerned. In view of the fast-changing nature of the services concerned and the technologies used to provide them, those rules should be laid down in technology-neutral and future-proof manner, so as not to hamper innovation ***and the fight against crime***.

(4a) The measures in this Regulation should be complemented by the Member States' strategies to avoid victimisation of the victims, to increase public awareness and inform people about victims' rights and on how to seek child-friendly and age appropriate reporting mechanisms.(AM 160)

(5) In order to achieve the objectives of this Regulation, it should cover providers of services that have the potential to be misused for the purpose of online child sexual abuse. As they are increasingly misused for that purpose, those services ~~should~~ ***could*** include publicly available ***number-independent*** interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those services **are** ~~as~~ publicly available. ***The mere use of a number as an identifier should not be considered to be equivalent to the use of a number to connect with publicly assigned numbers and should therefore, in itself, not be considered to be sufficient to qualify a service as a number-based interpersonal communications service. To this end, obligations under this Regulation should apply to number-independent interpersonal communications services, regardless of whether they use numbers for the provision of their service, such as messaging services, in so far as those services are publicly available and they allow for the dissemination and exchange of images and videos.*** As services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service, such as chat and similar functions as part of ***online games*** ~~gaming~~, image-sharing and video-hosting are ~~equally~~ ***also*** at risk of use ***for the purpose of online child sexual abuse***, they should also be covered by this Regulation, ***in so far as they allow for the dissemination and exchange of images and videos uploaded by their users.*** However, given the inherent differences between the various relevant information society services covered by this Regulation and the related varying risks that those services are misused for the purpose of online child sexual abuse and varying ability of the providers concerned to prevent and combat such abuse, the obligations imposed on the providers of those services should be differentiated in an appropriate manner. ***For example, where it is necessary to involve providers of information society services, including providers of intermediary services, any requests or orders for such involvement should, as a general rule, be directed to the specific provider that has the technical and operational ability to act against specific child sexual abuse material, so as to prevent and minimise any possible negative effects on the availability and accessibility of information that is not child sexual abuse material.***

(5a) Considering the specific nature of search engines and their role in addressing the dissemination of child sexual abuse material they should be subject to tailored obligations, namely delisting of instances of confirmed online child sexual abuse.

(6) Online child sexual abuse ~~frequently~~ ***can also*** involve~~s~~ the misuse of information society services offered in the Union by providers established in third countries. In order to ensure the effectiveness of the rules laid down in this Regulation and a level playing field within the internal market, those rules should apply to all providers, irrespective of

their place of establishment or residence, that offer services in the Union, as evidenced by a substantial connection to the Union.

(7) This Regulation should be without prejudice to the rules resulting from other Union acts, in particular Directive 2011/93 of the European Parliament and of the Council[3], Directive 2000/31/EC of the European Parliament and of the Council[4] and Regulation (EU) ***2022/2065*** ~~…/… of the European Parliament and of the Council[5] [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~, Directive 2010/13/EU of the European Parliament and of the Council [6], Regulation (EU) 2016/679 of the European Parliament and of the Council[7], and Directive 2002/58/EC of the European Parliament and of the Council[8].

(8) This Regulation should be considered *lex specialis* in relation to the generally applicable framework set out in Regulation (EU) ***2022/2065*** ~~…/…~~ [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~] laying down harmonised rules on the provision of certain information society services in the internal market. The rules set out in Regulation (EU) ***2022/2065*** ~~…/…~~ [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~] apply in respect of issues that are not or not fully addressed by this Regulation.

(9) Article 15(1) of Directive 2002/58/EC allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in certain specific provisions of that Directive relating to the confidentiality of communications when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, inter alia, to prevent, investigate, detect and prosecute criminal offences, provided certain conditions are met, including compliance with the Charter. Applying the requirements of that provision by analogy, this Regulation should limit the exercise of the rights and obligations provided for in Articles 5(1), (3) and 6(1) of Directive 2002/58/EC, insofar as strictly necessary to execute detection orders issued in accordance with this Regulation with a view to prevent and combat online child sexual abuse.

(10) In the interest of clarity and consistency, the definitions provided for in this Regulation should, where possible and appropriate, be based on and aligned with the relevant definitions contained in other acts of Union law, such as Regulation (EU) ***2022/2065*** ~~…/…~~ [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~].

(11) A substantial connection to the Union should be considered to exist where the relevant information society services has an establishment in the Union or, in its absence, ~~on the~~

---

3 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (*OJ L* 335, 17.12.2011, p. 1).

4 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

5 Regulation (EU) …/… of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (OJ L ….).

6 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media service (OJ L 95, 15.4.2010, p. 1).

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

8 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications') (OJ L 201, 31.7.2002, p. 37).

~~basis of the existence of a significant number of users~~ ***where the*** number of ***recipients of the service*** in one or more Member States ***is significant in relation to the population thereof, or on the basis of*** ~~or the~~ targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. The targeting of activities towards a Member State could also be derived from the availability of a software application in the relevant national software application store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1), point (c), of Regulation (EU) 1215/2012 of the European Parliament and of the Council[9]. Mere technical accessibility of a website from the Union should not, ***on that ground*** alone, be considered as establishing a substantial connection to the Union.

(12) For reasons of consistency and technological neutrality, the term 'child sexual abuse material' should for the purpose of this Regulation be defined as referring to any type of material constituting child pornography or pornographic performance within the meaning of Directive 2011/93/EU, which is capable of being disseminated through the use of hosting or interpersonal communication services. At present, such material typically consists of images or videos, without it however being excluded that it takes other forms, especially in view of future technological developments.

(13) The term 'online child sexual abuse' should cover not only the dissemination of material previously detected and confirmed as constituting child sexual abuse material ('known' material), but also of material not previously detected that is likely to constitute child sexual abuse material but that has not yet been confirmed as such ('new' material), as ~~well as activities constituting the solicitation of children ('grooming')~~. That is needed in order to address not only past abuse, the re-victimisation and violation of the victims' rights it entails, such as those to privacy and protection of personal data, but to also address recent, ongoing and imminent abuse, so as to prevent it as much as possible, to effectively protect children and to increase the likelihood of rescuing victims and stopping perpetrators.

(16 a) To further address online child sexual abuse effectively, an emphasis should be placed on public awareness raising, including through easily understandable campaigns and in education with a focus on strengthening digital skills and empowering children to use the internet safely. In addition, awareness raising should also focus on hotlines and help-lines where children can report abuse, as well as on improving access to institutional reporting by law enforcement and other authorities.

---

9 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

Batch 2

Compromise amendment on Chapter II, Section 1
Compromise amendment replacing all relevant amendments, including AM (276, 277, 278, 279, 48, 280, 49, 281, 50, 282, 51, 283, 284, 285, 286, 287, 288, 289, 290, 291, 52, 292, 293, 294, 295, 53, 296, 54, 297, 55, 298, 56, 299, 57, 300, 58, 59, 301, 302, 60, 303, 304, 305, 306, 307, 308, 309, 310, 311, 61, 312, 313, 314, 315, 316, 317, 62, 318, 319, 320, 321, 322, 323, 324, 63, 64, 325, 65, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 66, 338, 67, 339, 68, 337, 340, 341, 342, 69, 343, 344, 345, 70, 71, 346, 347, 348, 350, 351, 352, 353, 354, 72, 355, 356, 357, 73, 358, 359, 74, 360, 361, 362, 363, 364, 75, 365, 76, 366, 77, 78, 79, 80, 81, 82, 367, 368, 369, 370, 371, 83, 84, 372, 373, 374, 375, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 86, 389, 178, 10, 179, 180, 11, 181, 182, 183, 12, 184, 185, 186, 187, 188, 13, 189, 190, 191, 192, 14, 193, 194, 195, 15, 196, 197 and 16)

Article 3

Risk assessment

1. Providers of hosting services and providers of ***number-independent*** interpersonal communications services shall identify, analyse and assess, ***any systemic*** ~~for each such service that they offer, the~~ risk of use of ~~the~~ ***their*** service for the purpose of online child sexual abuse. ***That risk assessment shall be specific to the services they offer and proportionate to the systemic risk considering its severity and probability, including in the specific cases where service was misused to disseminate child sexual abuse materials.***

1 a. Without prejudice to Regulation (EU) 2022/2065, when conducting the risk assessment, providers of hosting services and providers of number-independent interpersonal communications services shall respect and avoid any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity, respect for private and family life, the protection of personal data, freedom of expression and information, including the freedom and pluralism of the media, the prohibition of discrimination, the rights of the child and consumer protection, as enshrined in Articles 1, 7, 8, 11, 21, 24 and 38 of the Charter respectively

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

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

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

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

      – measures taken to enforce such prohibitions and restrictions;

      – functionalities enabling ~~age verification~~ ***the effective protection of children online and preventing online child sexual abuse, without prejudice to Regulation EU2016/679***;

      – ***functionalities enabling appropriate parental control measures***

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

– ***functionalities enabling detection of known child sexual abuse material, insofar as they remain strictly limited to what is needed for the purpose of complying with their obligations under this Regulation, proportionate and effective, and the relevant technology used is sufficiently reliable to limit to the maximum extent possible the rate of errors in distinguishing between lawful and unlawful content, without the need of independent human assessment*;**

– ***functionalities ~~preventing uploads of content from the internet, requiring specific software, configurations, or authorisations to access it~~ allowing accessing the dark web;***

(b a) the ~~capacity~~ resources to meaningfully deal with reports and notifications about child sexual abuse in a timely manner;

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

(d) the manner in which the provider designed and operates the service, including the business model, governance and relevant systems and processes, ***the design of their recommender systems and any other relevant algorithmic system*** and the ***negative impact*** thereof on that risk, ***without prejudice to trade secrets under Directive (EU) 2016/943***;

(e) with respect to the risk of solicitation of children:

(i) the extent to which the service ***is targeting and is*** ~~is used or is likely to be~~ used by children;

(ii) where the service is used by children, ~~the different age groups of the child users and~~ ***the risk*** of solicitation of children ***particularly*** in relation to ~~those~~ different age groups;

(iii) the availability of functionalities creating or reinforcing the risk of solicitation of children, including the following functionalities:

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

– ***enabling unsolicited contact for users and, in particular, for adult users to engage and connect with unknown child users;***

– enabling users to ~~establish~~ ***initiate unsolicited direct*** contact with other users directly, in particular ***on services targeting child users or*** through private communications;

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

– ***enabling child users to create usernames that contain information on their location, age or a representation about, or imply, their age;***

– ***enabling users to know or infer the location of child users.***

2a. Where providers of hosting services and number independent interpersonal communication services seek to conduct the age assurance of users or to assess the age of child users, including through parental control tools, such measures shall not lead to maintaining, acquiring or processing more personal data than they already have and are strictly necessary in order to assess if user is a child user, including not processing sensitive data such as biometric data. Thus, this obligation shall not incentivize providers of hosting

services and number independent interpersonal communication services to collect the age of the user. Any methods used to assess the age of users shall be without prejudice to Union law on protection of personal data and shall respect the rights of the child, take particular regard of the risks for exclusion from the online world for children that are unable to comply with the requirements and provide for appropriate remedies and redress mechanisms.

3. The provider may request the EU Centre to perform a~~n~~ ***methodology*** analysis ***of*** ~~the~~ ***risk assessment and*** ~~of representative~~, anonymized data samples ~~to identify potential online child sexual abuse,~~ ***available to the EU Centre*** to support the risk assessment. ***The request cannot serve the purpose of evading the provider's obligations set up in this Regulation. The EU Centre shall perform the analysis in a timely manner.***

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

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

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

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

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

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

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

6. The Commission, in cooperation with Coordinating Authorities, ~~and~~ the EU Centre ***and the European Data Protection Board*** and after having conducted a public consultation, may issue guidelines on the application of paragraphs 1 to 5, ***in particular to present best practices and support for micro and small sized enterprises to be able to fulfil the obligations of this Article,*** 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.

6a. By way of derogation, providers that qualify as small and micro enterprises as defined in Commission Recommendation 2003/361/EC shall submit a simplified risk assessment by [Date of application of this Regulation + 6 months], from the date

referred to in Article 3(4) or by by 6 months from the date at which the provider started offering the service in the Union.

6b. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to provide practical support for micro and small enterprises and to supplement this Regulation with the simplified risk assessment under paragraph 6a of this Article.

Article 4

Risk mitigation

1. Providers of hosting services and providers of ***number-independent*** interpersonal communications services shall ***put in place*** ~~take~~ reasonable, ***effective and targeted specific*** mitigation measures, tailored to ***the type of service offered and proportionate to*** the risk identified pursuant to Article 3, ~~to minimise~~ ***with the aim of mitigating*** that risk. Such measures shall include ***at least*** some or all of the following:

(-a) adapting the design, features and functions of their services in order to ensure a high level of privacy, safety, and security by design and by default for children;

(a) ***testing and*** adapting, through appropriate technical and operational measures and staffing, the provider's content moderation or recommender systems, its decision-making processes, the operation or functionalities of the service, ~~or the content or enforcement of its terms and conditions~~***, including the speed and quality of processing notices and reports related to online child sexual abuse and, where appropriate, the expeditious removal of the content notified***;

(a a) introducing parental control features and functionalities that allow the parents or the legal guardians to exercise oversight over the child's activity;

(a b) informing users about services or organisations in the user's region on preventing child sexual abuse, counselling, victim support and educational resources by hotlines and child protection organisations, including platform mechanisms or tools placed in a prominent way that allows users and potential victims to seek help;

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

(c) initiating or adjusting cooperation, in accordance with competition law, with other providers of hosting services or providers of interpersonal communication services, public authorities, civil society organisations or, where applicable, entities awarded the status of trusted flaggers in accordance with Article ***22*** of Regulation (EU) ***2022/2065***. ~~…/… [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~ .

(c a) initiating and reinforcing awareness-raising measures and adapting their online interface for increased user information, including automatic mechanisms and interface design elements to inform users about external preventive intervention programmes;

(c b) initiating tools aimed at helping users to indicate child sexual abuse material and children, to signal abuse or obtain support, as appropriate.

2. The mitigation measures shall be:

(a) effective ***and proportionate*** in mitigating the identified ~~***serious***~~ ***systemic*** risk, ***taking into account the characteristics of the service provided and the manner in which that service is used***;

(b) targeted and proportionate in relation to that risk, taking into account, in particular, ***any impact on the functionality of the service and*** the seriousness of the risk as well as the provider's financial capabilities and technological ~~capabilities~~ ***limitations*** and the number of users;

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

(c a) based on clear objectives and methodologies for identifying and quantifying impacts on the identified ~~serious~~ risk and on the exercise of the fundamental rights of all affected parties;

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

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

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

5. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, ~~may~~ ***shall*** issue guidelines on the application of paragraphs 1, 2, 3 and 4, ***in particular to present best practices and recommend mitigation measures and support for micro and small sized enterprises to be able to fulfil the obligations of this Article,*** having due regard in particular to relevant technological developments and in the manners in which the services covered by those provisions are offered and used.

Article 5

Risk reporting

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

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

(b) any ***specific*** mitigation measures taken pursuant to Article 4***, and the effectiveness of such measures in the prevention, dissemination and detection of online child sexual abuse, ~~including~~ and the level of intrusiveness of such measures on their users and assessment of alternative options, and whether this was the least intrusive option available;***

(b a) where applicable, any indicators of accuracy or margin of error with the technology used, as well as rates of false positives, false negatives, and number of appeals;

(b b) where applicable, the number of orders received pursuant to Articles 7 and 14, including information on the median time needed to inform its receipt and to give an effect to the order;

(b c) where applicable, the number of notices submitted by users;

(b e) actions taken pursuant to online child sexual abuse by differentiating whether the action was taken on the basis of the law or on the basis of [Articles 7, 8a new, 12 or 14].

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

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

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

4. Without prejudice to Articles 7 and 27 to 29, where the requirements of Articles 3 and 4 have not been met, ***before taking any other steps pursuant to Article 7,*** ~~that~~ ***the*** Coordinating Authority shall require the provider to ***make specific updates to*** ~~re-conduct or update~~ the risk assessment or to introduce, review, discontinue or expand, as applicable, the mitigation measures, ***that do not adversely affect the fundamental rights or legitimate interests of the users of the service*** within a reasonable time period set by that Coordinating Authority. That time period shall not be longer than one month.

4 a. Where the requirements of Articles 3 and 4 have been met and the provider has successfully implemented and enforced mitigations measures that minimise and prevent the risk of use of their service for the purpose of online child sexual abuse, the Coordinating Authority shall issue a positive opinion that needs to be taken into account prior to any decision pursuant to Article 7.

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

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

6a. By way of derogation, providers that qualify as small and micro enterprises as defined in Commission Recommendation 2003/361/EC shall submit a simplified version of the report by 6 months, from the date referred to in Article 3(4).

6b. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to provide practical support for micro and small enterprises and supplement this Regulation with the simplified reporting under paragraph 6a of this Article.

Article 6

Obligations for software application stores

1. Providers of software application stores shall:

   a) ***indicate, based on the information provided by the*** ~~make reasonable efforts to assess, where possible together with the~~ providers of software applications ***developers,*** whether ~~each service offered through~~ the software applications ***contain features that could pose risk to children*** ~~***or*** that they intermediate of being used for the purpose of the solicitation of ***to*** children~~;

   (b) ***indicate, based on the information provided by*** ~~take reasonable measures to prevent child users from accessing~~ the software applications ***developers, if measures have been taken by the software applications to mitigate the risks*** ~~in relation to which they have identified a significant risk of use of the service concerned for the purpose of the solicitation of children~~***, and which measures have been taken to ensure safety and security by design and by default for children***;

   (c) ***indicate, based on the information provided by the provider of the applications, the minimum age for using an application, as set out in the terms and conditions of the provider of the application;*** ~~take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b).~~

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

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

4. The Commission, in cooperation with Coordinating Authorities, ~~and~~ the EU Centre and ***the European Data Protection Board and the Fundamental Rights Agency,*** 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.

Article 6 a

Security of communications and prohibition on general monitoring

1. Nothing in this Regulation shall be construed as prohibiting, restricting or undermining the provision or the use of encrypted services nor shall be interpreted as prohibiting providers of information society services from providing their services applying end-to-end encryption. Member States shall not prevent or discourage providers of relevant information society services from offering encrypted services or from providing their services applying encryption.

2. Nothing in this Regulation should undermine the prohibition of general monitoring under EU law.

(included above in Art. 3, 4 and 5)

Relevant recitals (13a, 13b, 14-19~~21~~):

(13a) Providers of online games falling under the scope of this Regulation should take the necessary technical and organisational measures to ensure safety and security by design and by default for children, including the option to prevent unsolicited contact between users, facilitating user-friendly reporting mechanisms and providing tools in a prominent way on their platform that allow users and potential victims to seek help from a help-line.

(13b) Where an online platform is primarily used for the dissemination of user generated pornographic content, the platform should take the necessary technical and organisational measures to ensure safety of children such as a user-friendly reporting mechanisms to report alleged child sexual abuse material, adequate professional human content moderation to rapidly process notices of alleged child sexual abuse material and provide tools to inform users in a prominent way about prevention programmes.

(14) With a view to minimising the risk that their services are used for the dissemination of known ~~or new~~ child sexual abuse material ~~or the solicitation of children~~, providers of hosting services and providers of publicly available ***number-independent*** interpersonal communications services should assess ***the existence of a systemic*** ~~such~~ risk ***stemming from the design and functioning*** of ~~for each of~~ the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements ***and safeguards*** to be taken into account should be provided. To allow for a full consideration of the specific characteristics of the services they offer, providers should be allowed to take account of additional elements where relevant. As risks evolve over time, in function of developments such as those related to technology and the manners in which the services in question are offered and used, it is appropriate to ensure that the risk assessment, ***as well as the effectivness and proportionality of specific measures, are*** ~~is~~ updated regularly and when needed for particular reasons. ***That risk assessment should be specific to the services offered and proportionate to the systemic risk considering its severity and probability.***

(15) Some of those providers of relevant information society services in scope of this Regulation may also be subject to an obligation to conduct a risk assessment under Regulation (EU) ***2022/2065*** ~~…/… [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~ with respect to information that they store and disseminate to the public. ***The obligations under this Regulation should not affect the obligations for very large online platforms and very large online search engines under Regulation (EU) 2022/2065. However, in order to ensure consistency and avoid duplication, very large online platforms and very large online search engines could also use, for the purpose of the risk assessment under this Regulation, the information already gathered*** for the purposes of ~~the present~~ Regulation ***2022/2065***, ***so that these*** ~~those~~ providers may draw on such a risk assessment and complement it with a more specific assessment of the risks of use of their services for the purpose of online child sexual abuse, as required by this Regulation.

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available ***number-independent*** interpersonal communications services should take reasonable ***specific*** measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers ***should consider, in particular, the negative impacts of such measures on the fundamental rights enshrined in the Charter on all parties involved and adopt appropriate and proportionate measures to protect children, for example by designing their online interfaces or parts thereof with the highest level of privacy, safety and security for children by default***

where appropriate or adopting standards for protection of children, or participating in codes of conduct for protecting children. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) ***2022/2065*** ~~*…/…* [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~ may consider to which extent mitigation measures adopted to comply with that obligation, which may include targeted measures to protect the rights of the child, ~~including age verification and parental control tools~~, may also serve to address the risk identified in the specific risk assessment pursuant to this Regulation, and to which extent further targeted mitigation measures may be required to comply with this Regulation.

(***16b***) ***Providers seeking to assess the age of child users as part of measures to ensure the effective protection of children online should process children's data in a privacy preserving and secure manner and in accordance with Regulation EU 2016/679, in particular during sign up. The measures and methods used should not lead to excessive data processing, profiling or identification of users, nor the processing of biometric or biometric-based data, should not allow data to be used for any other purpose and minimize the data shared with the provider or any other third party to the maximum extent possible in accordance with Regulation EU 2016/679. Self-reporting with minimal checks could be appropriate in many cases, in particular if the provider offers services with an age-appropriate design where children of all relevant age groups are recommended content that is likely to interest them. Methods for assessing the age of users should respect the rights of the child and take particular regard of the risks for exclusion from the online world for children that are unable to comply with the age assessment requirements.***

(16c) Parental control features and functionalities shall be limited to allowing parents or guardians to prevent children from accessing platforms or services that are inappropriate for their age, or to help prevent them from being exposed to content that is inappropriate; These measures shall be in line the Regulation 2016/679 and the Convention on the Rights of the Child and respect the integrity and safety of the device and shall not allow unauthorised access or control by third parties.

(17) To allow for innovation and ensure proportionality and technological neutrality, no exhaustive list of the compulsory mitigation measures should be established. Instead, providers should be left a degree of flexibility to design and implement ***specific*** measures tailored to the risk identified and the characteristics of the services they provide and the manners in which those services are used ***in line with children's increasing need for autonomy and rights to access to information and freedom of expression as they grow***. In particular, providers are free to design and implement, in accordance with Union law, measures based on their existing practices to detect online child sexual abuse in their services***. For example, providers of hosting services and providers of number-independent interpersonal communications services should take the*** necessary ***targeted measures and tools to adapt their online interface and protect child users from solicitation, including through increased user information and awareness-raising tools, parental control tools or mechanisms aimed at helping children signal abuse or obtain support*** ~~and indicate as part of the risk reporting their willingness and preparedness to eventually being issued a detection order under this Regulation, if deemed necessary by the competent national authority~~. ***Specific measures could include providing technical measures and tools that allow users to manage*** their ***own privacy visibility, reachability and safety, such as mechanisms for users to block or mute other users, mechanisms that ask for confirmation before displaying certain content, tools that prompt or warn users***.

(17 a) Fundamental rights in the digital sphere have to be guaranteed to the same extent as in the offline world. Safety and privacy need to be ensured, amongst others through end-to-

end encryption in private online communication and the protection of private content against any kind of general or targeted surveillance, be it by public or private actors. End-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. Any restrictions of encryption could potentially be abused by malicious third parties. In order to ensure effective consumer trust, nothing in this Regulation should be interpreted as prohibiting providers of information society services from providing their services applying encryption, restricting or undermining such encryption in the sense of being detrimental to users' expectations of confidential and secure communication services. Member States should not prevent providers of information society services from providing their services applying encryption, considering that such encryption is essential for trust in and security of the digital services, and effectively prevents unauthorised third party access.

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on mitigation measures. Therefore, providers of hosting services and providers of publicly available ***number-independent*** interpersonal communications services should, when designing and implementing the mitigation measures, give importance ~~not only~~ to ensuring their effectiveness, ~~but also~~ ***and*** to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which mitigation measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate mitigation measures, providers should at least duly consider the possible measures listed in this Regulation, as well as, where appropriate, other measures such as those based on industry best practices, including as established through self-regulatory cooperation, and those contained in guidelines from the Commission. ***Those mitigation measures should always be the least intrusive option possible, with the level of intrusiveness increasing only if justified by lack of effectiveness or implementation of the less intrusive option.*** When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

(19) In the light of their role as intermediaries facilitating access to software applications that may be misused for online child sexual abuse, providers of software application stores should be made subject to ***specific*** obligations ***under this Regulation*** ~~to take certain reasonable measures assess and mitigate that risk,. The providers should make that assessment in a diligent manner, making efforts that are reasonable under the given circumstances, having regard inter alia to the nature and extent of that risk as well as their financial and technological capabilities and size, and cooperating with the providers of the services offered through the software application where possible~~.

Batch 3

Compromise amendment on Chapter II, Section 1
Compromise amendment replacing all relevant amendments, including AM (390, 391, 392, 393, 394, 87, 398, 397, 399, 400, 402, 403, 88, 89, 405, 406, 407, 409, 90, 411, 91, 413, 414, 92, 415, 416, 418, 93, 419, 422, 95, 423, 96, 426, 427, 97, 428, 429, 430, 98, 431, 432, 99, 434, 435, 100, 101, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 447, 450, 105, 451, 106, 452, 453, 108, 458, 460, 110, 464, 467, 112, 113, 114, 472, 473, 115, 477, 117, 118, 484, 485, 489, 490, 497, 499, 502, 120, 507, 121, 122, 509, 123, 512, 513, 515, 124, 518, 125, 519, 520, 521, 523, 524, 126, 525, 526, 527, 528, 529, 530, 532, 198, 199, 17, 200, 18, 201, 202, 19, 203, 204, 20, 205, 206, 21, 207, 208, 209, 22, 210, 211, 212, 213, 23, 214, 215 and 24)

Article 7

Issuance of detection orders

1. ***As a last resort after all the measures in Article 3, 4 and 5 have been exhausted***, the ~~Coordinating Authority of establishment shall have the power to request the~~ competent judicial authority ***may issue, following a request by the Coordinating Authority of*** the Member State that designated it ~~or another independent administrative authority of that Member State to issue~~, a ***necessary and proportionate*** detection order requiring a provider of hosting services or a provider of ***number-independent*** interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 ***taking into account information on the specific user, specific group of users, or a specific incident*** to detect ***for a limited period of time and for the sole purpose of detecting*** online ***known or new*** child sexual abuse on a specific service ***without jeopardising the security of communications, as reffered to in Article 6a.***

As a general rule, the detection order shall be directed to the providers of hosting services and number-independent interpersonal communications services that can reasonably be expected to have the technical and operational ability to act.

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~~ ***all*** 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 ***and the actions required by the detection order are strictly neccessary, justified and proportionate*** it shall:

   (a) establish a draft request ***to the competent judicial authority of the Member State that designated it*** for the issuance of a detection order, specifying ***the grounds upon which the request is based***, ***the territorial, personal and the material scope and the duration of the order, as well as*** ~~and~~ ***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 ***relevant*** 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;

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

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

(a) draft an implementation plan setting out the measures it envisages taking to execute the intended detection order ***limited to the personal, territorial and material scope of the order and*** including detailed information regarding the envisaged technologies and safeguards ***and if any, the negative impacts and safeguards on the rights of all parties involved;***

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

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

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

Where, having regard to the implementation plan of the provider and ***taking utmost account of*** the opinion of the data protection authority, that Coordinating Authority continues to be of the view that the conditions of paragraph 4 have met, it shall submit the request for the issuance of the detection ***order***, adjusted where appropriate, to the competent judicial authority ~~or independent administrative authority~~. It shall attach the implementation plan of the provider and the opinions of the EU Centre and the data protection authority to that request.

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

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

(b) the reasons for issuing the detection order and 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 ***and without jeopardising the security of communications as reffered to in Article 6a***.

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, ***implications for the rights and legitimate interest of all parties concerned, and the respect of fundamental rights enshrined in the Charter,*** in particular:

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

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

(c) the views and the implementation plan and, ***where relevant the technical feasibility*** of the provider submitted in accordance with paragraph 3;

(d) the opinions of the EU Centre and of the data protection authority submitted in accordance with paragraph 3 ***and, where applicable, the opinion of the Coordinating Authority issued in accordance with Article 5(4b).***

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

5. As regards detection orders concerning the dissemination of know ***or 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, despite any~~ the mitigation measures that the provider may have taken or will take, ***have insufficient material impact on limiting the systemic risk and*** that the service is ***being*** used ***by suspect or suspects***, to an appreciable extent for the dissemination of known child sexual abuse material;

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

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

~~(a) it is likely that, despite any mitigation measures that the provider may have 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 where one of the users is a child user.~~

8. The Coordinating Authority of establishment when requesting the issuance of detection orders, and the competent judicial ~~or independent administrative~~ authority when issuing the detection order***,*** shall target and specify it in such a manner that the negative consequences referred to in paragraph 4, first subparagraph, point (b), remain limited to what is strictly necessary ***and proportionate*** to effectively address the ~~significant~~ ***systemic*** risk referred to in point (a) thereof, ***while not jeopardising the secuirty of communication as reffered to in Article 6a.***

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

In particular, they shall ensure that:

(a) where that risk is limited to an identifiable part or component of a service, the required measures are only applied in respect of that part or component;

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

(c) subject to paragraph 9, the period of application remains limited to what is strictly necessary ***and proportionate;***

(ca) under no circumstances shall the detection order require providers of interpersonal communications services to access the content of communications or make provision for methods to access these communications or to compromise their encryption;

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

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

The period of application of detection orders concerning the dissemination of known ~~or new~~ child sexual abuse material ***shall be proprotionate, taking all relevant factors into account*** and not exceed 24 months ~~and that of detection orders concerning the solicitation of children shall not exceed 12 months~~.

Article 8

Additional rules regarding detection orders

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

(a) information regarding the ***targeted and proportionate*** measures to be taken to execute the detection order, including the ***specific user or group of users must concern,*** indicators to be used and the safeguards to be provided for, including the reporting requirements set pursuant to Article 9(3) and, where applicable, any additional safeguards ~~as referred to in Article 7(8)~~ ***to protect the rights and legitimate interests of all users affected by the detection order***;

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

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

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

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

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

(g) a sufficiently detailed statement of reasons explaining why the detection order is issued, ***including grounds justifying the order***;

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

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

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

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

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

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

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

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

Article 8 a

Notification mechanism

1. Without prejudice to Article 16 of Regulation (EU) 2022/2065, relevant information society service providers shall establish mechanisms or use existing mechanisms that allow users to notify them of the presence on their service of specific content or activities that the user considers to be potential child sexual abuse, in particular of new child sexual abuse material and solicitation of children for sexual purposes.

2. Those mechanisms shall be easy to access, user- and child-friendly, and allow for the submission of the notification exclusively by electronic means.

3. Providers shall ensure that such notices are processed effectively without undue delay.

4. Where the notification contains an electronic contact information of the individual or entity that submitted it, the provider of the relevant information society services shall, without undue delay, send a confirmation of receipt of the notification and inform the user of its decision and actions taken in relation to the notification.

Article 9

Redress, information, reporting and modification of detection orders

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

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

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

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

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

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

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

Article 10

Technologies and safeguards

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

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

3. The technologies shall be:

(a) effective ***in collecting evidence and*** detecting the dissemination of known or new child sexual abuse material ***online*** ~~or the solicitation of children, as applicable~~;

(b) ***able to ensure the processing is limited to what is strictly necessary and*** not be able to extract any other information from the relevant communications than the information strictly necessary ***for the purpose of*** ~~to~~ ***detecting, reporting and removing*** ~~using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new~~ child sexual abuse material ~~or the solicitation of children, as applicable~~;

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

(d) sufficiently reliable ***and being able to distinguish between lawful and unlawful content without the need for any independent human assessment.***

(da) ~~in that they~~ limit**ing** to the maximum extent possible the rate of errors regarding the detection ***and where such errors occur, their consequences are rectified without delay.***

(da) ***respecting the confidentiality of communications enshrined in Article 7 of the Charter of Fundamental Rights of the European Union and without jeopardising the security of communication as reffered to in Article 6a;***

4. The ~~provider~~ ***issuing authority*** shall take all the necessary measures to ensure that the technologies ***specified in detection orders*** and indicators, ***are proportionate and strictly necessary*** ~~as well as the processing of personal data and other data in connection thereto, are used~~ for the sole purpose of detecting the dissemination of known ~~or new~~ child sexual abuse material ~~or the solicitation of children~~, ~~as applicable, insofar as strictly necessary to issue execute the detection orders addressed to them~~;

4a. The provider shall:

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

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

(ca) ensure effective internal procedures and safeguards to prevent general monitoring, surveillance and espionage.

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

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

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

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

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

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

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

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

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

Article 11

Guidelines regarding detection obligations

The Commission, in cooperation with the Coordinating Authorities and the EU Centre and after having conducted a public consultation, ***shall be empwered to adopt a*** ~~may issue~~ ***delegated act*** ~~guidelines~~ on the application of Articles 7 to 10, having due regard in particular to relevant technological developments and the manners in which the services covered by those provisions are offered and used.

Relevant recitals (20, 21, 22-28)

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures are deemed insufficient to limit the risk of use of a certain service for the purpose of online child sexual abuse, the Coordinating Authorities designated by Member States under this Regulation should be empowered to request ***as a last resort*** the issuance of detection orders. In order to avoid any undue interference with fundamental rights and to ensure proportionality, that power should be subject to a carefully balanced set of ***targeted*** limits and safeguards. For instance, considering that child sexual abuse material tends to be disseminated through hosting services and publicly available ***number-independent*** interpersonal communications services, ~~and that solicitation of children mostly takes place in publicly available interpersonal communications services~~, it should only be possible to address detection orders to providers of such services ***taking into account information on the ~~in relation to~~ specific suspects, or specific group of suspects or a specific incident.***

(21) Furthermore, as parts of those limits and safeguards, detection orders should only be issued after a diligent and objective assessment leading to the finding of a ~~significant~~ ***systemic*** risk of the specific service concerned being used for a given type of online child sexual abuse covered by this Regulation. One of the elements to be taken into account in this regard is the likelihood that the service is used to an appreciable extent, that is, beyond isolated and relatively rare instances, for such abuse. The criteria should vary so as to account of the different characteristics of the various types of online child sexual abuse at stake and of the different characteristics of the services used to engage in such abuse, as well as the related different degree of intrusiveness of the measures to be taken to execute the detection order.

(22) However, the finding of such a ~~significant~~ ***systemic*** risk should in itself be insufficient to justify the issuance of a detection order, given that in such a case the order might lead to disproportionate negative consequences for the rights and legitimate interests of other affected parties, in particular for the exercise of users' fundamental rights. Therefore, it should be ensured that detection orders can be issued only after the Coordinating Authorities and the competent judicial authority ~~or independent administrative authority~~ having objectively and diligently assessed, identified and weighted, on a case-by-case basis, not only the likelihood and seriousness of the potential consequences of the service being misused for the type of online child sexual abuse at issue, but also the ***specific results anticipated by the measure, the*** likelihood and seriousness of any potential negative consequences for other parties affected, ***including the users of the service***. With a view to avoiding the imposition of excessive burdens, the assessment should also take account of the financial and technological capabilities and size of the provider concerned.

(23) In addition, to avoid undue interference with fundamental rights and ensure proportionality, when it is established that those requirements have been met and a detection order is to be issued, it should still be ensured that the detection order is targeted***, justified, proportionate, limited in time*** and ***territorial scope and it is*** ~~specified~~ ***specific enough*** so as to ensure that any such negative consequences for affected parties do not go beyond what is strictly necessary to effectively address the ~~significant~~ ***systemic*** risk identified. This should concern, in particular, a limitation to an identifiable part or component of the service ~~where possible without prejudice to the effectiveness of the measure~~, such as specific types of channels of a publicly available ***number-independent*** interpersonal communications service, or to specific users or specific groups of users, to the extent that they can be taken in isolation and ***be reasonably suspected of distributing child sexual abuse material or to obtain information to effectively investigate a specific incident and collect the information required to assess the existence of criminal offence*** for the purpose of detection, as well as the specification of the safeguards additional to the ones already expressly specified in this Regulation, such as independent auditing, the provision of additional information or access to data, or reinforced human oversight and review, and the further limitation of the duration of application of the detection order that the Coordinating Authority deems necessary. To avoid unreasonable or disproportionate outcomes, such requirements should be set after an objective and diligent assessment conducted on a case-by-case basis.

(23a) Considering the particular characteristics of the services concerned and the corresponding need to make the providers thereof subject to certain specific obligations, it is necessary to specify that given the specific nature of cloud computing services and web-hosting services when serving as infrastructure, imposing on them the same obligations as for any hosting service provider might have a broader impact on users of cloud-hosted services. The detection order should therefore not be directed to cloud computing services and directed to the providers of hosting services and providers of (number-independent) interpersonal communications that can reasonably be expected to have the technical and operational ability to act against specific child abuse material.

(23 b) Monitoring private communications of all users of a number-independent interpersonal communications service in a general and indiscriminate manner is likely to infringe on the essence of their fundamental rights and the prohibition of general monitoring. ***T****he detection order shall be targeted against specific user or specific group of users suspected of distributing child sexual abuse material, or to specific person or persons the authority intends to investigate, or to obtain information to effectively investigate a case and collect the information required to assess the existence of criminal offence.*

(24) The competent judicial authority ~~or the competent independent administrative authority, as applicable in accordance with the detailed procedural rules set by the relevant Member State,~~ should ***have the data*** ~~be in a position~~ to take a well-informed decision on requests for the issuance of detections orders. That is of particular importance to ensure the necessary fair balance of the fundamental rights at stake and a consistent approach~~, especially in connection to detection orders concerning the solicitation of children~~. ***In particular, territorial scope of the detection orders should be clearly set out on the basis of the applicable law enabling the issuance of the order and should not exceed what is strictly necessary to achieve its objectives. In a cross-border context, the effect of the detection order should in principle be limited to the territory of the issuing Member State, unless if the judicial authority considers that the rights at stake require a wider territorial scope, in accordance with Union and international law, namely the principle of proportionality. Moreover, the duration of application of the detection order should be limited in time to what is strictly necessary and proportionate.*** ~~Therefore,~~ ***Furthermore,*** a procedure should be provided for that allows the providers concerned, the EU Centre on Child Sexual Abuse established by this Regulation ('EU Centre') and, where so provided in this Regulation, the competent data protection authority designated under Regulation (EU) 2016/679 to provide their views on the measures in question. They should do so ***without undue delay*** ~~as soon as possible~~, having regard to the important public policy objective at stake and the need to act without undue delay to protect children. In particular, data protections authorities should do their utmost to avoid extending the time period set out in Regulation (EU) 2016/679 for providing their opinions in response to a prior consultation. Furthermore, they should normally be able to provide their opinion well within that time period in situations where the European Data Protection Board has already issued guidelines regarding the technologies that a provider envisages deploying and operating to execute a detection order addressed to it under this Regulation.

~~(25) Where new services are concerned, that is, services not previously offered in the Union, the evidence available on the potential misuse of the service in the last 12 months is normally non-existent. Taking this into account, and to ensure the effectiveness of this Regulation, the Coordinating Authority should be able to draw on evidence stemming from comparable services when assessing whether to request the issuance of a detection order in respect of such a new service. A service should be considered comparable where it provides a functional equivalent to the service in question, having regard to all relevant facts and circumstances, in particular its main characteristics and functionalities, the manner in which it is offered and used, the user base, the applicable terms and conditions and risk mitigation measures, as well as the overall remaining risk profile.~~

(26) The measures taken by providers of hosting services and providers of publicly available ***number-independent*** interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be

understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. ***In particular, any action taken by a provider pursuant to the reception of a detection order should also be strictly targeted, in the sense that it should serve to remove or disable access to the specific items of information considered to constitute child sexual abuse material, without unduly affecting the freedom of expression and of information of the user***. ~~That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children.~~ When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties ***or states***, and thus to avoid undermining the security and confidentiality of the communications of users. In particular, ***providers should ensure effective internal procedures and safeguards to prevent general monitoring, surveillance and foreign espionage***

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers ~~detection~~ ***approved*** technologies that they may choose to use, on a free-of-charge basis, for the sole purpose of executing the detection orders addressed to them. The European Data Protection Board should be consulted on those technologies and the ways in which they should be best deployed to ensure compliance with applicable rules of Union law on the protection of personal data. The advice of the European Data Protection Board should be taken into account by the EU Centre when compiling the lists of available technologies and also by the Commission when preparing guidelines regarding the application of the detection obligations. The providers may operate the technologies made available by the EU Centre or by others or technologies that they developed themselves, as long as they meet the requirements of this Regulation.

(28) With a view to constantly assess the performance of the detection technologies and ensure that they are sufficiently ***accurate and*** reliable, as well as to identify false positives and ***false negative to*** avoid to the extent erroneous reporting to the EU Centre, providers should ensure ***adequate*** human oversight and, where necessary, human intervention, adapted to the type of detection technologies and the type of online child sexual abuse at issue. Such oversight should include regular assessment of the rates of false negatives and ***false*** positives generated by the technologies, based on an analysis of anonymised representative data samples. ~~In particular where the detection of the solicitation of children in publicly available interpersonal communications is concerned, service providers should ensure regular, specific and detailed human oversight and human verification of conversations identified by the technologies as involving potential solicitation of children~~.

Batch 4

Compromise amendment on Chapter II, Section 3
Compromise amendment replacing all relevant amendments, including AMs 533, 534, 127, 535, 536, 537, 538, 539, 540, 541, 542, 543, 128, 544, 545, 546, 547, 548, 549, 129, 550, 551, 552, 130, 216, 217, 25 and 218)

Article 12
Reporting obligations

1. Where a provider of hosting services or a provider of ***number-independent*** interpersonal communications services ~~becomes aware~~ ***obtains*** in any manner other than through a removal order issued in accordance with this Regulation ***actual knowledge of online child sexual abuse content on its services, or becomes aware of facts or circumstances from which the existence of such content is apparent,*** ~~of any information indicating potential online child sexual abuse on its services,~~ it shall promptly submit a report ***thereon to the competent law enforcement authorities and*** to the EU Centre in accordance with Article 13 ***and it shall expeditiously remove such content.*** 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 ***request from the competent law enforcement authorities or the EU Centre an authorisation to inform the user concerned*** ~~inform the user concerned~~***, which shall reply without undue delay, at maximum within two days. The notification to the user shall include*** providing information on the main content of the report, on the manner in which the provider has become aware of the potential child sexual abuse concerned, on the follow-up given to the report insofar as such information is available to the provider and on the user's possibilities of redress, including on the right to submit complaints to the Coordinating Authority in accordance with Article 34.

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

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

3. The provider shall establish and operate an ***easily found,*** accessible, ***effective,*** age-appropriate and user-friendly mechanism that allows users to ***easily*** flag to the provider potential online child sexual abuse on the service, ***including self-reporting of self-generated content. Those mechanisms shall allow for the submission of notices anonymously and*** ~~***exclusively***~~ ***by electronic means and for a clear indication of the exact electronic location of that information. The providers shall process any notices that they receive under the mechanisms referred to in this paragraph in a timely, diligent, non-arbitrary and objective manner.***

Article 13
Specific requirements for reporting

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

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

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

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

   (d) ~~all~~ available/***relevant*** data other than content data related to the potential online child sexual abuse, ***in line with Regulation (EU) 2016/679***;

   (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) ***a clear indication of the exact electronic location of the child sexual abuse material and, where necessary, additional information enabling the identification of such material;*** ~~information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address~~;

   (g) information concerning the identity of ~~any user~~ ***users, suspected to be*** involved in the potential online child sexual abuse; ***the report shall not contain information about the identity of the person to whom the content relates;***

   (h) ***an indication*** whether ~~the provider has also reported, or will also report,~~ the potential online child sexual abuse ***was reported*** 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, ***information on the actions taken by the provider and*** whether the provider has removed or disabled access to the material;

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

   (j a) information on how the provider has become aware of the reported online child sexual abuse;

   (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.

Relevant recitals (29, 29a):

(29) Providers of hosting services and providers of publicly available interpersonal communications services are uniquely positioned to ***address*** ~~detect potential~~ online child sexual abuse involving their services. The information that they may obtain when offering their services ~~is often indispensable~~ ***may help*** to effectively investigate and prosecute child sexual abuse offences. Therefore, they should be required to report on potential online child sexual abuse on their services, whenever they ***obtain actual knowledge or awareness of illegal activities or illegal content*** ~~become aware of it~~, that

is, when there are reasonable grounds to believe that a particular activity may constitute online child sexual abuse. Where such reasonable grounds exist, doubts about the potential victim's age should not prevent those providers from submitting reports. In the interest of effectiveness, it should be immaterial in which manner they obtain such awareness. Such awareness could, for example, be obtained through the execution of detection orders, information flagged by users or organisations acting in the public interest against child sexual abuse, or activities conducted on the providers' own initiative ***or through notices submitted to it by individuals in accordance with this Regulation in so far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content***. Those providers should report a minimum of information, as specified in this Regulation, for competent law enforcement authorities to be able to assess whether to initiate an investigation, where relevant, and should ensure that the reports are as complete as possible before submitting them.

(***29 a) It is important that relevant information society service providers, regardless of their size, put in place easily accessible and user and child-friendly notification mechanisms that facilitate the notification of child sexual abuse online, in particular new child sexual abuse material and solicitation. Such mechanisms should be clearly identifiable, located close to the information in question and easy to find and use by children. Having regard to the need to take due account of the fundamental rights guaranteed under the Charter of all parties concerned, any action taken by a provider after receiving a notification should be strictly targeted, in the sense that it should serve to report, remove or disable access to the specific child sexual abuse material, without unduly affecting the freedom of expression and of information of the recipients of the service. Micro and small sized enterprises should get support from the EU Centre to build up a corresponding mechanism.***

Batch 5

Compromise amendment on Chapter II, Section 4
Compromise amendment replacing all relevant amendments, including AM (553, 554, 131, 555, 556, 557, 132, 558, 133, 559, 560, 561, 562, 563, 134, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 26, 219, 27 and 220)

Article 14
Removal orders

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

2. The provider shall execute the removal order as soon as possible and in any event ***within the timeframe indicated in the order or*** within 24 hours of receipt thereof. ***For micro, small and medium enterprises, including open source providers, the removal order shall allow additional time, proportionate to the size and the resources of the provider.***

2 a. Before issuing a removal order, the judicial authorities of establishment shall take all reasonable steps to ensure that implementing the order will not interfere with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 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.

1a. If the order is modified or repealed as a result of a redress procedure, the provider shall as soon as possible take the necessary measures to comply with the modified or repealed order.

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 to the Coordinating Authority of establishment. The Coordinating Authority of establishment shall then, without undue delay, transmit a copy thereof to all other Coordinating Authorities through the system established in accordance with Article 39(2).

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

   In such a case:

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

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

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

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

Relevant recitals (30- 32)

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial authorities ~~or independent administrative authorities~~ to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences. ***Parents or guardians should have equal legal standing to request removal in the instance that the child is not able to do so due to age or other limitations.***

(31) The rules of this Regulation should not be understood as affecting the requirements regarding removal orders set out in Regulation (EU) ***2022/2065*** ~~*…/…* [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~.

(32) The obligations of this Regulation do not apply to providers of hosting services that do not offer their services in the Union. However, such services may still be used to disseminate child sexual abuse material to or by users in the Union, causing harm to children and society at large, even if the providers' activities are not targeted towards Member States and the total numbers of users of those services in the Union are limited. For legal and practical reasons, it may not be reasonably possible to have those providers remove or disable access to the material, not even through cooperation with the competent authorities of the third country where they are established. Therefore, in line with existing practices in several Member States, it should be possible to require providers of internet access services to take reasonable measures to block the access of users in the Union to the material.

Batch 6

Compromise amendment on Chapter II, Section 5/6
Compromise amendment replacing all relevant amendments, including AMs (575, 576, 577, 135, 578, 579, 136, 137, 138, 221, 222, 28, 223, 29, 224 and 30)

Article 16
Blocking orders

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

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

   To that end, it shall, where appropriate:

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

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

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 blocking order, where it considers that the following conditions are met:

   (a) there is evidence of the service having been used during the past 12 months, to an appreciable extent, for accessing or attempting to access the 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 that material, 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) the uniform resource locators indicate, in a sufficiently reliable manner, child sexual abuse material;

(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 blocking order, shall:

(a) 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 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, the Coordinating Authority shall, where necessary and at least once every year, assess whether any substantial changes to the grounds for issuing the blocking orders occurred and, in particular, whether the conditions of paragraph 4 continue to be met.

That 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, where necessary in the light of the outcome of that assessment or to take account of justified requests or the reports referred to in Article 18(5) and (6), respectively. The provisions of this Section shall apply to such requests, *mutatis mutandis*.

Article 17

Additional rules regarding blocking orders

1. The Coordinating Authority of establishment shall issue the blocking orders referred to in Article 16 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);

(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 specific service in respect of which the detection order is issued;

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

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

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

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

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 Coordinating Authority of establishment, using the template set out in Annex VIII.

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

Article 18

Redress, information and reporting of blocking orders

1. Providers of internet access services that have received a blocking order, as well as users who provided or were prevented from accessing a specific item of material indicated by the uniform resource locators in execution of such orders, shall have a right to effective redress. That right shall include the right to challenge the blocking order before the courts of the Member State of the competent judicial authority or independent administrative authority that issued the blocking order.

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

For the purpose of the first subparagraph, a blocking 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. The provider shall establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it, within a reasonable timeframe, complaints about alleged infringements of its obligations under this Section. It shall process such complaints in an objective, effective and timely manner.

4. Where a provider prevents users from accessing the uniform resource locators pursuant to a blocking order issued in accordance with Article 17, it shall take reasonable measures to inform the users of the following:

   (a) the fact that it does so pursuant to a blocking order;

   (b) the reasons for doing so, providing, upon request, a copy of the blocking order;

   (c) the users' right of judicial redress referred to in paragraph 1, their rights to submit complaints to the provider through the mechanism referred to in paragraph 3 and to the Coordinating Authority in accordance with Article 34, as well as their right to submit the requests referred to in paragraph 5.

5. The provider and the users referred to in paragraph 1 shall be entitled to request the Coordinating Authority that requested the issuance of the blocking order to assess whether users are wrongly prevented from accessing a specific item of material indicated by uniform resource locators pursuant to the blocking order. The provider shall also be entitled to request modification or revocation of the blocking order, where it considers it necessary due to substantial changes to the grounds for issuing the blocking orders that occurred after the issuance thereof, in particular substantial changes preventing the provider from taking the required reasonable measures to execute the blocking order,

   The Coordinating Authority shall, without undue delay, diligently assess such requests and inform the provider or the user submitting the request of the outcome thereof. Where it considers the request to be justified, it shall request modification or revocation of the blocking order in accordance with Article 16(7) and inform the EU Centre.

6. Where the period of application of the blocking order exceeds 24 months, the Coordinating Authority of establishment shall require the provider to report to it on the measures taken to execute the blocking order, including the safeguards provided for, at least once, halfway through the period of application.

Section 6
Additional provisions

Article 19

Liability of providers

~~Providers of relevant information society services shall not be liable for child sexual abuse offences solely because they carry out, in good faith, the necessary activities to comply with the requirements of this Regulation, in particular activities aimed at detecting, identifying, removing, disabling of access to, or reporting online child sexual abuse in accordance with those requirements.~~

Providers of relevant information society services shall not be liable for child sexual abuse offences solely because they carry out, in good faith ***and in a diligent manner, voluntary own-initiative investigations or take other measures*** ~~the necessary activities~~ to comply with the requirements of this Regulation, in particular activities aimed at detecting, identifying,

removing, disabling of access to, blocking or reporting online child sexual abuse in accordance with those requirements.

Article 20
Victims' right to information

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

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

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

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

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

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

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

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

   (b) the date of the report;

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

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

Article 21
Victims' right of assistance and support for removal

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

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

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

3. The requests referred to in paragraphs 1 and 2 shall indicate the relevant item or items of child sexual abuse material.

4. The EU Centre's support referred to in paragraph 2 shall include, as applicable:

(a) support in connection to requesting the provider's assistance referred to in paragraph 1;

(b) verifying whether the provider removed or disabled access to that item or those items, including by conducting the searches referred to in Article 49(1);

(c) notifying the item or items of known child sexual abuse material depicting the person to the provider and requesting removal or disabling of access, in accordance with Article 49(2);

(d) where necessary, informing the Coordinating Authority of establishment of the presence of that item or those items on the service, with a view to the issuance of a removal order pursuant to Article 14.

Article 22
Preservation of information

1. Providers of hosting services and providers of interpersonal communications services shall preserve the content data and other data processed in connection to the measures taken to comply with this Regulation and the personal data generated through such processing, only for one or more of the following purposes, as applicable:

(a) executing a detection order issued pursuant to Article 7, or a removal order issued pursuant to Article 14;

(b) reporting potential online child sexual abuse to the EU Centre pursuant to Article 12;

(c) blocking the account of, or suspending or terminating the provision of the service to, the user concerned;

(d) handling users' complaints to the provider or to the Coordinating Authority, or the exercise of users' right to administrative or judicial redress, in respect of alleged infringements of this Regulation;

(e) responding to requests issued by competent law enforcement authorities and judicial authorities in accordance with the applicable law, with a view to providing them with the necessary information for the prevention, detection, investigation or prosecution of child sexual abuse offences, insofar as the content data and other data relate to a report that the provider has submitted to the EU Centre pursuant to Article 12.

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

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

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

Providers shall ensure that the information referred to in paragraph 1 is preserved in a secure manner and that the preservation is subject to appropriate technical and

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

Article 23

Points of contact

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

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

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

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

Article 24

Legal representative

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

2. The legal representative shall reside or be established in one of the Member States where the provider offers its services.

3. The provider shall mandate its legal representatives to be addressed in addition to or instead of the provider by the Coordinating Authorities, other competent authorities of the Member States and the Commission on all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation, including detection orders, removal orders and blocking orders.

4. The provider shall provide its legal representative with the necessary powers and resources to cooperate with the Coordinating Authorities, other competent authorities of the Member States and the Commission and comply with the decisions referred to in paragraph 3.

5. The designated legal representative may be held liable for non-compliance with obligations of the provider under this Regulation, without prejudice to the liability and legal actions that could be initiated against the provider.

6. The provider shall notify the name, ***postal*** address, the electronic mail address and telephone number of its legal representative designated pursuant to paragraph 1 to the Coordinating Authority in the Member State where that legal representative resides or is established, and to the EU Centre. They shall ensure that that information is up to date and publicly available.

7. The designation of a legal representative within the Union pursuant to paragraph 1 shall not amount to an establishment in the Union.

Relevant recitals (33-42):

(33) In the interest of consistency, efficiency and effectiveness and to minimise the risk of circumvention, such blocking orders should be based on the list of uniform resource locators, leading to specific items of verified child sexual abuse, compiled and provided centrally by the EU Centre on the basis of diligently verified submissions by the relevant authorities of the Member States. In order to avoid the taking of unjustified or disproportionate measures, especially those that would unduly affect the fundamental rights at stake, notably, in addition to the rights of the children, the users' freedom of expression and information and the providers' freedom to conduct a business, appropriate limits and safeguards should be provided for. In particular, it should be ensured that the burdens imposed on the providers of internet access services concerned are not unreasonable, that the need for and proportionality of the blocking orders is diligently assessed also after their issuance and that both the providers and the users affected have effective means of judicial as well as non-judicial redress.

(34) ***The legal certainty provided by the horizontal framework set out by Regulation (EU) 2022/2065 as regards conditional exemptions from liability for providers of intermediary services, should be preserved. The rules on liability of providers of intermediary services set out in this Regulation should therefore be consistent with Regulation (EU) 2022/2065 and only establish when the provider of intermediary services concerned cannot be held liable in relation to illegal content provided by the recipients of the service. Those rules should not be understood to provide a positive basis for establishing when a provider can be held liable, which is for the applicable rules of Union or national law to determine. In order to allow for an efficient reporting system and*** considering that acquiring, possessing, knowingly obtaining access and transmitting child sexual abuse material constitute criminal offences under Directive 2011/93/EU, it is necessary to exempt providers of relevant information society services from criminal liability when they are involved in such activities, ***including when carrying out voluntary own-initiative investigations, or taking other measures,*** insofar as their activities remain strictly limited to what is needed for the purpose of complying with their obligations ***in compliance with Union law, including*** this Regulation and they act in good faith ***and in a diligent manner***

(35) The dissemination of child sexual abuse material is a criminal offence that affects the rights of the victims depicted. Victims should therefore have the right to obtain, upon request, from the EU Centre yet via the Coordinating Authorities, relevant information if known child sexual abuse material depicting them is reported by providers of hosting services or providers of publicly available interpersonal communications services in accordance with this Regulation.

(36) Given the impact on the rights of victims depicted in such known child sexual abuse material and the typical ability of providers of hosting services to limit that impact by helping ensure that the material is no longer available on their services, those providers should assist victims who request the removal or disabling of access of the material in question. That assistance should remain limited to what can reasonably be asked from the provider concerned under the given circumstances, having regard to factors such as the content and scope of the request, the steps needed to locate the items of known child

sexual abuse material concerned and the means available to the provider. The assistance could consist, for example, of helping to locate the items, carrying out checks and removing or disabling access to the items. Considering that carrying out the activities needed to obtain such removal or disabling of access can be painful or even traumatic as well as complex, victims should also have the right to be assisted by the EU Centre in this regard, via the Coordinating Authorities.

(37) To ensure the efficient management of such victim support functions, victims should be allowed to contact and rely on the Coordinating Authority that is most accessible to them, which should channel all communications between victims and the EU Centre.

(38) For the purpose of facilitating the exercise of the victims' right to information and of assistance and support for removal or disabling of access, victims should be allowed to indicate the relevant item or items of child sexual abuse material in respect of which they are seeking to obtain information or removal or disabling of access either by means of providing the image or images or the video or videos themselves, or by means of providing the uniform resource locators leading to the specific item or items of child sexual abuse material, or by means of any other representation allowing for the unequivocal identification of the item or items in question.

(39) To avoid disproportionate interferences with users' rights to private and family life and to protection of personal data, the data related to instances of potential online child sexual abuse should not be preserved by providers of relevant information society services, unless and for no longer than necessary for one or more of the purposes specified in this Regulation and subject to an appropriate maximum duration. As those preservation requirements relate only to this Regulation, they should not be understood as affecting the possibility to store relevant content data and traffic data in accordance with Directive 2002/58/EC or the application of any legal obligation to preserve data that applies to providers under other acts of Union law or under national law that is in accordance with Union law.

(40) In order to facilitate smooth and efficient communications by electronic means, including, where relevant, by acknowledging the receipt of such communications, relating to matters covered by this Regulation, providers of relevant information society services should be required to designate a single point of contact and to publish relevant information relating to that point of contact, including the languages to be used in such communications. ***The single point of contact should allow for direct communication with the users of the service for issues related to this Regulation.*** In contrast to the provider's legal representative, the point of contact should serve operational purposes and should not be required to have a physical location. Suitable conditions should be set in relation to the languages of communication to be specified, so as to ensure that smooth communication is not unreasonably complicated. For providers subject to the obligation to establish a compliance function and nominate compliance officers in accordance with Regulation (EU) ***2022/2065*** ~~*.../...* [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~, one of these compliance officers may be designated as the point of contact under this Regulation, in order to facilitate coherent implementation of the obligations arising from both frameworks.

(41) In order to allow for effective oversight and, where necessary, enforcement of this Regulation, providers of relevant information society services that are not established in a third country and that offer services in the Union should have a legal representative in the Union and inform the public and relevant authorities about how the legal representative can be contacted. In order to allow for flexible solutions where needed and notwithstanding their different purposes under this Regulation, it should be

possible, if the provider concerned has made this clear, for its legal representative to also function as its point of contact, provided the relevant requirements of this Regulation are complied with.

(42) Where relevant and convenient, subject to the choice of the provider of relevant information society services and the need to meet the applicable legal requirements in this respect, it should be possible for those providers to designate a single point of contact and a single legal representative for the purposes of Regulation (EU) ***2022/2065*** ~~…/… [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~ and this Regulation.

Batch 7

Compromise amendment on Chapter III, Section
Compromise amendment replacing all relevant amendments, including AM (580, 581, 582, 583, 584, 585, 139, 586, 587, 588, 589, 590, 591, 593, 594, 596, 597, 598, 599, 600, 601, 602, 140, 603, 141, 604, 605, 606, 607, 608, 609, 610, 611, 142, 612, 613, 143, 144, 614, 145, 615, 616, 617, 146, 147, 618, 619, 620, 621, 622, 623, 624, 625, 626, 148, 627, 149, 628, 150, 629, 630, 631, 151, 632, 633, 634, 152, 635, 153, 225, 226, 31, 227, 228, 229, 230, 231, 232, 233 and 32)

Article 25

Coordinating Authorities for child sexual abuse issues and other competent authorities

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

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

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

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

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

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

5. Each Member State shall ensure that a contact point is designated or established within the Coordinating Authority's office to ***efficiently*** handle requests for clarification, feedback and other communications in relation to all matters related to the ***objective,*** application and enforcement of this Regulation in that Member State***, including communication with trusted organisations providing assistance to victims, education and awareness raising***. Member States shall make the information on the contact point publicly available and communicate it to the EU Centre. They shall keep that information updated

6. Within two weeks after the designation of the Coordinating Authorities pursuant to paragraph 2, the EU Centre shall set up an online register listing the Coordinating Authorities and their contact points. The EU Centre shall regularly publish any modification thereto.

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

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

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

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

   ~~(d) verify the effectiveness of a detection order or a removal order issued upon the request of the requesting Coordinating Authority.~~ ***help with regard to risk assessments, mitigation measures and orders.***

8. The EU Centre shall provide such assistance***, without undue delay,*** free of charge and in accordance with its tasks and obligations under this Regulation ~~and insofar as its resources and priorities allow~~.

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

Article 26

Requirements for Coordinating Authorities

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

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

   (a) are ***independent*** ~~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, ***or coordination with public authrorities relevant to combat child sexual abuse*** to the extent that such supervision ***and coordination*** 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. ***Without prejudice to national or Union legislation on whistle-blower protection,*** 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

1. Where needed for carrying out their tasks, Coordinating Authorities shall have the following powers of investigation, 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, ***or to request a judicial authority in their Member States to order*** ~~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 powers to the Coordinating Authorities.

Article 28

Enforcement powers

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

   (a) the power to accept the commitments offered by those providers in relation to their compliance with this Regulation and to make those commitments binding;

(b) the power to order ***specific measures to bring about*** the cessation of infringements of this Regulation and, where appropriate, to impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end;

(c) the power to impose fines, or request a judicial authority in their Member State to do so, in accordance with Article 35 for infringements of this Regulation, including non-compliance with any of the orders issued pursuant to Article 27 and to point (b) of this paragraph;

(d) the power to impose a periodic penalty payment in accordance with Article 35 to ensure that an infringement of this Regulation is terminated in compliance with an order issued pursuant to point (b) of this paragraph or for failure to comply with any of the orders issued pursuant to Article 27 and to point (b) of this paragraph;

(e) the power to adopt interim measures to avoid the risk of serious harm.

2. Member States may grant additional enforcement powers to the Coordinating Authorities.

3. As regards paragraph 1, points (c) and (d), Coordinating Authorities shall have the enforcement powers set out in those points also in respect of the other persons referred to in Article 27, for failure to comply with any of the orders issued to them pursuant to that Article.

4. They shall only exercise those enforcement powers after having provided those other persons in good time with all relevant information relating to such orders, including the applicable time period, the fines or periodic payments that may be imposed for failure to comply and redress possibilities.

Article 29

Additional enforcement powers

1. Where needed for carrying out their tasks, Coordinating Authorities shall have the additional enforcement powers referred to in paragraph 2, in respect of providers of relevant information society services under the jurisdiction of the Member State that designated them, provided that:

(a) all other powers pursuant to Articles 27 and 28 to bring about the cessation of an infringement of this Regulation have been exhausted;

(b) the infringement persists ***and***;

(c) the infringement causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law.

2. Coordinating Authorities shall have the additional enforcement powers to take the following measures:

(a) require the management body of the providers to examine the situation within a reasonable time period and to:

(i) adopt and submit an action plan setting out the necessary measures to terminate the infringement;

(ii) ensure that the provider takes those measures;

(iii) report on the measures taken;

(b) request the competent judicial authority ~~or independent administrative authority~~ of the Member State that designated the Coordinating Authority to order the temporary restriction of access of users of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider on which the infringement takes place, where the Coordinating Authority considers that:

(i) the provider has not sufficiently complied with the requirements of point (a);

(ii) the infringement persists and causes serious harm;

(iii) the infringement results in the regular and structural facilitation of child sexual abuse offences.

3. The Coordinating Authority shall, prior to submitting the request referred to in paragraph 2, point (b), invite interested parties to submit written observations on its intention to submit that request within a reasonable time period set by that Coordinating Authority. That time period shall not be less than two weeks.

The invitation to submit written observations shall:

(a) describe the measures that it intends to request;

(b) identify the intended addressee or addressees thereof.

The provider, the intended addressee or addressees and any other third party demonstrating a legitimate interest shall be entitled to participate in the proceedings regarding the request.

4. Any measure ordered upon the request referred to in paragraph 2, point (b), shall be proportionate to the nature, gravity, recurrence and duration of the infringement, without unduly restricting access to lawful information by users of the service concerned.

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

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

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

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

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

Article 30

Common provisions on investigatory and enforcement powers

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

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

Article 31

Searches to verify compliance

Coordinating Authorities shall have the power to carry out searches on publicly accessible material ~~on hosting services~~ to detect the dissemination of ~~known~~ ~~or new~~ child sexual abuse material, using the indicators contained in the databases referred to in Article 44(1), ***point (a)*** and (b), ~~where necessary to verify whether~~ ***in relation to*** the providers of hosting services under the jurisdiction of the Member State that designated the Coordinating Authorities ~~comply with their~~ ***and the*** obligations under this Regulation.

Article 32

Notification of known child sexual abuse material

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

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

Article 32 a
Public awarness campaigns

Coordinating Authorities shall, in coordination with the EU Centre, increase public awareness regarding the nature of the problem of online child sexual abuse material, how to seek assistance, and how to work with providers of relevant information society services to remove content and coordinate victim identification efforts undertaken in collaboration with existing victim identification programmes. Coordinating Authorities and the EU Centre shall regularly carry out public awareness campaigns to inform about victims' rights and measures to prevent and combat child sexual abuse and how to seek child-friendly and age appropriate reporting and assistance.

Section 3

Other provisions on enforcement

Article 33

Jurisdiction

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

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

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

Article 34

Right of users of the service to lodge a complaint

1. Users ***and any body, organisation or association mandated to exercise the rights conferred by this Regulation on their behalf*** shall have the right to lodge a complaint alleging an infringement of this Regulation affecting them against providers of relevant information society services with the Coordinating Authority designated by the Member State where the user resides or is established.

   1 a. During these proceedings, both parties shall have the right to be heard and receive appropriate information about the status of the complaint, in accordance with national law.

2. Coordinating Authorities shall provide child-friendly mechanisms to submit a complaint under this Article and adopt a child-sensitive approach when handling complaints submitted by children, taking due account of the child's age, maturity, views, needs and concerns.

3. The Coordinating Authority receiving the complaint shall assess the complaint and, where appropriate, transmit it to the Coordinating Authority of establishment ***accompanied, where considered appropriate, by an opinion***.

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

Article 35

Penalties

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

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

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

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

4. Member States shall ensure that the maximum amount of a periodic penalty payment shall not exceed 5 % of the average daily ***worldwide*** ~~global~~ turnover of the provider or the other person referred to in Article 27***(1)(a)*** in the preceding financial year per day, calculated from the date specified in the decision concerned.

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

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

   (b) whether the infringement was intentional or negligent;

   (c) any previous infringements by the provider or the other person, ***referred to in Article 27(1)(a);***

   (d) the financial strength of the provider or the other person, ***referred to in Article 27(1)(a)***;

   (e) the level of cooperation of the provider or the other person, ***referred to in Article 27(1)(a)***;

   (f) the nature and size of the provider or the other person, in particular whether it is a micro, small or medium-sized enterprise;

   (g) the degree of fault of the provider or other person, ***referred to in Article 27(1)(a)***, taking into account the technical and organisational measures taken by it to comply with this Regulation.

Section 4

Cooperation

Article 36

Identification and submission of online child sexual abuse

1. Coordinating Authorities shall submit to the EU Centre, without undue delay and through the system established in accordance with Article 39(2):

   (a) specific items of material and transcripts of conversations ***related to a specific person, specific group of people, or specific incident*** that Coordinating Authorities or that the competent judicial authorities or other independent administrative authorities of a Member State have identified, after a diligent assessment, as constituting child sexual abuse material or the solicitation of children, as applicable, for the EU Centre to generate indicators in accordance with Article 44(3);

   (b) exact uniform resource locators indicating specific items of material ***related to a specific person, specific group of people, or specific incident*** that Coordinating Authorities or that competent judicial authorities or other independent administrative authorities of a Member State have identified, after a diligent

assessment, as constituting child sexual abuse material, hosted by providers of hosting services not offering services in the Union, that cannot be removed due to those providers' refusal to remove or disable access thereto and to the lack of cooperation by the competent authorities of the third country having jurisdiction, for the EU Centre to compile the list of uniform resource locators in accordance with Article 44(3).

Member States shall take the necessary measures to ensure that the Coordinating Authorities that they designated receive, without undue delay, ***the encrypted copies of*** material identified as child sexual abuse material, the transcripts of conversations ***related to a specific person, specific group of people, or specific incident*** identified as the solicitation of children, and the uniform resource locators, identified by a competent judicial authority or other independent administrative authority than the Coordinating Authority, for submission to the EU Centre in accordance with the first subparagraph.

2. Upon the request of the EU Centre where necessary to ensure that the data contained in the databases referred to in Article 44(1) are complete, accurate and up-to-date, Coordinating Authorities shall verify or provide clarifications or additional information as to whether the conditions of paragraph 1, points (a) and (b) have been and, where relevant, continue to be met, in respect of a given submission to the EU Centre in accordance with that paragraph.

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 ~~investigatory and enforcement~~ measures to ensure compliance with this Regulation.

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. (624)

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~~ ***details*** of the investigatory or enforcement measures taken or envisaged in relation thereto to ensure compliance with this Regulation. (626)

Article 38

Joint investigations

1. Coordinating Authorities ***shall ~~share~~ exchange best practice standards and guidance on the detection and removal of child sexual abuse material and*** may participate in joint investigations, which may be coordinated with the support of the EU Centre, of matters covered by this Regulation, concerning providers of relevant information society services that offer their services in several Member States.

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

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

Article 39

General cooperation and information-sharing system

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

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

3. The Coordinating Authorities, ***hotlines and help-lines***, 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.

3 a. Where the EU Centre receives a report from a hotline, or where a provider that submitted the report to the EU Centre has indicated that the report is based on the information received from a hotline, the EU Centre shall coordinate with the relevant Coordinating Authorities in order to avoid duplicated reporting on the same material that has already been reported to the national law enforcement authorities by the hotlines and monitor the removal of the child sexual abuse material or cooperate with the relevant hotline to track the status.

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

CHAPTER IV

EU CENTRE TO PREVENT AND COMBAT CHILD SEXUAL ABUSE

Section 1

Principles

Article 40

Establishment and scope of action of the EU Centre

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

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

Article 41

Legal status

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

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

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

Article 42

Seat

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

Section 2

Tasks

Article 43

Tasks of the EU Centre

The EU Centre shall:

(1) facilitate the risk assessment process referred to in Section 1 of Chapter II, by:

(a) supporting the Commission in the preparation of the guidelines referred to in Article 3(8), Article 4(5), Article 6(4) and Article 11, including by collecting and providing relevant information, expertise and best practices, taking into account advice from the Technology Committee referred to in Article 66;

(b) upon request from a provider of relevant information services, providing an analysis of anonymised data samples for the purpose referred to in Article 3(3);

(2) facilitate the detection process referred to in Section 2 of Chapter II, by:

(a) providing the opinions on intended detection orders referred to in Article 7(3), first subparagraph, point (d);

(b) maintaining and operating the databases of indicators referred to in Article 44;

(c) giving providers of hosting services and providers of interpersonal communications services that received a detection order access to the relevant databases of indicators in accordance with Article 46;

(d) making technologies available to providers for the execution of detection orders issued to them, in accordance with Article 50(1);

(3) facilitate the reporting process referred to in Section 3 of Chapter II, by:

(a) maintaining and operating the database of reports referred to in Article 45;

(b) assessing, processing and, where necessary, forwarding the reports and providing feedback thereon in accordance with Article 48;

(4) facilitate the removal process referred to in Section 4 of Chapter II and the other processes referred to in Section 5 and 6 of that Chapter, by:

(a) receiving the removal orders transmitted to it pursuant to Article 14(4) in order to fulfil the verification function referred to in Article 49(1);

(b) cooperating with and responding to requests of Coordinating Authorities in connection to intended blocking orders as referred to in Article 16(2);

(c) receiving and processing the blocking orders transmitted to it pursuant to Article 17(3);

(d) providing information and support to victims in accordance with Articles 20 and 21;

(e) maintaining up-to-date records of contact points and legal representatives of providers of relevant information society services as provided in accordance with Article 23(2) and Article 24(6);

(5) support the Coordinating Authorities and the Commission in the performance of their tasks under this Regulation and facilitate cooperation, coordination and communication in connection to matters covered by this Regulation, by:

(a) creating and maintaining an online register listing the Coordinating Authorities and their contact points referred to in Article 25(6);

(b) providing assistance to the Coordinating Authorities as provided for in Article 25(7);

(c) assisting the Commission, upon its request, in connection to its tasks under the cooperation mechanism referred to in Article 37;

(d) creating, maintaining and operating the information-sharing system referred to in Article 39;

(e) assisting the Commission in the preparation of the delegated and implementing acts and the guidelines that the Commission adopts under this Regulation;

(f) providing information to Coordinating Authorities, upon their request or on its own initiative, relevant for the performance of their tasks under this Regulation, including by informing the Coordinating Authority of establishment of potential infringements identified in the performance of the EU Centre's other tasks;

(6) facilitate the generation and sharing of knowledge with other Union institutions, bodies, offices and agencies, Coordinating Authorities or other relevant authorities of the Member States to contribute to the achievement of the objective of this Regulation, by:

(a) collecting, recording, analysing and providing information, providing analysis based on anonymised and non-personal data gathering, and providing expertise on matters regarding the prevention and combating of online child sexual abuse, in accordance with Article 51;

(b) supporting the development and dissemination of research and expertise on those matters and on assistance to victims, including by serving as a hub of expertise to support evidence-based policy;

(c) drawing up the annual reports referred to in Article 84.

Article 44

Databases of indicators

1. The EU Centre shall create, maintain and operate databases of the following three types of indicators of online child sexual abuse:

(a) indicators to detect the dissemination of child sexual abuse material previously detected and identified as constituting child sexual abuse material in accordance with Article 36(1);

(b) indicators to detect the dissemination of child sexual abuse material not previously detected and identified as constituting child sexual abuse material in accordance with Article 36(1);

(c) indicators to detect the solicitation of children.

2. The databases of indicators shall solely contain:

(a) relevant indicators, consisting of digital identifiers to be used to detect the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, on hosting services and interpersonal communications services, generated by the EU Centre in accordance with paragraph 3;

(b) as regards paragraph 1, point (a), the relevant indicators shall include a list of uniform resource locators compiled by the EU Centre in accordance with paragraph 3;

(c) the necessary additional information to facilitate the use of the indicators in accordance with this Regulation, including identifiers allowing for a distinction between images, videos and, where relevant, other types of material for the detection of the dissemination of known and new child sexual abuse material and language identifiers for the detection of solicitation of children.

3. The EU Centre shall generate the indicators referred to in paragraph 2, point (a), solely on the basis of the child sexual abuse material and the solicitation of children identified

as such by the Coordinating Authorities or the courts or other independent authorities of the Member States, submitted to it by the Coordinating Authorities pursuant to Article 36(1), point (a).

The EU Centre shall compile the list of uniform resource locators referred to in paragraph 2, point (b), solely on the basis of the uniform resource locators submitted to it pursuant to Article 36(1), point (b).

4. The EU Centre shall keep records of the submissions and of the process applied to generate the indicators and compile the list referred to in the first and second subparagraphs. It shall keep those records for as long as the indicators, including the uniform resource locators, to which they correspond are contained in the databases of indicators referred to in paragraph 1.

Article 45

Database of reports

1. The EU Centre shall create, maintain and operate a database for the reports submitted to it by providers of hosting services and providers of interpersonal communications services in accordance with Article 12(1) and assessed and processed in accordance with Article 48.

2. The database of reports shall contain the following information:

(a) the report;

(b) where the EU Centre considered the report manifestly unfounded, the reasons and the date and time of informing the provider in accordance with Article 48(2);

(c) where the EU Centre forwarded the report in accordance with Article 48(3), the date and time of such forwarding and the name of the competent law enforcement authority or authorities to which it forwarded the report or, where applicable, information on the reasons for forwarding the report solely to Europol for further analysis;

(d) where applicable, information on the requests for and provision of additional information referred to in Article 48(5);

(e) where available, information indicating that the provider that submitted a report concerning the dissemination of known or new child sexual abuse material removed or disabled access to the material;

(f) where applicable, information on the EU Centre's request to the Coordinating Authority of establishment to issue a removal order pursuant to Article 14 in relation to the item or items of child sexual abuse material to which the report relates;

(g) relevant indicators and ancillary tags associated with the reported potential child sexual abuse material.

Article 46

Access, accuracy and security

1. Subject to paragraphs 2 and 3, solely EU Centre staff and auditors duly authorised by the Executive Director shall have access to and be entitled to process the data contained in the databases referred to in Articles 44 and 45.

2. The EU Centre shall give providers of hosting services, providers of interpersonal communications services and providers of internet access services access to the databases of indicators referred to in Article 44, where and to the extent necessary for them to execute the detection or blocking orders that they received in accordance with Articles 7 or 16. It shall take measures to ensure that such access remains limited to what is strictly necessary for the period of application of the detection or blocking orders concerned and that such access does not in any way endanger the proper operation of those databases and the accuracy and security of the data contained therein.

3. The EU Centre shall give Coordinating Authorities access to the databases of indicators referred to in Article 44 where and to the extent necessary for the performance of their tasks under this Regulation.

4. The EU Centre shall give Europol and the competent law enforcement authorities of the Member States access to the databases of indicators referred to in Article 44 where and to the extent necessary for the performance of their tasks of investigating suspected child sexual abuse offences.

5. The EU Centre shall give Europol access to the databases of reports referred to in Article 45, where and to the extent necessary for the performance of its tasks of assisting investigations of suspected child sexual abuse offences

6. The EU Centre shall provide the access referred to in paragraphs 2, 3, 4 and 5 only upon the reception of a request, specifying the purpose of the request, the modalities of the requested access, and the degree of access needed to achieve that purpose. The requests for the access referred to in paragraph 2 shall also include a reference to the detection order or the blocking order, as applicable.

   The EU Centre shall diligently assess those requests and only grant access where it considers that the requested access is necessary for and proportionate to the specified purpose.

7. The EU Centre shall regularly verify that the data contained in the databases referred to in Articles 44 and 45 is, in all respects, complete, accurate and up-to-date and continues to be necessary for the purposes of reporting, detection and blocking in accordance with this Regulation, as well as facilitating and monitoring of accurate detection technologies and processes. In particular, as regards the uniform resource locators contained in the database referred to Article 44(1), point (a), the EU Centre shall, where necessary in cooperation with the Coordination Authorities, regularly verify that the conditions of Article 36(1), point (b), continue to be met. Those verifications shall include audits, where appropriate. Where necessary in view of those verifications, it shall immediately complement, adjust or delete the data.

8. The EU Centre shall ensure that the data contained in the databases referred to in Articles 44 and 45 is stored in a secure manner and that the storage is subject to appropriate technical and organisational safeguards. Those safeguards shall ensure, in particular, that the data can be accessed and processed only by duly authorised persons for the purpose for which the person is authorised and that a high level of security is achieved. The EU Centre shall regularly review those safeguards and adjust them where necessary.

Article 47

Delegated acts relating to the databases

The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to supplement this Regulation with the necessary detailed rules concerning:

(a) the types, precise content, set-up and operation of the databases of indicators referred to in Article 44(1), including the indicators and the necessary additional information to be contained therein referred to in Article 44(2);

(b) the processing of the submissions by Coordinating Authorities, the generation of the indicators, the compilation of the list of uniform resource locators and the record-keeping, referred to in Article 44(3);

(c) the precise content, set-up and operation of the database of reports referred to in Article 45(1);

(d) access to the databases referred to in Articles 44 and 45, including the modalities of the access referred to in Article 46(1) to (5), the content, processing and assessment of the requests referred to in Article 46(6), procedural matters related to such requests and the necessary measures referred to in Article 46(6);

(e) the regular verifications and audits to ensure that the data contained in those databases is complete, accurate and up-to-date referred to in Article 46(7) and the security of the storage of the data, including the technical and organisational safeguards and regular review referred to in Article 46(8).

Article 48

Reporting

1. The EU Centre shall expeditiously assess and process reports submitted by providers of hosting services and providers of interpersonal communications services in accordance with Article 12 to determine whether the reports are manifestly unfounded or are to be forwarded.

2. Where the EU Centre considers that the report is manifestly unfounded, it shall inform the provider that submitted the report, specifying the reasons why it considers the report to be unfounded.

3. Where the EU Centre considers that a report is not manifestly unfounded, it shall forward the report, together with any additional relevant information available to it, to Europol and to the competent law enforcement authority or authorities of the Member State likely to have jurisdiction to investigate or prosecute the potential child sexual abuse to which the report relates.

   Where that competent law enforcement authority or those competent law enforcement authorities cannot be determined with sufficient certainty, the EU Centre shall forward the report, together with any additional relevant information available to it, to Europol, for further analysis and subsequent referral by Europol to the competent law enforcement authority or authorities.

4. Where a provider that submitted the report has indicated that the report requires urgent action, the EU Centre shall assess and process that report as a matter of priority and, where it forwards the report in accordance with paragraph 3 and it considers that the report requires urgent action, shall ensure that the forwarded report is marked as such.

5. Where the report does not contain all the information required in Article 13, the EU Centre may request the provider that submitted the report to provide the missing information.

6. Where so requested by a competent law enforcement authority of a Member State in order to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences, the EU Centre shall:

   (a) communicate to the provider that submitted the report that it is not to inform the user concerned, specifying the time period during which the provider is not to do so;

   (b) where the provider that submitted the report is a provider of hosting services and the report concerns the potential dissemination of child sexual abuse material, communicate to the provider that it is not to remove or disable access to the material, specifying the time period during which the provider is not to do so.

7. The time periods referred to in the first subparagraph, points (a) and (b), shall be those specified in the competent law enforcement authority's request to the EU Centre, provided that they remain limited to what is necessary to avoid interference with the relevant activities and does not exceed 18 months.

8. The EU Centre shall verify whether a provider of hosting services that submitted a report concerning the potential dissemination of child sexual abuse material removed or disabled access to the material, insofar as the material is publicly accessible. Where it considers that the provider did not remove or disable access to the material expeditiously, the EU Centre shall inform the Coordinating Authority of establishment thereof.

Article 49

Searches and notification

1. The EU Centre shall have the power to conduct searches on hosting services for the dissemination of publicly accessible child sexual abuse material, using the relevant indicators from the database of indicators referred to in Article 44(1), points (a) and (b), in the following situations:

   (a) where so requested to support a victim by verifying whether the provider of hosting services removed or disabled access to one or more specific items of known child sexual abuse material depicting the victim, in accordance with Article 21(4), point (c);

   (b) where so requested to assist a Coordinating Authority by verifying the possible need for the issuance of a detection order or a removal order in respect of a specific service or the effectiveness of a detection order or a removal order that the Coordinating Authority issued, in accordance with Article 25(7), points (c) and (d), respectively.

2. The EU Centre shall have the power to notify, after having conducted the searches referred to in paragraph 1, providers of hosting services of the presence of one or more specific items of known child sexual abuse material on their services and request them to remove or disable access to that item or those items, for the providers' voluntary consideration.

The request shall clearly set out the identification details of the EU Centre and a contact point, the necessary information for the identification of the item or items, as well as the reasons for the request. The request shall also clearly state that it is for the provider's voluntary consideration.

3. Where so requested by a competent law enforcement authority of a Member State in order to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences, the EU Centre shall not submit a notice, for as long as necessary to avoid such interference but no longer than 18 months.

Article 50

Technologies, information and expertise

1. The EU Centre shall make available technologies that providers of hosting services and providers of interpersonal communications services may acquire, install and operate, free of charge, where relevant subject to reasonable licensing conditions, to execute detection orders in accordance with Article 10(1).

   To that aim, the EU Centre shall compile lists of such technologies, having regard to the requirements of this Regulation and in particular those of Article 10(2).

   Before including specific technologies on those lists, the EU Centre shall request the opinion of its Technology Committee and of the European Data Protection Board. The Technology Committee and the European Data Protection Board shall deliver their respective opinions within eight weeks. That period may be extended by a further six weeks where necessary, taking into account the complexity of the subject matter. The Technology Committee and the European Data Protection Board shall inform the EU Centre of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

2. The EU Centre shall collect, record, analyse and make available relevant, objective, reliable and comparable information on matters related to the prevention and combating of child sexual abuse, in particular:

   (a) information obtained in the performance of its tasks under this Regulation concerning detection, reporting, removal or disabling of access to, and blocking of online child sexual abuse;

   (b) information resulting from the research, surveys and studies referred to in paragraph 3;

   (c) information resulting from research or other activities conducted by Member States' authorities, other Union institutions, bodies, offices and agencies, the competent authorities of third countries, international organisations, research centres and civil society organisations.

3. Where necessary for the performance of its tasks under this Regulation, the EU Centre shall carry out, participate in or encourage research, surveys and studies, either on its own initiative or, where appropriate and compatible with its priorities and its annual work programme, at the request of the European Parliament, the Council or the Commission.

4. The EU Centre shall provide the information referred to in paragraph 2 and the information resulting from the research, surveys and studies referred to in paragraph 3, including its analysis thereof, and its opinions on matters related to the prevention and combating of online child sexual abuse to other Union institutions, bodies, offices and agencies, Coordinating Authorities, other competent authorities and other public authorities of the Member States, either on its own initiative or at request of the relevant authority. Where appropriate, the EU Centre shall make such information publicly available.

5. The EU Centre shall develop a communication strategy and promote dialogue with civil society organisations and providers of hosting or interpersonal communication services to raise public awareness of online child sexual abuse and measures to prevent and combat such abuse.

Section 3

Processing of information

Article 51

Processing activities and data protection

1. In so far as is necessary for the performance of its tasks under this Regulation, the EU Centre may process personal data.

2. The EU Centre shall process personal data as strictly necessary for the purposes of:

   (a) providing the opinions on intended detection orders referred to in Article 7(3);

   (b) cooperating with and responding to requests of Coordinating Authorities in connection to intended blocking orders as referred to in Article 16(2);

   (c) receiving and processing blocking orders transmitted to it pursuant to Article 17(3);

   (d) cooperating with Coordinating Authorities in accordance with Articles 20 and 21 on tasks related to victims' rights to information and assistance;

   (e) maintaining up-to-date records of contact points and legal representatives of providers of relevant information society services as provided in accordance with Article 23(2) and Article 24(6);

   (f) creating and maintaining an online register listing the Coordinating Authorities and their contact points referred to in Article 25(6);

   (g) providing assistance to Coordinating Authorities in accordance with Article 25(7);

   (h) assisting the Commission, upon its request, in connection to its tasks under the cooperation mechanism referred to in Article 37;

   (i) create, maintain and operate the databases of indicators referred to in Article 44;

   (j) create, maintain and operate the database of reports referred to in Article 45;

   (k) providing and monitoring access to the databases of indicators and of reports in accordance with Article 46;

   (l) performing data quality control measures in accordance with Article 46(7);

(m) assessing and processing reports of potential online child sexual abuse in accordance with Article 48;

(n) cooperating with Europol and partner organisations in accordance with Articles 53 and 54, including on tasks related to the identification of victims;

(o) generating statistics in accordance with Article 83.

3. The EU Centre shall store the personal data referred to in paragraph 2 only where and for as long as strictly necessary for the applicable purposes listed in paragraph 2.

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

Section 4

Cooperation

Article 52

Contact officers

1. Each Coordinating Authority shall designate at least one contact officer, who shall be the main contact point for the EU Centre in the Member State concerned. The contact officers may be seconded to the EU Centre. Where several contact officers are designated, the Coordinating Authority shall designate one of them as the main contact officer.

2. Contact officers shall assist in the exchange of information between the EU Centre and the Coordinating Authorities that designated them. Where the EU Centre receives reports submitted in accordance with Article 12 concerning the potential dissemination of new child sexual abuse material or the potential solicitation of children, the contact officers designated by the competent Member State shall facilitate the process to determine the illegality of the material or conversation, in accordance with Article 36(1).

3. The Management Board shall determine the rights and obligations of contact officers in relation to the EU Centre. Contact officers shall enjoy the privileges and immunities necessary for the performance of their tasks.

4. Where contact officers are seconded to the EU Centre, the EU Centre shall cover the costs of providing them with the necessary premises within the building and adequate support for contact officers to perform their duties. All other costs that arise in connection with the designation of contact officers and the performance of their tasks shall be borne by the Coordinating Authority that designated them.

Article 53

Cooperation with Europol

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

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

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

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

Article 54

Cooperation with partner organisations

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

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

Section 5

Organisation

Article 55

Administrative and management structure

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

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

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

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

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

Part 1: Management Board

Article 56

Composition of the Management Board

1. The Management Board shall be composed of one representative from each Member State and two representatives of the Commission, all as members with voting rights.

2. The Management Board shall also include one independent expert observer designated by the European Parliament, without the right to vote.

Europol may designate a representative to attend the meetings of the Management Board as an observer on matters involving Europol, at the request of the Chairperson of the Management Board.

3. Each member of the Management Board shall have an alternate. The alternate shall represent the member in his/her absence.

4. Members of the Management Board and their alternates shall be appointed in the light of their knowledge in the field of combating child sexual abuse, taking into account relevant managerial, administrative and budgetary skills. Member States shall appoint a representative of their Coordinating Authority, within four months of [*date of entry into force of this Regulation*]. All parties represented in the Management Board shall make efforts to limit turnover of their representatives, in order to ensure continuity of its work. All parties shall aim to achieve a balanced representation between men and women on the Management Board.

5. The term of office for members and their alternates shall be four years. That term may be renewed.

Article 57

Functions of the Management Board

1. The Management Board shall:

(a) give the general orientations for the EU Centre's activities;

(b) contribute to facilitate the effective cooperation with and between the Coordinating Authorities;

(c) adopt rules for the prevention and management of conflicts of interest in respect of its members, as well as for the members of the Technological Committee and of any other advisory group it may establish and publish annually on its website the declaration of interests of the members of the Management Board;

(d) adopt the assessment of performance of the Executive Board referred to in Article 61(2);

(e) adopt and make public its Rules of Procedure;

(f) appoint the members of the Technology Committee, and of any other advisory group it may establish;

(g) adopt the opinions on intended detection orders referred to in Article 7(4), on the basis of a draft opinion provided by the Executive Director;

(h) adopt and regularly update the communication and dissemination plans referred to in Article 77(3) based on an analysis of needs.

Article 58

Chairperson of the Management Board

1. The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members. The Chairperson and the Deputy Chairperson shall be elected by a majority of two thirds of the members of the Management Board.

The Deputy Chairperson shall automatically replace the Chairperson if he/she is prevented from attending to his/her duties.

2. The term of office of the Chairperson and the deputy Chairperson shall be four years. Their term of office may be renewed once. If, however, their membership of the Management Board ends at any time during their term of office, their term of office shall automatically expire on that date.

Article 59

Meetings of the Management Board

1. The Chairperson shall convene the meetings of the Management Board.
2. The Executive Director shall take part in the deliberations, without the right to vote.
3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, or at the request of at least one-third of its members.
4. The Management Board may invite any person whose opinion may be of interest to attend its meetings as an observer.
5. The members of the Management Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.
6. The EU Centre shall provide the secretariat for the Management Board.

Article 60

Voting rules of the Management Board

1. Unless provided otherwise in this Regulation, the Management Board shall take decisions by absolute majority of its members.
2. Each member shall have one vote. In the absence of a member, his/her alternate shall be entitled to exercise his/her right to vote.
3. The Executive Director shall not take part in the voting.
4. The Management Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.

Part 2: Executive Board

Article 61

Composition and appointment of the Executive Board

1. The Executive Board shall be composed of the Chairperson and the Deputy Chairperson of the Management Board, two other members appointed by the Management Board from among its members with the right to vote and two representatives of the Commission to the Management Board. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board.

   The Executive Director shall participate in meetings of the Executive Board without the right to vote.

2. The term of office of members of the Executive Board shall be four years. In the course of the 12 months preceding the end of the four-year term of office of the Chairperson

and five members of the Executive Board, the Management Board or a smaller committee selected among Management Board members including a Commission representative shall carry out an assessment of performance of the Executive Board. The assessment shall take into account an evaluation of the Executive Board members' performance and the EU Centre's future tasks and challenges. Based on the assessment, the Management Board may extend their term of office once.

Article 62

Tasks of the Executive Board

1. The Executive Board shall be responsible for the overall planning and the execution of the tasks conferred on the EU Centre pursuant to Article 43. The Executive Board shall adopt all the decisions of the EU Centre with the exception of the decisions that shall be taken by the Management Board in accordance with Article 57.

2. In addition, the Executive Board shall have the following tasks:

   (a) adopt, by 30 November of each year, on the basis of a proposal by the Executive Director, the draft Single Programming Document, and shall transmit it for information to the European Parliament, the Council and the Commission by 31 January the following year, as well as any other updated version of the document;

   (b) adopt the draft annual budget of the EU Centre and exercise other functions in respect of the EU Centre's budget;

   (c) assess and adopt a consolidated annual activity report on the EU Centre's activities, including an overview of the fulfilment of its tasks and send it, by 1 July each year, to the European Parliament, the Council, the Commission and the Court of Auditors and make the consolidated annual activity report public;

   (d) adopt an anti-fraud strategy, proportionate to fraud risks taking into account the costs and benefits of the measures to be implemented, an efficiency gains and synergies strategy, a strategy for cooperation with third countries and/or international organisations, and a strategy for the organisational management and internal control systems

   (e) adopt rules for the prevention and management of conflicts of interest in respect of its members;

   (f) adopt its rules of procedure;

   (g) exercise, with respect to the staff of the EU Centre, the powers conferred by the Staff Regulations on the Appointing Authority and by the Conditions of Employment of Other Servants on the EU Centre Empowered to Conclude a Contract of Employment[1] ("the appointing authority powers");

   (h) adopt appropriate implementing rules for giving effect to the Staff Regulations and the Conditions of Employment of Other Servants in accordance with Article 110(2) of the Staff Regulations;

[1] Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1)

(i) appoint the Executive Director and remove him/her from office, in accordance with Article 65;

(j) appoint an Accounting Officer, who may be the Commission's Accounting Officer, subject to the Staff Regulations and the Conditions of Employment of other servants, who shall be totally independent in the performance of his/her duties;

(k) ensure adequate follow-up to findings and recommendations stemming from the internal or external audit reports and evaluations, as well as from investigations of the European Anti-Fraud Office (OLAF);

(l) adopt the financial rules applicable to the EU Centre;

(m) take all decisions on the establishment of the EU Centre's internal structures and, where necessary, their modification.

(n) appoint a Data Protection Officer;

(o) adopt internal guidelines further specifying the procedures for the processing of information in accordance with Article 51, after consulting the European Data Protection Supervisor;

(p) authorise the conclusion of memoranda of understanding referred to in Article 53(3) and Article 54(2).

3. With respect to the powers mentioned in paragraph 2 point (g) and (h), the Executive Board shall adopt, in accordance with Article 110(2) of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and Article 6 of the Conditions of Employment, delegating relevant appointing authority powers to the Executive Director. The Executive Director shall be authorised to sub-delegate those powers.

4. In exceptional circumstances, the Executive Board may by way of a decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation by the latter and exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.

5. Where necessary because of urgency, the Executive Board may take certain provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters.

Article 63

Voting rules of the Executive Board

1. The Executive Board shall take decisions by simple majority of its members. Each member of the Executive Board shall have one vote. The Chairperson shall have a casting vote in case of a tie.

2. The representatives of the Commission shall have a right to vote whenever matters pertaining to Article 62(2), points (a) to (l) and (p) are discussed and decided upon. For the purposes of taking the decisions referred to in Article 62(2), points (f) and (g), the representatives of the Commission shall have one vote each. The decisions referred to in Article 62(2), points (b) to (e), (h) to (l) and (p), may only be taken if the representatives of the Commission casts a positive vote. For the purposes of taking the decisions referred to in Article 62(2), point (a), the consent of the representatives of

the Commission shall only be required on the elements of the decision not related to the annual and multi-annual working programme of the EU Centre.

The Executive Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.

Part 3: Executive Director

Article 64

Responsibilities of the Executive Director

1. The Executive Director shall manage the EU Centre. The Executive Director shall be accountable to the Management Board.
2. The Executive Director shall report to the European Parliament on the performance of his/her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his/her duties.
3. The Executive Director shall be the legal representative of the EU Centre.
4. The Executive Director shall be responsible for the implementation of the tasks assigned to the EU Centre by this Regulation. In particular, the Executive Director shall be responsible for:
   (a) the day-to-day administration of the EU Centre;
   (b) preparing decisions to be adopted by the Management Board;
   (c) implementing decisions adopted by the Management Board;
   (d) preparing the Single Programming Document and submitting it to the Executive Board after consulting the Commission;
   (e) implementing the Single Programming Document and reporting to the Executive Board on its implementation;
   (f) preparing the Consolidated Annual Activity Report (CAAR) on the EU Centre's activities and presenting it to the Executive Board for assessment and adoption;
   (g) preparing an action plan following-up conclusions of internal or external audit reports and evaluations, as well as investigations by the European Anti-Fraud Office (OLAF) and by the European Public Prosecutor's Office (EPPO) and reporting on progress twice a year to the Commission and regularly to the Management Board and the Executive Board;
   (h) protecting the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of OLAF and EPPO by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative, including financial penalties;
   (i) preparing an anti-fraud strategy, an efficiency gains and synergies strategy, a strategy for cooperation with third countries and/or international organisations and a strategy for the organisational management and internal control systems for the EU Centre and presenting them to the Executive Board for approval;

(j) preparing draft financial rules applicable to the EU Centre;

(k) preparing the EU Centre's draft statement of estimates of revenue and expenditure and implementing its budget;

(l) preparing and implementing an IT security strategy, ensuring appropriate risk management for all IT infrastructure, systems and services, which are developed or procured by the EU Centre as well as sufficient IT security funding.

(m) implementing the annual work programme of the EU Centre under the control of the Executive Board;

(n) drawing up a draft statement of estimates of the EU Centre's revenue and expenditure as part of the EU Centre's Single Programming Document and implementing the budget of the EU Centre pursuant to Article 67;

(o) preparing a draft report describing all activities of the EU Centre with a section on financial and administrative matters;

(p) fostering recruitment of appropriately skilled and experienced EU Centre staff, while ensuring gender balance.

5. Where exceptional circumstances so require, the Executive Director may decide to locate one or more staff in another Member State for the purpose of carrying out the EU Centre's tasks in an a more efficient, effective and coherent manner. Before deciding to establish a local office, the Executive Director shall obtain the prior consent of the Commission, the Management Board and the Member State concerned. The decision shall be based on an appropriate cost-benefit analysis that demonstrates in particular the added value of such decision and specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of the EU Centre. A headquarters agreement with the Member State(s) concerned may be concluded.

Article 65

Executive Director

1. The Executive Director shall be engaged as a temporary agent of the EU Centre under Article 2(a) of the Conditions of Employment of Other Servants.

2. The Executive Director shall be appointed by the Executive Board, from a list of candidates proposed by the Commission, following an open and transparent selection procedure.

3. For the purpose of concluding the contract with the Executive Director, the EU Centre shall be represented by the Chairperson of the Executive Board.

4. The term of office of the Executive Director shall be five years. Six months before the end of the Executive Director's term of office, the Commission shall complete an assessment that takes into account an evaluation of the Executive Director's performance and the EU Centre's future tasks and challenges.

5. The Executive Board, acting on a proposal from the Commission that takes into account the assessment referred to in paragraph 3, may extend the term of office of the Executive Director once, for no more than five years.

6. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post at the end of the overall period.

7. The Executive Director may be dismissed only upon a decision of the Executive Board acting on a proposal from the Commission.

8. The Executive Board shall take decisions on appointment, extension of the term of office or dismissal of the Executive Director by a majority of two-thirds of its members with voting rights.

Subsection 5: Technology Committee

Article 66

Establishment and tasks of the Technology Committee

1. The Technology Committee shall consist of technical experts appointed by the Management Board in view of their excellence and their independence, following the publication of a call for expressions of interest in the Official Journal of the European Union.

2. Procedures concerning the appointment of the members of the Technology Committee and its operation shall be specified in the rules of procedure of the Management Board and shall be made public.

3. The members of the Committee shall be independent and shall act in the public interest. The list of members of the Committee shall be made public and shall be updated by the EU Centre on its website.

4. When a member no longer meets the criteria of independence, he or she shall inform the Management Board. Alternatively, the Management Board may declare, on a proposal of at least one third of its members or of the Commission, a lack of independence and revoke the person concerned. The Management Board shall appoint a new member for the remaining term of office in accordance with the procedure for ordinary members.

5. The mandates of members of the Technology Committee shall be four years. Those mandates shall be renewable once.

6. The Technology Committee shall

   (a) contribute to the EU Centre's opinions referred to in Article 7(3), first subparagraph, point (d);

   (b) contribute to the EU Centre's assistance to the Coordinating Authorities, the Management Board, the Executive Board and the Executive Director, in respect of matters related to the use of technology;

   (c) provide internally, upon request, expertise on matters related to the use of technology for the purposes of prevention and detection of child sexual abuse online.

Section 6

Establishment and Structure of the Budget

Subsection 1

Single Programming Document

Article 67

Budget establishment and implementation

1. Each year the Executive Director shall draw up a draft statement of estimates of the EU Centre's revenue and expenditure for the following financial year, including an establishment plan, and shall send it to the Executive Board.
2. The Executive Board shall, on the basis of the draft statement of estimates, adopt a provisional draft estimate of the EU Centre's revenue and expenditure for the following financial year and shall send it to the Commission by 31 January each year.
3. The Executive Board shall send the final draft estimate of the EU Centre's revenue and expenditure, which shall include a draft establishment plan, to the European Parliament, the Council and the Commission by 31 March each year.
4. The Commission shall send the statement of estimates to the European Parliament and the Council, together with the draft general budget of the Union.
5. On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates that it considers necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall place before the European Parliament and the Council in accordance with Articles 313 and 314 of the Treaty on the Functioning of the European Union.
6. The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to the EU Centre.
7. The European Parliament and the Council shall adopt the EU Centre's establishment plan.
8. The EU Centre's budget shall be adopted by the Executive Board. It shall become final following the final adoption of the general budget of the Union. Where necessary, it shall be adjusted accordingly.
9. The Executive Director shall implement the EU Centre's budget.
10. Each year the Executive Director shall send to the European Parliament and the Council all information relevant to the findings of any evaluation procedures.

Article 68

Financial rules

The financial rules applicable to the EU Centre shall be adopted by the Executive Board after consultation with the Commission. They shall not depart from Delegated Regulation (EU) 2019/715[2] unless such a departure is specifically required for the operation of the EU Centre and the Commission has given its prior consent.

[2] OJ L 122, 10.5.2019, p. 1.

1.

Subsection 2

Presentation, implementation and control of the budget

Article 69

Budget

1. Estimates of all revenue and expenditure for the EU Centre shall be prepared each financial year, which shall correspond to the calendar year, and shall be shown in the EU Centre's budget, which shall be balanced in terms of revenue and of expenditure.

2. Without prejudice to other resources, the EU Centre's revenue shall comprise a contribution from the Union entered in the general budget of the Union.

3. The EU Centre may benefit from Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 68 and with the provisions of the relevant instruments supporting the policies of the Union.

4. The EU Centre's expenditure shall include staff remuneration, administrative and infrastructure expenses, and operating costs.

5. Budgetary commitments for actions relating to large-scale projects extending over more than one financial year may be broken down into several annual instalments.

Article 70

Presentation of accounts and discharge

1. The EU Centre's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).

2. The EU Centre shall send a report on the budgetary and financial management for year N to the European Parliament, the Council and the Court of Auditors by 31 March of year N + 1.

3. The Commission's accounting officer shall send the EU Centre's provisional accounts for year N, consolidated with the Commission's accounts, to the Court of Auditors by 31 March of year N + 1.

4. The Management Board shall deliver an opinion on the EU Centre's final accounts for year N.

5. The EU Centre's accounting officer shall, by 1 July of year N + 1, send the final accounts for year N to the European Parliament, the Council, the Commission, the Court of Auditors and national parliaments, together with the Management Board's opinion.

6. The final accounts for year N shall be published in the Official Journal of the European Union by 15 November of year N + 1.

7. The Executive Director shall send to the Court of Auditors, by 30 September of year N + 1, a reply to the observations made in its annual report. He or she shall also send the reply to the Management Board.

8. The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for year N.

9. On a recommendation from the Council acting by a qualified majority, the European Parliament shall, before 15 May of year N + 2, grant a discharge to the Executive Director in respect of the implementation of the budget for year N.

Section 7

Staff

Article 71

General provisions

1. The Staff Regulations and the Conditions of Employment of Other Servants and the rules adopted by agreement between the institutions of the Union for giving effect thereto shall apply to the EU Centre for all matters not covered by this Regulation.

2. The Executive Board, in agreement with the Commission, shall adopt the necessary implementing measures, in accordance with the arrangements provided for in Article 110 of the Staff Regulations.

3. The EU Centre staff, in particular those working in areas related to detection, reporting and removal of online child sexual abuse, shall have access to appropriate counselling and support services.

Article 72

Seconded national experts and other staff

1. The EU Centre may make use of seconded national experts or other staff not employed by it.

2. The Executive Board shall adopt rules related to staff from Member States, including the contact officers referred to in Article 52, to be seconded to the EU Centre and update them as necessary. Those rules shall include, in particular, the financial arrangements related to those secondments, including insurance and training. Those rules shall take into account the fact that the staff is seconded and to be deployed as staff of the EU Centre. They shall include provisions on the conditions of deployment. Where relevant, the Executive Board shall aim to ensure consistency with the rules applicable to reimbursement of the mission expenses of the statutory staff.

Article 73

Privileges and immunities

Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on the Functioning of the European Union shall apply to the EU Centre and its staff.

Privileges and immunities of contact officers and members of their families shall be subject to an agreement between the Member State where the seat of the EU Centre is located and the other Member States. That agreement shall provide for such privileges and immunities as are necessary for the proper performance of the tasks of contact officers.

Article 74

Obligation of professional secrecy

1. Members of the Management Board and the Executive Board, and all members of the staff of the EU Centre, including officials seconded by Member States on a temporary basis, and all other persons carrying out tasks for the EU Centre on a contractual basis, shall be subject to the requirements of professional secrecy pursuant to Article 339 of the Treaty on the Functioning of the European Union even after their duties have ceased.

2. The Executive Board shall ensure that individuals who provide any service, directly or indirectly, permanently or occasionally, relating to the tasks of the EU Centre, including officials and other persons authorised by the Executive Board or appointed by the coordinating authorities for that purpose, are subject to requirements of professional secrecy equivalent to those in paragraph 1.

3. The EU Centre shall establish practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.

4. The EU Centre shall apply Commission Decision (EU, Euratom) 2015/444[3].

Article 75

Security rules on the protection of classified and sensitive non-classified information

1. The EU Centre shall adopt its own security rules equivalent to the Commission's security rules for protecting European Union Classified Information (EUCI) and sensitive non-classified information, as set out in Commission Decisions (EU, Euratom) 2015/443[4] and (EU, Euratom) 2015/444. The security rules of the EU Centre shall cover, inter alia, provisions for the exchange, processing and storage of such information. The Executive Board shall adopt the EU Centre's security rules following approval by the Commission.

2. Any administrative arrangement on the exchange of classified information with the relevant authorities of a third country or, in the absence of such arrangement, any exceptional ad-hoc release of EUCI to those authorities, shall be subject to the Commission's prior approval.

Section 8

General provisions

Article 76

Language arrangements

The provisions laid down in Regulation No 1[5] shall apply to the EU Centre. The translation services required for the functioning of the EU Centre shall be provided by the Translation Centre for the bodies of the European Union.

---

3 Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

4 Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).

5 Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385/58).

Article 77

Transparency and communication

1. Regulation (EC) No 1049/2001[6] shall apply to documents held by the EU Centre. The Management Board shall, within six months of the date of its first meeting, adopt the detailed rules for applying that Regulation.

2. The processing of personal data by the EU Centre shall be subject to Regulation (EU) 2018/1725. The Management Board shall, within six months of the date of its first meeting, establish measures for the application of that Regulation by the EU Centre, including those concerning the appointment of a Data Protection Officer of the EU Centre. Those measures shall be established after consultation of the European Data Protection Supervisor.

3. The EU Centre may engage in communication activities on its own initiative within its field of competence. Communication activities shall be carried out in accordance with relevant communication and dissemination plans adopted by the Management Board.

Article 78

Anti-fraud measures

1. In order to combat fraud, corruption and other unlawful activities, Regulation (EU, Euratom) No 883/2013[7] shall apply.

2. The EU Centre shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by OLAF within six months from [*date of start of operations as set out in Article 82*] and shall adopt the appropriate provisions applicable to its staff using the template set out in the Annex to that Agreement.

3. The European Court of Auditors shall have the power of audit, on the basis of documents and on the spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the EU Centre.

4. OLAF may carry out investigations, including on-the-spot checks and inspections with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by the EU Centre, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96[8].

---

6 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Official Journal L 145 , 31/05/2001 P. 0043 – 0048.

7 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999. (OJ L 248, 18.9.2013, p. 1).

8 Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities. (OJ L 292, 15.11.1996, p. 2).

5. Without prejudice to paragraphs 1, 2, 3, and 4, cooperation agreements with third countries and international organisations, contracts, grant agreements and grant decisions of the EU Centre shall contain provisions expressly empowering the European Court of Auditors and OLAF to conduct such audits and investigations, in accordance with their respective competences.

Article 79

Liability

1. The EU Centre's contractual liability shall be governed by the law applicable to the contract in question.
2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the EU Centre.
3. In the case of non-contractual liability, the EU Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its departments or by its staff in the performance of their duties.
4. The Court of Justice of the European Union shall have jurisdiction in disputes over compensation for damages referred to in paragraph 3.
5. The personal liability of its staff towards the Centre shall be governed by the provisions laid down in the Staff Regulations or Conditions of Employment applicable to them.

Article 80

Administrative inquiries

The activities of the EU Centre shall be subject to the inquiries of the European Ombudsman in accordance with Article 228 of the Treaty on the Functioning of the European Union.

Article 81

Headquarters Agreement and operating conditions

1. The necessary arrangements concerning the accommodation to be provided for the EU Centre in the Member State where the seat of the EU Centre is located and the facilities to be made available by that Member State, together with the specific rules applicable in that Member State to the Executive Director, members of the Executive Board, EU Centre staff and members of their families shall be laid down in a Headquarters Agreement between the EU Centre and the Member State where the seat of the EU Centre is located, concluded after obtaining the approval of the Executive Board and no later than *[2 years after the entry into force of this Regulation]*.
2. The Member State where the seat of the EU Centre is located shall provide the best possible conditions to ensure the smooth and efficient functioning of the EU Centre, including multilingual, European-oriented schooling and appropriate transport connections.

Article 82

Start of the EU Centre's activities

1. The Commission shall be responsible for the establishment and initial operation of the EU Centre until the Executive Director has taken up his or her duties following his or

her appointment by the Executive Board in accordance with Article 65(2). For that purpose:

(a) the Commission may designate a Commission official to act as interim Executive Director and exercise the duties assigned to the Executive Director;

(b) by derogation from Article 62(2)(g) and until the adoption of a decision as referred to in Article 62(4), the interim Executive Director shall exercise the appointing authority power;

(c) the Commission may offer assistance to the EU Centre, in particular by seconding Commission officials to carry out the activities of the EU Centre under the responsibility of the interim Executive Director or the Executive Director;

(d) the interim Executive Director may authorise all payments covered by appropriations entered in the EU Centre's budget after approval by the Executive Board and may conclude contracts, including staff contracts, following the adoption of the EU Centre's establishment plan.

Relevant recitals (43 - 58, 70)

(43) In the interest of the effective application and, where necessary, enforcement of this Regulation, each Member State should designate at least one existing or newly established authority competent to ensure such application and enforcement in respect of providers of relevant information society services under the jurisdiction of the designating Member State.

(44) In order to provide clarity and enable effective, efficient and consistent coordination and cooperation both at national and at Union level, where a Member State designates more than one competent authority to apply and enforce this Regulation, it should designate one lead authority as the Coordinating Authority, whilst the designated authority should automatically be considered the Coordinating Authority where a Member State designates only one authority. For those reasons, the Coordinating Authority should act as the single contact point with regard to all matters related to ***contributing to the achievements of the objective*** of this Regulation, ***including for recognised organisations providing assistance to victims, education and awareness raising,*** without prejudice to the enforcement powers of other national authorities.

(45) Considering the EU Centre's particular expertise and central position in connection to the implementation of this Regulation, Coordinating Authorities should be able to request the assistance of the EU Centre in carrying out certain of their tasks. Such assistance should be without prejudice to the respective tasks and powers of the Coordinating Authorities requesting assistance and of the EU Centre and to the requirements applicable to the performance of their respective tasks and the exercise of their respective powers provided in this Regulation.

(46) Given the importance of their tasks and the potential impact of the use of their powers for the exercise of fundamental rights of the parties affected, it is essential that Coordinating Authorities are fully independent. To that aim, the rules and assurances applicable to Coordinating Authorities should be similar to those applicable to courts and tribunals, in order to guarantee that they constitute, and can in all respects act as, independent administrative authorities.

(47) The Coordinating Authority, as well as other competent authorities, play a crucial role in ensuring the effectiveness of the rights and obligations laid down in this Regulation and the achievement of its objectives. Accordingly, it is necessary to ensure that those authorities have not only the necessary investigatory and enforcement powers, but also ***all*** necessary ***resources, including sufficient*** financial, human, technological and other resources to ***efficiently*** carry out their tasks under this Regulation. In particular, given the variety of providers of relevant information society services and their use of advanced technology in offering their services, it is essential that the Coordinating Authority, as well as other competent authorities, are equipped with the necessary number of staff, including experts with specialised skills. The resources of Coordinating Authorities should be determined taking into account the size, complexity and potential societal impact of the providers of relevant information society services under the jurisdiction of the designating Member State, as well as the reach of their services across the Union.

(48) Given the need to ensure the effectiveness of the obligations imposed, Coordinating Authorities should be granted enforcement powers to address infringements of this

Regulation. These powers should include the power to temporarily restrict access of users of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider on which the infringement takes place. In light of the high level of interference with the rights of the service providers that such a power entails, the latter should only be exercised when certain conditions are met. Those conditions should include the condition that the infringement results in the regular and structural facilitation of child sexual abuse offences, which should be understood as referring to a situation in which it is apparent from all available evidence that such facilitation has occurred on a large scale and over an extended period of time.

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders, removal orders or blocking orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, using the relevant indicators provided by the EU Centre, to detect the dissemination of ~~known or new child~~ ***online*** sexual abuse material through publicly available material ~~in the hosting services~~ of the providers concerned**.**

(50) With a view to ensuring that providers of hosting services are aware of the misuse made of their services and to afford them an opportunity to take expeditious action to remove or disable access on a voluntary basis, Coordinating Authorities of establishment should be able to notify those providers of the presence of known child sexual abuse material on their services and requesting removal or disabling of access thereof~~, for the providers' voluntary consideration~~. Such notifying activities should be clearly distinguished from the Coordinating Authorities' powers under this Regulation to request the issuance of removal orders, which impose on the provider concerned a binding legal obligation to remove or disable access to the material in question within a set time period.

(51) In order to provide clarity and ensure effective enforcement of this Regulation, a provider of relevant information society services should be under the jurisdiction of the Member State where its main establishment is located, that is, where the provider has its head office or registered office within which the principal financial functions and operational control are exercised. In respect of providers that do not have an establishment in the Union but that offer services in the Union, the Member State where their appointed legal representative resides or is established should have jurisdiction, considering the function of legal representatives under this Regulation.

(52) To ensure effective enforcement and the safeguarding of users' rights under this Regulation, it is appropriate to facilitate the lodging of complaints about alleged non-compliance with obligations of providers of relevant information society services under this Regulation. This should be done by allowing users to lodge such complaints with the Coordinating Authority in the territory of the Member State where the users reside or are established, irrespective of which Member State has jurisdiction in respect of the provider concerned. For the purpose of lodging of complaints, users can decide to rely on organisations acting in the public interest against child sexual abuse. However, in order not to endanger the aim of establishing a clear and effective system of oversight and to avoid the risk of inconsistent decisions, it should remain solely for the Coordinating Authority of establishment to subsequently exercise any of its investigatory or enforcement powers regarding the conduct complained of, as appropriate, without prejudice to the competence of other supervisory authorities within their mandate.

(53) Member States should ensure that for infringements of the obligations laid down in this Regulation there are penalties that are effective, proportionate and dissuasive, taking into account elements such as the nature, gravity, recurrence and duration of the infringement, in view of the public interest pursued, the scope and kind of activities carried out, as well as the economic capacity of the provider of relevant information society services concerned.

(54) The rules of this Regulation on supervision and enforcement should not be understood as affecting the powers and competences of the data protection authorities under Regulation (EU) 2016/679.

(55) It is essential for the proper functioning of the system of mandatory detection and blocking of online child sexual abuse set up by this Regulation that the EU Centre receives, via the Coordinating Authorities, ***the encrypted copies of specific items of*** material identified as constituting child sexual abuse material or transcripts of conversations identified as constituting the solicitation of children, ***related to a specific person or a specific group of people or specific incident***, such as may have been found for example during criminal investigations, so that that material or conversations can serve as an accurate and reliable basis for the EU Centre to generate indicators of such abuses. In order to achieve that result, the identification should be made after a diligent assessment, conducted in the context of a procedure that guarantees a fair and objective outcome, either by the Coordinating Authorities themselves or by a court or another independent administrative authority than the Coordinating Authority. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to ~~new~~ child sexual abuse material ~~and the solicitation of children~~ reported under this Regulation, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting**.**

(56) With a view to ensuring that the indicators generated by the EU Centre for the purpose of detection are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material or conversations to the attention of the Coordinating Authorities for those purposes.

(57) Certain providers of relevant information society services offer their services in several or even all Member States, whilst under this Regulation only a single Member State has jurisdiction in respect of a given provider. It is therefore imperative that the Coordinating Authority designated by the Member State having jurisdiction takes account of the interests of all users in the Union when performing its tasks and using its powers, without making any distinction depending on elements such as the users' location or nationality, and that Coordinating Authorities cooperate with each other in an effective and efficient manner. To facilitate such cooperation, the necessary mechanisms and information-sharing systems should be provided for. That cooperation shall be without prejudice to the possibility for Member States to provide for regular exchanges of views with other public authorities where relevant for the performance of the tasks of those other authorities and of the Coordinating Authority.

(58) In particular, in order to facilitate the cooperation needed for the proper functioning of the mechanisms set up by this Regulation, the EU Centre should establish and maintain the necessary information-sharing systems. When establishing and maintaining such systems, the EU Centre should cooperate with the European Union Agency for Law

Enforcement Cooperation ('Europol') and national authorities to build on existing systems and best practices, where relevant.

(59) To support the implementation of this Regulation and contribute to the achievement of its objectives, the EU Centre should serve as a central facilitator, carrying out a range of specific tasks. The performance of those tasks requires strong guarantees of independence, in particular from law enforcement authorities, as well as a governance structure ensuring the effective, efficient and coherent performance of its different tasks, and legal personality to be able to interact effectively with all relevant stakeholders. Therefore, it should be established as a decentralised Union agency.

(60) In the interest of legal certainty and effectiveness, the tasks of the EU Centre should be listed in a clear and comprehensive manner. With a view to ensuring the proper implementation of this Regulation, those tasks should relate in particular to the facilitation of the detection, reporting and blocking obligations imposed on providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services. However, for that same reason, the EU Centre should also be charged with certain other tasks, notably those relating to the implementation of the risk assessment and mitigation obligations of providers of relevant information society services, the removal of or disabling of access to child sexual abuse material by providers of hosting services, the provision of assistance to Coordinating Authorities, as well as the generation and sharing of knowledge and expertise related to online child sexual abuse.

(61) The EU Centre should provide reliable information on which activities can reasonably be considered to constitute online child sexual abuse, so as to enable the detection and blocking thereof in accordance with this Regulation. Given the nature of child sexual abuse material, that reliable information needs to be provided without sharing the material itself. Therefore, the EU Centre should generate accurate and reliable indicators, based on identified child sexual abuse material and solicitation of children submitted to it by Coordinating Authorities in accordance with the relevant provisions of this Regulation. These indicators should allow technologies to detect the dissemination of either the same material (known material) or of different child sexual abuse material (new material), or the solicitation of children, as applicable.

(62) For the system established by this Regulation to function properly, the EU Centre should be charged with creating databases for each of those three types of online child sexual abuse, and with maintaining and operating those databases. For accountability purposes and to allow for corrections where needed, it should keep records of the submissions and the process used for the generation of the indicators.

(63) For the purpose of ensuring the traceability of the reporting process and of any follow-up activity undertaken based on reporting, as well as of allowing for the provision of feedback on reporting to providers of hosting services and providers of publicly available interpersonal communications services, generating statistics concerning reports and the reliable and swift management and processing of reports, the EU Centre should create a dedicated database of such reports. To be able to fulfil the above purposes, that database should also contain relevant information relating to those reports, such as the indicators representing the material and ancillary tags, which can indicate, for example, the fact that a reported image or video is part of a series of images and videos depicting the same victim or victims.

(64) Given the sensitivity of the data concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of indicators and databases of reports, on the data contained therein and on their security. In particular, the data concerned should not be stored for longer than is strictly necessary. For the above reasons, access to the database of indicators should be given only to the parties and for the purposes specified in this Regulation, subject to the controls by the EU Centre, and be limited in time and in scope to what is strictly necessary for those purposes.

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU Centre should assess those reports in order to identify those that are manifestly unfounded, that is, where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is manifestly unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

(66) With a view to contributing to the effective application of this Regulation and the protection of victims' rights, the EU Centre should be able, upon request, to support victims and to assist Competent Authorities by conducting searches of hosting services for the dissemination of known child sexual abuse material that is publicly accessible, using the corresponding indicators. Where it identifies such material after having conducted such a search, the EU Centre should also be able to request the provider of the hosting service concerned to remove or disable access to the item or items in question, given that the provider may not be aware of their presence and may be willing to do so on a voluntary basis.

(67) Given its central position resulting from the performance of its primary tasks under this Regulation and the information and expertise it can gather in connection thereto, the EU Centre should also contribute to the achievement of the objectives of this Regulation by serving as a hub for knowledge, expertise and research on matters related to the prevention and combating of online child sexual abuse. In this connection, the EU Centre should cooperate with relevant stakeholders from both within and outside the Union and allow Member States to benefit from the knowledge and expertise gathered, including best practices and lessons learned.

(68) Processing and storing certain personal data is necessary for the performance of the EU Centre's tasks under this Regulation. In order to ensure that such personal data is adequately protected, the EU Centre should only process and store personal data if strictly necessary for the purposes detailed in this Regulation. It should do so in a secure manner and limit storage to what is strictly necessary for the performance of the relevant tasks.

(69) In order to allow for the effective and efficient performance of its tasks, the EU Centre should closely cooperate with Coordinating Authorities, the Europol and relevant partner organisations, such as the US National Centre for Missing and Exploited Children or the International Association of Internet Hotlines ('INHOPE') network of

hotlines for reporting child sexual abuse material, within the limits sets by this Regulation and other legal instruments regulating their respective activities. To facilitate such cooperation, the necessary arrangements should be made, including the designation of contact officers by Coordinating Authorities and the conclusion of memoranda of understanding with Europol and, where appropriate, with one or more of the relevant partner organisations.

(70) ***Hotlines play a very important role in the fight against child sexual abuse online at Union level, namely with regard to reporting, detection and rapid removal of child sexual abuse material. Help-lines are also essential in providing support for children in need.*** Longstanding Union support for both INHOPE and its member hotlines recognises that hotlines are in the frontline in the fight against online child sexual abuse. The EU Centre should leverage the network of hotlines and encourage that they ~~work together~~ ***cooperate and coordinate*** effectively with the Coordinating Authorities, providers of relevant information society services and law enforcement authorities of the Member States. The hotlines' expertise and experience is an invaluable source of information on the early identification of common threats and solutions, as well as on regional and national differences across the Union. ***Member States are therefore encouraged to further enhance the operational capacities of hotlines and help-line.***

(71) Considering Europol's mandate and its experience in identifying competent national authorities in unclear situation and its database of criminal intelligence which can contribute to identifying links to investigations in other Member States, the EU Centre should cooperate closely with it, especially in order to ensure the swift identification of competent national law enforcement authorities in cases where that is not clear or where more than one Member State may be affected.

(72) Considering the need for the EU Centre to cooperate intensively with Europol, the EU Centre's headquarters should be located alongside Europol's, which is located in The Hague, the Netherlands. The highly sensitive nature of the reports shared with Europol by the EU Centre and the technical requirements, such as on secure data connections, both benefit from a shared location between the EU Centre and Europol. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol, notably those regarding human resources management, information technology (IT), including cybersecurity, the building and communications. Sharing such support services is more cost-efficient and ensure a more professional service than duplicating them by creating them anew.

(73) To ensure its proper functioning, the necessary rules should be laid down regarding the EU Centre's organisation. In the interest of consistency, those rules should be in line with the Common Approach of the European Parliament, the Council and the Commission on decentralised agencies.

(74) In view of the need for technical expertise in order to perform its tasks, in particular the task of providing a list of technologies that can be used for detection, the EU Centre should have a Technology Committee composed of experts with advisory function. The Technology Committee may, in particular, provide expertise to support the work of the EU Centre, within the scope of its mandate, with respect to matters related to detection of online child sexual abuse, to support the EU Centre in contributing to a high level of technical standards and safeguards in detection technology.

Batch 8

Compromise amendment on Chapter V and VI
Compromise amendment replacing all relevant amendments, including AMs 641, 154, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 155, 669, 156, 670, 157 and 234

Article 83

Data collection

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

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

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

      – the ~~error~~ rates of ***false positives and false negatives*** the technologies deployed to detect online child sexual abuse, ~~and~~ measures taken to prevent or remedy any errors and ***steps taken to mitigate the harm caused by any inaccuracy;***

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

   (b) the number of removal orders issued to the provider in accordance with Article 14 and the ~~average~~ ***median*** time ~~needed~~ for removing or disabling access to the item or items of child sexual abuse material in question***, counting from the moment the order entered the provider's system***;

   (b a) the number and duration of delayed ~~s to~~ removals, requested by competent authorities or law enforcement authorities for the integrity of the investigations;

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

   (c a) the number of instances the provider was asked to provide additional support to law enforcement authorities in relation to content that was removed;

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

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

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

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

– ***the nature of the report and its key characteristics;***

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

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

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

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

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

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

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

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

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

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

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

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

3. The EU Centre shall collect data and generate statistics on the detection, reporting, removal of or disabling of access to online child sexual abuse under this Regulation. The data shall ***include*** ~~be in particular on the following topics~~:

(a) the number of indicators in the databases of indicators referred to in Article 44 and the ~~development~~ ***change*** of that number as compared to previous years;

(b) the number of submissions of child sexual abuse material and solicitation of children referred to in Article 36(1), broken down by Member State that designated the submitting Coordinating Authorities, and, in the case of child sexual abuse material, the number of indicators generated on the basis thereof and the number of ***still active*** uniform resource locators included in the list of uniform resource locators in accordance with Article 44(3);

(c) the total number of reports submitted to the EU Centre in accordance with Article 12, broken down by provider of hosting services and provider ***of number-independent*** interpersonal communications services that submitted the report and by Member State the competent authority of which the EU Centre forwarded the reports to in accordance with Article 48(3);

(d) the online child sexual abuse to which the reports relate, including the number of items of potential ~~known and new~~ child sexual abuse material and instances of potential solicitation of children, the Member State the competent authority of which the EU Centre forwarded the reports to in accordance with Article 48(3), and type of relevant information society service that the reporting provider offers;

(e) the number of reports that the EU Centre considered ***unfounded or*** manifestly unfounded, as referred to in Article 48(2);

(f) the number of reports relating to potential child sexual abuse material and solicitation of children that were assessed as not constituting child sexual abuse material of which the EU Centre was informed pursuant to Article 36(3), broken down by Member State;

(g) the results of the searches in accordance with Article 49(1), including the number of images, videos and URLs by Member State where the material is hosted;

(h) where the same item of potential child sexual abuse material was reported more than once to the EU Centre in accordance with Article 12 or detected more than once through the searches in accordance with Article 49(1), the number of times that that item was reported or detected in that manner.

(i) the number of notices and number of providers of hosting services notified by the EU Centre pursuant to Article 49(2);

(j) number of victims of online child sexual abuse assisted by the EU Centre pursuant to Article 21(2), and the number of these victims that requested to receive such assistance in a manner accessible to them due to disabilities.

4. The providers of hosting services, providers of interpersonal communications services and providers of internet access services, the Coordinating Authorities and the EU Centre shall ensure that the data ***stored*** referred to in paragraphs 1, 2 and 3, respectively, is stored no longer than is necessary for the transparency reporting referred to in Article 84. The data stored shall not contain any personal data.

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

Article 84

Transparency reporting

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

1 a. The annual report shall also include the following information:

(a) the number and subject matter of detection orders and removal orders to act against alleged online child sexual abuse and the number of notifications received in accordance with Article 32 and the effects given to those orders;

(b) the number of notifications and requests received pursuant to Articles 8a and 35a and an overview of their follow-up;

(c) the number of users affected by detection and removal orders;

(d) information on the effectiveness of the different technologies used and on the false positive and false negative rates of those technologies, as well as statistics on appeals and the effect they have on the users of its services and information of the effectiveness of the measures and obligations under Articles 3, 4, 5 and 7;

(e) information on the tools used by the provider to become aware of the reported online child sexual abuse, including data and aggregate statistics on how technologies used by the provider work.

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

3. Where a Member State has designated several competent authorities pursuant to Article 25, it shall ensure that the Coordinating Authority draws up a single report

covering the activities of all competent authorities under this Regulation and that the Coordinating Authority receives all relevant information and support needed to that effect from the other competent authorities concerned.

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

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

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

CHAPTER VI

FINAL PROVISIONS

Article 85

Evaluation

1. By [*five years after the entry into force of this Regulation*], and every five years thereafter, the Commission shall evaluate this Regulation and submit a report on its application to the European Parliament and the Council. ***The implementation report shall address, among others the possible use of new technologies, their impact, effectiveness and accuracy for the purpose of combating online child sexual abuse*** ~~***and in particular to detect, report and remove online child sexual abuse***~~***. The report shall be accompanied, where appropriate, by an impact assessment and a legislative proposal.***

1 a ***By [two years after the entry into force of this Regulation] the Commission shall carry out an evaluation on the effectiveness of the detection order in relation to the amount of detected child sexual abuse material compared to the years before the entry into force of this Regualtion. The Commission shall submit a report on its main findings to the European Parliament and the Council. The report shall be accompanied, where appropriate, by an impact assessment and a legislative proposal.***

2. By [*five years after the entry into force of this Regulation*], and every five years thereafter, the Commission shall ensure that an evaluation in accordance with Commission guidelines of the EU Centre's performance in relation to its objectives, mandate, tasks and governance and location is carried out. The evaluation shall, in particular, address the possible need to modify the tasks of the EU Centre, and the financial implications of any such modification.

3. On the occasion of every second evaluation referred to in paragraph 2, the results achieved by the EU Centre shall be assessed, having regard to its objectives and tasks, including an assessment of whether the continuation of the EU Centre is still justified with regard to those objectives and tasks.

4. The Commission shall report to the European Parliament and the Council the findings of the evaluation referred to in paragraph 3. The findings of the evaluation shall be made public.

5. For the purpose of carrying out the evaluations referred to in paragraphs 1, 2 and 3, the Coordinating Authorities and Member States and the EU Centre shall provide information to the Commission at its request.

6. In carrying out the evaluations referred to in paragraphs 1, 2 and 3, the Commission shall take into account the relevant evidence at its disposal.

7. Where appropriate, the reports referred to in paragraphs 1 and 4 shall be accompanied by legislative proposals.

Article 86

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 3, 8, 13, 14, 17, 47 and 84 shall be conferred on the Commission for ***a*** period of ***5 years*** from [date of adoption of the Regulation]. ***The Commission shall draw up a report in respect of the delegation of power not later than 9 months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than 3 months before the end of each period.***

3. The delegation of power referred to in Articles 3, 8, 13, 14, 17, 47 and 84 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day after the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 3, 8, 13, 14, 17, 47 and 84 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 87

Committee procedure

1. For the purposes of the adoption of the implementing acts referred to in Article 39(4), the Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

Article 88

Repeal

Regulation (EU) 2021/1232 is repealed from [*date of application of this Regulation*].

Article 89

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 6 months after its entry into force.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

Relevant recitals (75- 84):

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available ***number-independent*** interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on anonymised gathering of non-personal data and to publish ***in a machine-readable format*** annual reports on their activities under this Regulation. The Coordinating Authorities should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

(76) In the interest of good governance and drawing on the statistics and information gathered and transparency reporting mechanisms provided for in this Regulation, the Commission should carry out an evaluation of this Regulation within five years of the date of its entry into force, and every five years thereafter.

(77) The evaluation should be based on the criteria of efficiency, necessity, effectiveness, proportionality, relevance, coherence and Union added value. It should assess the functioning of the different operational and technical measures provided for by this Regulation, including the effectiveness of measures to enhance the detection, reporting and removal of online child sexual abuse, the effectiveness of safeguard mechanisms, ***the possible use of new technologies, their impact, effectiveness and accuracy for the purpose of combating online child sexual abuse*** as well as the impacts on potentially affected fundamental rights, the freedom to conduct a business, the right to private life and the protection of personal data. The Commission should also assess the impact on potentially affected interests of third parties.

(78) Regulation (EU) 2021/1232 of the European Parliament and of the Council[9] provides for a temporary solution in respect of the use of technologies by certain providers of publicly available ***number-independent*** interpersonal communications services for the purpose of combating online child sexual abuse~~, pending the preparation and adoption of a long-term legal framework. This Regulation provides that long-term legal framework~~ . Regulation (EU) 2021/1232 should therefore be repealed.

(79) In order to achieve the objectives of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to amend the Annexes to this Regulation and to supplement it by laying down detailed rules concerning the setting up, content and access to the databases operated by the EU Centre, concerning the form, precise content and other details of the reports and the reporting process, concerning the determination and charging of the costs incurred by the EU Centre to support providers in the risk assessment, as well as concerning technical requirements for the information sharing systems supporting communications between Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services.

(80) It is important that the Commission carry out appropriate consultations during its preparatory work for delegated acts, including via open public consultation and at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law Making[10]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of the Commission expert groups dealing with the preparation of delegated acts.

(81) In order to ensure uniform conditions for the implementation of the information-sharing system, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[11].

---

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

10 Inter-institutional Agreement of 13 April 2016 on Better Law Making (OJ L 123, 12.5.2016, p. 1).

11 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(82) In order to allow all affected parties sufficient time to take the necessary measures to comply with this Regulation, provision should be made for an appropriate time period between the date of its entry into force and that of its application.

(83) Since the objectives of this Regulation, namely contributing to the proper functioning of the internal market by setting out clear, uniform and balanced rules to prevent and combat child sexual abuse in a manner that is effective and that respects the fundamental rights, cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(84) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[12] and delivered their opinion on […].

[12] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).