Council of the European Union

Brussels, 14 June 2024
(OR. en)

11277/24

Interinstitutional File: 2022/0155(COD)

LIMITE

JAI 1059
ENFOPOL 307
CRIMORG 98
IXIM 167
DATAPROTECT 243
CYBER 199
COPEN 323
FREMP 306
TELECOM 213
COMPET 682
MI 624
CONSOM 224
DIGIT 161
CODEC 1557

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	9093/24
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Partial mandate for negotiations with the European Parliament

I. BACKGROUND/INTRODUCTION

1. On 11 May 2022, the Commission submitted to the Council and the European Parliament a proposal for a Regulation laying down rules to prevent and combat child sexual abuse[1], which aims to oblige online service providers, such as providers of hosting services and interpersonal communication services, to prevent the dissemination, detect, report and remove child sexual abuse material ('CSAM'), to prevent, detect and report the solicitation of children ('grooming'), and to set up a new decentralised EU agency (the 'EU Centre') to support the

[1] 9068/22.

implementation of the proposed Regulation, together with a network of national Coordinating Authorities and other competent authorities.

2. The draft Regulation is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU) (ordinary legislative procedure).

3. The European Data Protection Board and the European Data Protection Supervisor adopted a joint opinion on 28 July 2022.

4. The European Economic and Social Committee adopted an opinion on 21 September 2022.

5. The Council Legal Service issued a written opinion on 26 April 2023[2].

6. The Law Enforcement Working Party - Police (LEWP-P) discussed the proposal at its meetings on 18 May 2022, 22 June 2022, 5 July 2022, 20 July 2022, 6 September 2022, 22 September 2022, 5 October 2022, 19 October 2022, 3 November 2022, 24 November 2022, 19 and 20 January 2023, 24 February 2023, 16 March 2023, 29 March 2023, 13 April 2023, 27 and 28 April 2023, 12 May 2023, 25 and 26 May 2023, 2 June 2023, 13 June 2023, 5 July 2023, 26 July 2023, 5 September 2023, 14 September 2023, 1 March 2024, 19 March 2024, 3 April 2024, 15 April 2024, 8 May 2024, 24 May 2024 and 4 June 2024 with a view to preparing a mandate for negotiations with the European Parliament.

7. In the European Parliament, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) has the lead responsibility for the negotiations on the proposal. It appointed MEP Javier Zarzalejos (EPP, ES) as rapporteur in October 2022. The LIBE Committee adopted its report on 14 November 2023, and the position of the European Parliament was deemed adopted on 22 November 2023.

8. Article 42 of this Regulation about the seat of the EU Centre to prevent and combat child sexual abuse is excluded from the text for the partial negotiation mandate. The selection of the seat is subject to an inter-institutional agreement on the selection procedure applicable to new EU agencies following the example of the selection of the seat of the future Anti-Money Laundering Authority.

---

[2] 8787/23.

II. MAIN ELEMENTS OF THE PRESIDENCY COMPROMISE TEXT

9. The Presidency compromise text amends the Commission's proposal on several aspects. It aims at addressing the concerns of delegations expressed at the meetings of the Law Enforcement Working Party – Police by adding further safeguards to protect cyber security and to ensure proportionality and the respect to fundamental rights, while preserving the objectives and the effectiveness of the proposed Regulation. The main elements of the compromise are set out below:

a) General provisions (Article 1(5)):
   - Cyber security and encryption are protected in a comprehensive way.

b) Risk assessment and mitigation obligations by providers (Articles 3 to 5b, Recitals 14-18c):
   - An enhanced risk assessment and a risk categorisation of services is introduced with a methodology for determining the risk of specific services based on a set of objective criteria (related to the size, type and core architecture of the service, the provider's policies and safety by design functionalities and a mapping of users' tendencies);
   - Following the outcome of this risk categorisation process, systems or parts thereof will be classified as 'high risk', 'medium risk' or 'low risk'. Based on this categorisation, additional risk mitigation measures can be imposed on the providers classified in the medium and high-risk categories;
   - In case significant risks still prevail after the implementation of the additional risk mitigation measures, the Coordinating Authority may consider requesting the issuance of a detection order as a measure of last resort to services that are classified as high risk;
   - Providers can also flag voluntarily to the Coordinating Authority of establishment whether they have suspicions of their services being used for child sexual abuse that might require issuing detection orders;
   - The possibility for the Coordinating Authority to authorise relevant providers to display a "sign of reduced risk" is introduced.

POLITICO

c) Detection orders (Articles 7 to 11, 22a, Recitals 20-28):

- Detection in interpersonal communication including in services using end-to-end encryption is enabled via upload moderation requiring the users' consent;
- Technologies used for detection have to be vetted with regard to their effectiveness, their impact on fundamental rights and risks to cyber security and be approved by implementing act, with specific safeguards applying to technologies for detection in services using end-to-end encryption;
- The scope of detection orders is limited to visual content and URLs, while text and audio content are excluded, which still allows to detect the solicitation of children to some extent;
- The application of detection orders to new child sexual abuse material is subject to delayed reporting after two hits to reduce false positives, and the pseudonymisation of detected material prior to human verification;
- Requirements for independent administrative authorities issuing detection orders are added, and the Coordinating Authorities of establishment may issue detection orders subject to prior authorisation by a judicial authority or an independent administrative authority;
- The possibility for the Coordinating Authority to request the EU Centre to conduct tests on the service in question to gather evidence and objective indications of a significant risk of online child sexual abuse is provided;
- Detection will not apply to accounts used by the State for national security purposes, maintaining law and order or military purposes;
- The obligation for relevant providers to keep logs of data related to detection orders is added.

d) Removal, blocking and delisting orders (Articles 2(x), 14 to 18c, Recitals 30-33b)

- The delisting order is introduced as a new measure and online search engines are added to the list of relevant information society services;
- A procedure for cross-border removal and delisting orders has been established, following largely the model of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

POLITICO

e) Authorities of the Member States (Articles 2(ta), 25-26, 38a, Recitals 45-46b)

- The concept of "competent authority of establishment" is introduced;
- The possibility for Member States to designate more than one competent authority is provided;
- A legal basis for the mutual assistance among the competent authorities of the Member States is provided.

f) EU Centre to prevent and combat child sexual abuse (Articles 40-82, Recitals 58-74a):

- The tasks of the EU Centre are expanded to assist more strongly in the risk assessment and mitigation process, to conduct simulation tests in connection with the possible issuance of detection orders, to support the vetting of detection technologies, and to develop or facilitate the development of technologies;
- Clarifications about the cooperation between the EU Centre and Europol are included;
- The possibility for the cooperation of the EU Centre with other EU agencies and bodies, third countries and international organisations is introduced;
- The tasks of the Executive Board, which should not be established, are conferred on the Management Board of the EU Centre;
- Rules for the nomination and the appointment of the members of the Technology Committee and the establishment of a Victims Board, both advising the EU Centre, are introduced;
- The tasks of the Technology Committee have been expanded to contribute to the EU Centre's work with regard to the vetting and further development of detection technologies;
- The budgetary provisions are aligned with the Framework Financial Regulation, notably to include the Single Programming Document, the need to take into account the recommendations of the European Court of Auditors for final accounts and the voluntary financial contribution from Member States and third countries.

g) Evaluation (Article 85, Recitals 75-77)

- Specifications about the evaluation to be carried out by the Commission five years after the entry into force of this Regulation for the first time are introduced.

POLITICO

h) Amendment of the "Temporary Regulation"[3] (Article 88, Recital 78)

- The extension of the application of the Temporary Regulation until 54 months after the entry into force of this Regulation is introduced to enable the continuation of the current regime of voluntary detection for the period of transition to the long-term framework.

i) Entry into force and application (Article 89, Recital 78a)

- The Presidency text foresees that this Regulation will apply 24 months after its entry into force, the provisions related to detection orders after 48 months and the amendments to the Temporary Regulation immediately.

j) Other changes emphasised by the Presidency:

- Safeguards regarding the age verification and age assessment measures applied by relevant providers are introduced in Article 6)(1)(c) and Recital 16a;
- The possibility for users to be represented by a body in complaint procedures is introduced in Articles 34-34a.

III. CONCLUSION

10. The Permanent Representatives Committee is invited to confirm agreement on the text of the partial mandate for negotiations with the European Parliament, as set out in the annex to this note[4], to enable the Presidency to conduct those negotiations.

11. In accordance with the approach to legislative transparency endorsed by Coreper on 14 July 2020[5], and in full consistency with Regulation (EC) 1049/2001 and the Council's Rules of Procedure, the text of the mandate thus agreed will be made public unless the Permanent Representatives Committee objects.

---

3 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, amended by Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024.

4 Changes to the Commission proposal are marked in **bold** and ~~strikethrough~~.

5 9493/20.

POLITICO

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Having regard to the opinion of the European Data Protection Board and the European Data Protection Supervisor[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(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 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, especially by children.

---

1 OJ C , , p. .
2 OJ C , , p. .
3 OJ C , , p. .

(2) Given the central importance of relevant information society services, those 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 misused for the purpose of child sexual abuse, those providers often being the only ones in a position to prevent and combat such abuse. The measures taken should be targeted, carefully balanced and proportionate, 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 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. In the light of the inherently cross-border nature of the internet and the service provision concerned, those national laws, which diverge, 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 and 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.

(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 include publicly available interpersonal communications services, such as messaging services and web-based e-mail services, in so far as those service**s** ~~as~~ **are** publicly available. 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 gaming, image-sharing and video-hosting are equally at risk of misuse, they should also be covered by this Regulation. 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.

(6) Online child sexual abuse frequently involves 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[4], Directive 2000/31/EC of the European Parliament and of the Council[5] and Regulation (EU) **2022/2065** ~~…/… of the European Parliament and of the Council[6] [*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 [7,] Regulation (EU) 2016/679 of the European Parliament and of the Council[8], and Directive 2002/58/EC of the European Parliament and of the Council[9].

POLITICO

4 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).

5 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).

6 Regulation (EU) **2022/2065** ~~…/…~~ 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 ….).

7 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).

8 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).

9 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).

(8) This Regulation should be considered *lex specialis* in relation to the generally applicable framework set out in Regulation (EU) **2022/2065** ~~…/… of the European Parliament and of the Council~~[10] ~~[*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** ~~…/… of the European Parliament and of the Council~~[11] ~~[*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** ~~…/… of the European Parliament and of the Council~~[12] ~~[*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~.

POLITICO

---

10 Regulation (EU) ~~…/…~~ **2022/ 2065** 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 ….).

11 Regulation (EU) ~~…/…~~ **2022/2065** 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 ….).

12 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 ….).

(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 basis of the existence of a significant number of users in one or more Member States, 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[13]. Mere technical accessibility of a website from the Union should not, 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.

(12a) In the light of the more limited risk of their use for the purpose of child sexual abuse and the need to preserve confidential information, including classified information, information covered by professional secrecy and trade secrets, electronic communications services that are not publicly available, such as those used for national security purposes, should be excluded from the scope of this Regulation. Accordingly, this Regulation should not apply to interpersonal communications services that are not available to the general public and the use of which is instead restricted to persons involved in the activities of a particular company, organisation, body or authority.

POLITO

[13] 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).

(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.

(14) With a view to minimising the risk that their services are misused 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 interpersonal communications services should assess such risk for each of the services that they offer in the Union. To guide their risk assessment, a non-exhaustive list of elements 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 is updated regularly and when needed for particular reasons.

(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** ~~…/… of the European Parliament and of the Council~~[14] ~~[*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. For the purposes of the present Regulation, 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.

POLITO

[14] Regulation (EU) ~~…/…~~ **2022/2065** 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 ….).

(16) In order to prevent and combat online child sexual abuse effectively, providers of hosting services and providers of publicly available interpersonal communications services should take reasonable measures to mitigate the risk of their services being misused for such abuse, as identified through the risk assessment. Providers subject to an obligation to adopt mitigation measures pursuant to Regulation (EU) **2022/2065** ~~…/… of the European Parliament and of the Council~~[15] ~~[*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.

(16a) Age verification and age assessment measures taken under this Regulation should preserve privacy, respecting the principles relating to the processing of personal data, notably the principles of lawfulness, purpose limitation and data minimisation, including by being in compliance with Regulation (EU) 2016/679. Those measures should take as a primary consideration the best interest of the child, including the protection of their personal data, be proportionate, transparent, effective and accurate. The obligation to ensure data protection by design and default is of particular importance to protect the personal data of children while ensuring a safe online environment for children. The age verification and age assessment measures should also be non-discriminatory and accessible.

(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 measures tailored to the risk identified and the characteristics of the services they provide and the manners in which those services are used. 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 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.

POLITO

15 Regulation (EU) ~~…/…~~ **2022/2065** 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 ….).

(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 interpersonal communications services should, when designing and implementing the mitigation measures, give importance not only to ensuring their effectiveness, but also 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. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

(18a) In the interest of ensuring effective oversight and compliance, and given the importance of ensuring that all possible risk mitigation measures have been taken in accordance with this Regulation prior to the issuance of any detection order, the Coordinating Authorities should be granted specific powers to require providers of hosting services or providers of interpersonal communications services to adjust their risk assessment or mitigation measures so as to ensure compliance with the relevant requirements of this Regulation. Those specific powers should leave the Coordinating Authorities' general investigatory and enforcement powers under this Regulation unaffected. Therefore, imposing such a requirement regarding the further risk assessment or mitigation measures could be combined, where appropriate, with other investigatory or enforcement measures, such as imposing a periodic penalty payment to ensure compliance with that requirement or imposing a fine for failure to comply with this Regulation.

POLITO

(18b) With a view to make risk mitigation measures and detection orders more targeted, the services or parts or components thereof should be categorised according to their risks based on objective criteria and a methodology established in this Regulation that may be updated, if required due to technological developments, by a delegated act of the Commission. Following the risk assessment and the mitigation measures put in place by the providers, their reports to the Coordinating Authority of establishment should include a self-assessment facilitating the categorisation of services by the Coordinating Authority of establishment. The risk categorisation, decided by the Coordinating Authority of establishment, taking into account the risk assessment and the risk mitigation measures already undertaken by the providers and the self-assessment by the providers, would have as objective to determine the risk level of services or parts and components thereof. The EU Centre could support the Coordinating Authority of establishment by providing an assessment of the effectiveness of the mitigation measures, technical expertise on the technologies put in place as part of the mitigation measures or by testing the services. Based on this categorisation decision, the Coordinating Authority of establishment can impose additional risk mitigation measures on the providers classified in the medium and high-risk categories. Supposing significant risks still prevail after the implementation of the additional risk mitigation measures, the Coordinating Authority may consider making a request to a competent judicial authority to issue a detection order as a measure of last resort to services or parts or components thereof that are classified as high risk. Providers may flag voluntarily to the Coordinating Authority of establishment whether there is suspicion of their services being used for child sexual abuse that might require the issuing of detection orders.

POLITICO

(18c) In order to increase transparency, providers of hosting services and providers of interpersonal communications services should be provided with the possibility to inform their users in an easily recognisable and officially authorised manner as regards their compliance with relevant parts of this Regulation. They should therefore be authorised, upon their request, to display a sign of reduced risk when the Coordinating Authority considers that they have carried out the risk assessment and have taken all reasonable risk mitigation measures in accordance with this Regulation, and that there is no need to initiate the process for the issuance of a detection order. These providers should make clear to users that the sign of reduced risk should not be understood as indicating that the risk of online child sexual abuse is completely eliminated. Coordinating Authorities may require these providers to conduct more frequent risk assessments or to take other measures, including by providing additional information, where necessary for it to be able to verify that the conditions for the authorisation to display the sign of reduced risk continue to be met. In any case, the Coordinating Authority that issued the authorisation for a service provider to display such a sign of reduced risk should reassess at least every 6 months whether the conditions for this authorisation are still met.

(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 obligations to take certain reasonable measures to 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.

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, ~~when~~ **after** mitigating measures ~~are~~ **have been** deemed insufficient to limit the risk of misuse 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 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 limits and safeguards. For instance, considering that child sexual abuse material tends to be disseminated through hosting services and publicly available 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.

(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 risk of the specific service concerned being misused 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 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 likelihood and seriousness of any potential negative consequences for other parties affected. 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.

(22a) With a view to establishing that there are objective indications about the existence of a significant risk that might require the issuing of a detection order, the Coordinating Authority of establishment should provide the competent judicial authority with information that the service or parts or components of the service have been used for online child sexual abuse and that the risk mitigation measures have not been sufficient to mitigate that significant risk.

POLITO

(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 and specified 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 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 interpersonal communications service, or to specific users or specific groups **or types** of users, to the extent that they can be taken in isolation 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) To further avoid undue interference with fundamental rights and ensure proportionality, detection orders should cover only visual content, which should be understood as images and the visual components of videos, including charts, infographics, logos, animations, iconography, gifs, stickers or the visual components of livestreaming, and URLs, while the detection of audio communication and text should be excluded. Despite that limitation of detection to images and the visual components of videos, the solicitation of children could still be identified to some extent through the detection of visual material exchanged. To increase the accuracy of detection, the reporting by providers of hosting services and providers of publicly available interpersonal communications services on potential online new child sexual abuse material should be limited to that material either notified to them by a user or detected repeatedly on their services. As an additional safeguard to protect privacy, the reporting to the EU Centre of potential new child sexual abuse material detected in the service of a provider, should be done in a pseudonymized way, so that the personal data cannot be attributed to a specific data subject prior to human verification.

(23b) In order to ensure that users are appropriately informed and that affected users can exercise their right of redress, providers of hosting services or of interpersonal communications services that received a detection order issued under this Regulation should be required to provide certain specific information in connection to the measures taken pursuant to those orders. That requirement should not preclude those service providers from providing additional information on a voluntary basis. However, no such required or voluntary provision of information should reduce the effectiveness of the measures in question. In addition, that requirement should be without prejudice to any other obligations to provide information pursuant to other acts of Union law, in particular Regulation (EU) 2016/679.

(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 be in a position to take a well-informed decision on requests for the issuance **or for authorising the issuing by the Coordinationg Authority of establishment** 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~~. Therefore, 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. **In this regard, the national data protection authorities should, where appropriate, cooperate with other competent national authorities, in particular those referred to in Article 15a(3) of Directive 2002/58/EC and in Article 5 of Directive (EU) 2018/1972.** They should do so 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.

POUCO

(26) The measures taken by providers of hosting services and providers of publicly available 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. 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. **Having regard to the availability of technologies that can be used to meet the requirements of this Regulation whilst still allowing for end-to-end encryption, nothing in this Regulation should be interpreted as prohibiting, requiring to disable, or making end-to-end encryption impossible. Providers should remain free to offer services using end-to-end encryption and should not be obliged by this Regulation to decrypt data or create access to end-to-end encrypted data.** 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, and thus to avoid undermining **cyber**security and **the** confidentiality of the communications of users, **while ensuring the effective detection of online child sexual abuse and the fair balance of all the fundamental rights at stake**. **To avoid the significant impairment of cybersecurity, providers should identify, analyse and assess the possible cybersecurity risks derived from the implementation of the technologies used to execute the detection order and put in place the necessary mitigation measures to minimise such risks.**

(26a) While end-to-end encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society, the European Union needs to ensure the effective prevention of and fight against serious crime such as child sexual abuse. Providers should therefore not be obliged to prohibit or make impossible end-to-end encryption. Nonetheless, it is crucial that services employing end-to-end encryption do not inadvertently become secure zones where child sexual abuse material can be shared or disseminated without possible consequences. Therefore, child sexual abuse material should remain detectable in all interpersonal communications services through the application of vetted technologies, when uploaded, under the condition that the users give their explicit consent under the provider's terms and conditions for a specific technology being applied to such detection in the respective service. Users not giving their consent should still be able to use that part of the service that does not involve the sending of visual content and URLs. This ensures that the detection mechanism can access the data in its unencrypted form for effective analysis and action, without compromising the protection provided by end-to-end encryption once the data is transmitted. To avoid the weakening of the protection provided by the encryption, technologies intended to be used for detection in services using end-to-end encryption should be certified by the EU Centre and tested with the support of its Technology Committee before undergoing the vetting procedure foreseen for all detection technologies.

(26b) In order to ensure uniform conditions for the implementation of the detection orders, implementing powers should be conferred on the Commission to approve the technologies that can be used to execute the detection orders. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.

(27) In order to facilitate the providers' compliance with the detection obligations, the EU Centre should make available to providers detection 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 reliable, as well as to identify false positives and avoid to the extent erroneous reporting to the EU Centre, providers should ensure 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 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.~~

(29) Providers of hosting services and providers of publicly available interpersonal communications services are uniquely positioned to detect potential online child sexual abuse involving their services. The information that they may obtain when offering their services is often indispensable 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 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. 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.

(29a) Metadata connected to reported potential online child sexual abuse may be useful for investigative purposes and for the purpose to identify a suspect of a child sexual abuse offence. For the purpose of this Regulation, the term 'metadata' should be understood as data other than content data referring to information about documents, files or communications. Metadata may include, depending on the case, information about the time, IP address and place of, port number and the devices used for, the creation or exchange of the documents, files or communications at issue and about any modifications made thereto.

(29b) There should be an expedited reporting procedure when the information reported by the provider reasonably justifies the conclusion that there is likely to be an imminent threat to the life or safety of a child or when the information indicates ongoing abuse. The expedited reporting procedure should limit the information required to be reported to the most necessary items of information and include the rest of the information required in the standard reporting procedure only if immediately available. The expedited reporting procedure should also include an expedited processing by the EU Centre. In addition to the cases that require expedited reporting, the provider should indicate in the report other situations that require urgent action but not expedited reporting, such as situations where the provider is aware of an ongoing investigation and the information reported by the provider reasonably justifies the conclusion that such information could be beneficial to that investigation.

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, ~~Coordinating Authorities of establishment~~ **the competent authority of each Member State, where applicable its judicial authority,** should have the power 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.

(31) The rules of this Regulation should not be understood as affecting the requirements regarding removal orders **or the rules on no general monitoring or active fact-finding obligations** set out in Regulation (EU) **2022/2065** ~~…/… of the European Parliament and of the Council~~[16] ~~[*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*]~~.

(31a) The rules of this Regulation should not be understood as affecting the relevant national requirements providing, in accordance with Union law, procedural safeguards regarding the issuing of removal, blocking or delisting orders, such as the control of the conformity with the applicable legal requirements of these orders by an independent authority.

---

16 Regulation (EU) ~~…/…~~ **2022/2065** 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 ….).

(31b) **In order to allow Member States to organise the process of issuance of removal, blocking or delisting orders in a manner compatible with their respective constitutional requirements and to enhance prior judicial control where deemed appropriate, they should have the possibility to require their respective competent authorities to request the competent judicial authority of the Member State concerned to issue some or all of those three types of orders under this Regulation. That possibility to derogate should however only concern the question which authority issues the orders. Accordingly, when a Member State makes use of that possibility, the competent authority concerned should remain responsible for assessing the need for the order at stake and for complying with all of the procedural requirements of this Regulation related to its preparation and follow-up. In that case, whilst it is for the competent judicial authority to conduct an additional verification of whether the conditions of this Regulation for issuing the order in question have been met, those conditions themselves should remain unaltered and be applied consistently across the Union. In the interest of effectiveness, that possibility should be subject to the Member State concerned taking all reasonable measures to ensure that the issuance of the orders by their judicial authorities does not lead to any undue delays. In addition, in the interest of transparency and legal certainty, it should be ensured that the necessary information regarding the use of the possibility is publicly available.**

(31c) **In the interest of effectiveness, it should be possible for the competent authorities of Member States to issue, in accordance with this Regulation, removal orders also against providers of hosting services that have their main establishment, or their legal representative, in another Member State. Given the particularity of this situation, it is appropriate to provide for a specific procedure applicable to such cross-border removal orders, so as to allow, but not require under Union law, the Coordinating Authority of that Member State to scrutinise them in respect of certain serious or manifest infringements that may occur in exceptional cases, insofar as the application of that specific procedure is required to comply with the constitutional law of the relevant Member State. To that aim, such cross-border removal orders should be transmitted via that Coordinating Authority to the provider of hosting services concerned. However, if that Coordinating Authority establishes by reasoned decision, after having carried out a diligent and objective assessment and after having informed the Coordinating Authority of the Member State whose authority issued the removal order and taken into account its response insofar as possible, that such an infringement occurred, the removal order should not be transmitted and should not take legal effect, it then being for the authority that issued the cross-border removal order to take the necessary steps to withdraw or annul it upon being notified of the reasoned decision. All actions required as part of this procedure should be taken as swiftly as possible and in any event within the set time periods, so as to ensure that any undue delays are avoided, and as much as possible in sincere cooperation between the competent authorities involved.**

(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**, when less intrusive measures such as the removal of the material are not reasonably possible or it is likely that such measures will fail.**

(33) In the interest of consistency, efficiency and effectiveness and to minimise the risk of circumvention, such blocking orders ~~should~~ **could** 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.

(33a) To ensure that online child sexual abuse material is delisted as swiftly as possible after its detection, the competent authority of each Member State, or where applicable its judicial authority, should have the power to issue a delisting order addressed to providers of online search engines. As delisting may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the delisting, 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.

POLITO

(33b) In the interest of ensuring effective cooperation in the delisting of online child sexual abuse material, it should be possible for the competent authorities of each Member State, or where applicable its judicial authority, to issue a delisting order to a provider of an online search engine that does not have its main establishment or legal representative in the Member State of the authority that issued the delisting order. Given the particularity of this situation, and in the interest of consistency, provision should be made for a procedure applicable to such cross-border delisting orders that is the same as the procedure for cross-border removal orders.

(34) 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, insofar as their activities remain strictly limited to what is needed for the purpose of complying with their obligations under this Regulation and they act in good faith.

(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.

PUBLIC

(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. **In that regard, the requirements to preserve such data in connection to the execution of detection orders should not be understood as allowing or requiring the preservation of all users' data processed for such detection purposes in general. They should rather be understood as requiring only the preservation of content data and other data processed insofar as this is strictly necessary to use the relevant technologies meeting the requirements of this Regulation, covering in particular caching-like activities involving the automatic and intermediate preservation for purely technical reasons and for very short periods of time needed to use the relevant indicators to detect possible child sexual abuse online, as well as to apply the safeguards required under this Regulation in connection to the use of those technologies, covering in particular the application of measures to prevent, detect and remedy misuse, to ensure regular human oversight and to carry out regular reviews**. 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. **In order to achieve the specific purposes set out in this Regulation, providers of hosting services and providers of interpersonal communications services should keep logs with the time and duration of the processing and, where applicable, the person performing the processing, in accordance with Regulation (EU) 2016/679.**

POINT

(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. 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** ~~…/… of the European Parliament and of the Council~~[17] [*~~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** …/… of the European Parliament and of the Council[18] [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*] and this Regulation.

~~(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.~~

---

17 Regulation (EU) ~~…/…~~**2022/2065** 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 ….).

18 Regulation (EU) ~~…/…~~**2022/2065** 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 ….).

~~(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 the application of this Regulation, 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~~ **competent** ~~A~~**a**uthorities 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~~ **competent** ~~A~~**a**uthorities 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.

(45a) For the purposes of this Regulation, Member States should designate competent authorities. This should not necessarily imply the establishment of a new authority and it should be possible for each Member State to entrust an existing body with the functions provided for in this Regulation, and to decide on the number of competent authorities to be designated. With a view to leaving Member States a degree of flexibility so as to implement solutions best adapted to their particular circumstances, whilst also ensuring the coordination at domestic level and cooperation at EU level needed to ensure the consistent, efficient and effective application of this Regulation, Member States should be able to designate several competent authorities yet be required in that case to appoint one of them as the Coordinating Authority for which certain tasks are exclusively reserved under this Regulation. In particular, the Coordinating Authority should act as the single contact point with regard to all matters related to the application of this Regulation, without prejudice to the enforcement powers of other national authorities. Therefore, each mention of competent authorities in this Regulation should be interpreted as referring to the relevant competent authorities designated by the Member States, including where relevant Coordinating Authorities, while each mention of Coordinating Authorities should be interpreted as referring to Coordinating Authorities only, to the exclusion of any other competent authorities that the Member States may have designated. Member States should also be able to provide for the ex post administrative or judicial review of the orders issued by competent authorities, in accordance with national law, including when such review is not specifically provided for 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.~~

(46a) Member States should be free to designate any suitable national authority, including administrative, law enforcement or judicial ones as appropriate, as competent authority for the purpose of this Regulation, provided that all requirements of this Regulation relating to them are fully respected, including as regards the competent authorities' status and the manner in which they perform their tasks, their investigatory and enforcement powers, complaint-handling and cooperation at EU level. Member States should also be free to designate a judicial authority or independent administrative authority for the issuance of certain orders in accordance with this Regulation, as well as the requirements resulting from the Charter, in particular as regards effective judicial redress against the competent authorities' decisions.

(46b) In order to ensure that the competent authorities designated under this Regulation carry out their tasks under this Regulation in an objective, adequate and responsible manner, in compliance with the fundamental rights guaranteed under the Charter and without any undue interference, certain requirements in this respect should be provided for. Those requirements should not be interpreted as precluding judicial review of the activities of competent authorities in accordance with EU law or with national law.

(47) **Competent authorities, including Coordinating Authorities** ~~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 the necessary financial, human, technological and other resources to adequately 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~~ **competent a**uthorities 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 **or delisting orders** ~~that it~~ issued, are effectively complied in practice, ~~each Coordinating authority~~ **competent authorities** 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 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.~~

Nothing in this Regulation precludes competent authorities designated therein to submit notices to providers of hosting services on the basis of notice and action mechanisms pursuant to Article 16 of Regulation (EU) 2022/2065 (Digital Services Act) to notify them of the presence of one or more specific items of known child sexual abuse material, nor to request the status of trusted flagger under the conditions established under Article 22 of that Regulation.

(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.

(52a) Without prejudice to the rights of users to turn to a representative in accordance with the Directive (EU) 2020/1828 or to any other type of representation under national law, users should also have the right to mandate a legal person or a public body to exercise their rights provided for in this Regulation.

(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.

POLITICO

(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~~ **competent a**uthorities, material identified as constituting child sexual abuse material ~~or transcripts of conversations identified as constituting the solicitation of children~~, 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, **subject to adequate oversight by judicial authorities** ~~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~~ **extracts of conversations** should be done proactively by the ~~Coordinating~~ **competent a**uthorities. However, the EU Centre should also be allowed to bring certain material or conversations to the attention of the ~~Coordinating~~ **competent a**uthorities for those purposes.

(56a) Member States should set up expedited procedures for the diligent assessment of suspected child sexual abuse, so as to allow for the swift submission to the EU Centre of the specific items of material, extracts of conversations and uniform resource locators concerned upon the reliable establishment of the illegality. With a view to facilitating and expediting such assessment, it should be possible for Member States to provide that competent authorities carry out the assessment of illegality of the content, under the oversight of the competent judicial authorities.

POLITICO

(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.

(57a) "Joint investigations" under Article 38 should be interpreted as formal inquiries by Coordinating Authorities concerning the compliance of the provider of relevant information society services with the obligations arising from this Regulation. Insofar as the penalties for infringements of those obligations provided for by the Member State concerned pursuant to this Regulation are not criminal in nature, "joint investigations" under Article 38 should not be interpreted as criminal investigations, which are usually conducted by law enforcement authorities under national law.

(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.

PUBLIC

(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~~ **competent a**uthorities, as well as the generation and sharing of knowledge and expertise related to online child sexual abuse**, including on prevention**. **The EU Centre should, in accordance with its tasks under this Regulation, also assess the initiatives related to preventing and combating online child sexual abuse to determine whether they can be considered as best practices, using standardised assessment tools where possible, and make available these best practices, including through a dedicated database, to support the knowledge hub function of the EU Centre and prevent duplication of efforts and initiatives, promoting efficiency and collaboration among stakeholders.**

(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~~ **competent a**uthorities 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.

POLITO

(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.

(64a) Considering its role as central knowledge hub on matters related to the implementation of this Regulation at EU level, the EU Centre should, in accordance with this Regulation, leverage all means at its disposal to facilitate the work of Europol and competent law enforcement authorities, for example by ensuring that information received by law enforcement authorities is relevant, complete and as easy as possible to access and consult. In particular, the EU Centre should give Europol and the competent law enforcement authorities of the Member States access to the database of indicators when necessary for the purpose of their tasks of investigating suspected child sexual abuse offences.

(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** ~~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.

POLITO

(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 **the competent authorities including the** Coordinating Authorities, ~~the~~ Europol and relevant partner organisations, such as the US National Centre for Missing and Exploited Children, **the European Crime Prevention Network ('EUCPN')** 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) 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 effectively with the ~~Coordinating~~ **competent a**uthorities, 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.

(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.

POLITICO

(71a) Europol and the EU Centre should cooperate closely when performing their respective, distinct tasks and responsibilities in accordance with this Regulation and Regulation (EU) 2016/794.[19] This Regulation should not be understood as altering in any way Regulation (EU) 2016/794 and Europol's tasks and responsibilities under that Regulation. For example, in relation to the processing of reports from service providers, the EU Centre should, subject to the filtering provided for in this Regulation, forward those reports to Europol and to the competent national law enforcement authority or authorities, together with the additional relevant information, including for victim identification purposes, as prescribed by this Regulation, whereas Europol could continue to assist national law enforcement in criminal investigations concerning such reports in accordance with its mandate. Also, in relation to the storage of reports, the EU Centre should perform the tasks specified in this Regulation, in particular create maintain and operate a database for those purposes, whereas Europol could, in accordance with its mandate, continue to expand with the reports received from the EU Centre its own databases of criminal intelligence shared with national authorities, notably for criminal investigation purposes.

~~(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.

---

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

(74a) In view of the need for assistance to victims' expertise in order to perform its tasks, the EU Centre should have a Victims Board, composed of adult victims of child sexual abuse and persons with relevant expertise, with an advisory function. The Victims Board 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 the tasks of providing information to victims, and assistance and support for removal, via the Coordinating Authorities.

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available 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 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 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.

POLITICO

(78) Regulation (EU) 2021/1232 of the European Parliament and of the Council[20] provides for a temporary solution in respect of the use of technologies by certain providers of publicly available 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. **It is important that child sexual abuse online can be effectively and lawfully combated without interruptions and that there is a smooth transition between the temporary regime created by Regulation (EU) 2021/1232 and the long-term regime created by this Regulation. Therefore, the necessary amendment should be made to Regulation (EU) 2021/1232 and it should be repealed with effect from the moment at which all relevant provisions of this Regulation have started to apply** ~~Regulation (EU) 2021/1232 should therefore be repealed~~.

(78a) The rules of this Regulation should apply as soon as possible. However, account should be taken of the need for all parties involved, and in particular the EU Centre, to take the necessary preparatory measures. Therefore, the relevant provisions of this Regulation should only start to apply after certain appropriate time periods. During this transition period, general rules that refer to several measures, some of which have not entered into application yet, should be understood as not being applicable to the measures that have not entered into application yet. Thus, for example, during that period, it should be possible to issue a blocking order in accordance with this Regulation, subject to the order in such a case having to be executed without making use of the database of indicators provided by the EU Centre, which would still be under preparation during such transition period.

(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.

[20] 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).

(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[21]. 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[22].

(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[23] and delivered their opinion on **28 July 2022** ~~[...]~~.

POLITO

21 Inter-institutional Agreement of 13 April 2016 on Better Law Making (OJ L 123, 12.5.2016, p. 1).

22 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).

23 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).

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

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

   It establishes, in particular:

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

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

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

   (d) obligations on providers of internet access services to **prevent users from accessing** ~~access~~ child sexual abuse material;

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

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

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

POLITICO

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 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)**~~.../...~~ of the European Parliament and of the Council[24] [*~~on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC~~*];

(ba) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act);

(c) Directive 2010/13/EU;

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

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

3a. This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to the right for respect to private life and family life and to freedom of expression and information.

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

5. Without prejudice to Article 10a, this Regulation shall not prohibit, make impossible, weaken, circumvent or otherwise undermine cybersecurity measures, in particular encryption, including end-to-end encryption, implemented by the relevant information society services or by the users. This Regulation shall not create any obligation that would require a provider of hosting services or a provider of interpersonal communications services to decrypt data or create access to end-to-end encrypted data, or that would prevent providers from offering end-to-end encrypted services.

---

[24] Regulation (EU) ~~.../...~~ **2022/2065** 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 ….).

Article 2

Definitions

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

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

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

(c) 'software application' means a digital product or service as defined in Article 2, point **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[25];

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

(i) a hosting service;

(ii) an interpersonal communications service;

(iii) a software applications store;

(iv) an internet access service**;**

(v) online search engines.

[25] 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).

(g) 'to offer services in the Union' means to offer services in the Union as defined in Article **3** ~~2~~, point (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;

(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[26];

(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 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)** ~~2, point (o)~~, of Regulation (EU) **2022/2065** ~~…/… *[on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*~~;

[26] 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).

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

(t) 'content moderation' means the activities as defined in Article **3, point (t)** ~~2, point (p)~~, of Regulation (EU) **2022/2065** ~~*…/… [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]*~~;

(ta) 'Competent authority of establishment' means the competent authority 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;

(u) 'Coordinating Authority of establishment' means the **competent authority designated as 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)** ~~2, point (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;

(x) 'online search engine' means an intermediary service as defined in Article 3, point (j), of Regulation (EU) 2022/2065;

(y) 'visual content' means images and the visual components of videos;

(z) 'hit' means a match established by comparison between the indicators to detect the dissemination of new child sexual abuse material and the visual content subject to detection.

POLITICO

CHAPTER II

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

Section 1
Risk assessment and mitigation obligations

Article 3

Risk assessment

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

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

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

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

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

   – measures taken to enforce such prohibitions and restrictions;

   – functionalities enabling age verification;

   – **functionalities enabling parental control or parental consent mechanisms;**

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

   – **measures taken to ensure a robust and swift process to handle notified potential child sexual abuse;**

   – **functionalities enabling the providers the compilation and generation of relevant statistical information for assessment purposes.**

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

   (ca) age appropriate measures taken by the provider to promote users' digital literacy and safe use of the service;

POLITICO

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

(da) the availability of functionalities enabling users to share images or videos with other users, in particular through private communications, and of functionalities enabling the providers to assess how easily, quickly, and widely such material may be disseminated further by means of the service;

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

(i) the extent to which the service 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 in relation to those 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 search for child users;

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

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

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

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

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**, the information to be provided** 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, **depending on the risk category determined in accordance with Article 5(2),** at least once every three years **for low-risk services, at least once every two years for medium-risk services and at least once every year for high-risk services** from the date at which it last carried out or updated the risk assessment. However:

(a) for a **high-risk** 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~~ **four** 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**, including from Coordinating Authorities of other Member States or from providers offering low-risk or medium-risk services,** indicating a possible substantial change in the risk that the service is used for the purpose of online child sexual abuse.

4a. The risk assessment shall gather information on the limitation of the risk to an identifiable part or component of the service where possible, such as specific types of channels of an interpersonal communications service, or to specific users or specific groups or types of users where possible, to the extent that such part, component, specific users or specific groups or types of users can be assessed in isolation for the purpose of mitigating the risk of online child sexual abuse.

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

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

Article 4

Risk mitigation

1. **If p**roviders of hosting services and providers of interpersonal communications services **have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they** shall take **all** reasonable mitigation measures, tailored to ~~the~~ **that** risk ~~identified~~ ~~pursuant to Article 3~~, to minimise that risk. **The risk mitigation measures shall be limited to an identifiable part or component of the service, or to specific users or specific groups or types of users, where possible, without prejudice to the effectiveness of the measure.**

   Such measures shall **at least** include some or all of the following:

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

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

   (c) initiating or adjusting cooperation, in accordance with competition law, with other providers of hosting services or providers of interpersonal communication**s** services, public authorities, civil society organisations or, where applicable, entities awarded the status of trusted flaggers in accordance with Article **22** ~~19~~ of Regulation (EU) **2022/2065** ~~…/…~~ [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~];

   (d) initiating or adjusting functionalities that enable users to notify online child sexual abuse to the provider through tools that are easily accessible and age-appropriate;

   (e) initiating or adjusting functionalities that enable users to control what information about them is shared to other users and how other users may contact them, and introducing default suitable privacy settings for users who are children;

POLITICO

(f) initiating or adjusting functionalities that provide information to users about notification mechanisms and direct users to helplines and trusted organisations, where users detect material or conversations indicating potential online child sexual abuse;

(g) initiating or adjusting functionalities that allow the providers to collect statistical data to better assess the risks and the effectiveness of the mitigation measures. This data shall not include any personal data.

2. The mitigation measures shall be:

(a) effective in mitigating the identified risk;

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

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

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

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

Those age verification and age assessment measures shall be privacy preserving, respecting the principles relating to the processing of personal data, notably the principles of lawfulness, purpose limitation and data minimisation, proportionate, transparent, effective, accurate, non-discriminatory, accessible and take as a primary consideration the best interest of the child.

3a. Providers of hosting services and providers of interpersonal communications services may request the EU Centre to assist in identifying and assessing technical aspects of specific mitigation measures referred to in paragraphs 1, 2 and 3.

The costs incurred by the EU Centre for providing such assistance 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 identification and assessment of risk mitigation measures. The EU Centre shall make available information to determine those costs.

The assistance provided by the EU Centre shall not affect the responsibility of the provider to comply with the requirements applicable to the mitigation measures and for any decisions it may take in connection to or as a result of the application of those measures.

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, the information to be provided and the application of the exemption for micro, small and medium-sized enterprises.

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

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

Article 5

*Risk reporting **and categorisation***

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

   (a) the **premise for the risk assessment pursuant to Article 3(2), the** process and the results of the risk assessment conducted or updated pursuant to Article 3, including the assessment of any potential remaining risk referred to in Article 3(5);

   (b) any mitigation measures taken pursuant to Article 4 **and, where applicable, Article 5a, and the results thereof including the effectiveness of these measures and how they comply with the requirements of Article 4(2), and in case of age assessment and verification measures, how they comply with the requirements of Article 4 (3);**

   (ba) any other mitigation measures implemented before carrying out the risk assessment and, when available, complementary informations about the effectiveness of these measures;

(c) where potential remaining risk as referred to in Article 3(5) is identified, any available information relevant for identifying as precisely as possible the parts or components of the service, or the specific users or groups or types of users, in respect of which the potential remaining risk arises;

(ca) a self-assessment against the criteria established for the categorisation of risks of the service or the parts or components of the service, following the template established in accordance with Article 5(2a);

(d) whether the provider requests to the Coordinating Authority of establishment the authorisation to display the sign of reduced risk as referred to in Article 5b.

This report shall include available statistical information to support and illustrate the development and effectiveness of mitigation measures.

Providers of hosting services and providers of interpersonal communications services may notify in this report whether there is evidence of the service or parts or components of the service being used for the purpose of online child sexual abuse that might require the issuing of a detection order in accordance with Article 7(4).

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 **diligently** carried out or updated and the mitigation measures have been taken in accordance with the requirements of Articles 3 and 4 **and evaluate the level of the remaining risk**.

Based on the evaluation of the level of the remaining risk and taking into account the self-assessment carried out by the providers of hosting services and providers of interpersonal communications against the criteria established for the categorisation of risks, the Coordinating Authority of establishment shall determine the risk category allocated to the service or the parts or components of the service, following the methodology and criteria established in accordance with Article 5(2a).

The service or the parts or components of the service shall be classified into the following categories:

(a) High risk;

(b) Medium risk;

(c) Low risk.

POLICO

The decision of the Coordinating Authority of establishment determining the risk category, including the date by when the provider is required to update the risk assessment, shall be communicated to the providers concerned, recorded by the Coordinating Authority of establishment and notified to the EU Centre.

The Coordinating Authority of establishment may request the EU Centre to assist in evaluating the mitigation measures taken by the provider, evaluating the level of the remaining risk and in determining the risk category allocated to the service or the parts or components of the service.

If the provider has submitted the request referred to in point (d) of paragraph 1, the Coordinating Authority shall decide on the issuance of the authorisation to display the sign of reduced risk in accordance to Article 5b.

2a. **The risk categorisation shall be based on the report submitted by the providers to the Coordinating Authority of establishment in line with Article 5, in particular the risk assessment by the providers, the mitigation measures undertaken by them and their self-assessment, and any other relevant information available to the Coordinating Authority of establishment or the EU Centre. The methodology and the criteria for the risk categorisation shall enable an objective, transparent and comprehensible classification of the risks of services related to child sexual abuse based on the scoring of risk indicators as outlined below:**

(a) **The template for the self-assessment of providers shall be issued in different versions taking into account the size and the type of the services offered by the providers as indicated in ANNEX XIV.**

(b) **The scoring shall be based on the following criteria: the size, type and core architecture of the service, the policies and safety by design functionalities in place to address the identified risks and a mapping of user tendencies.**

(c) **The risk criteria shall be broken down in risk indicators as outlined in the list of risk indicators included in ANNEX XIV.**

(d) **The risk indicators shall be weighted in a transparent and understandable manner according to their impact on the risks of a service related to child sexual abuse based on the methodology and criteria laid down in ANNEX XIV.**

(e) **The result of the scoring shall be quantitative and comparable, and provide for a classification into high-risk, medium-risk and low-risk services.**

The Commission shall be empowered to adopt delegated acts in accordance with Article 86 to detail and amend ANNEX XIV laying down the methodology and criteria for the risk categorisation in line with this paragraph, and to establish and amend the template for the self-assessment by providers.

POLICE

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~~ **paragraph 2** shall be suspended until that additional information is provided.

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

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

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

Article 5a

Adjusted or additional risk assessment or risk mitigation measures

1. Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that a provider offering a service or parts or components of a service classified as high risk or medium risk has not met the requirements of Articles 3 or 4, it shall require the provider of hosting services or the provider of interpersonal communications services to carry out one or several of the following actions, with respect to those parts or components of a service classified as high risk or medium risk, as appropriate:

(a) to re-conduct or update the risk assessment in accordance with Article 3, including where appropriate by modifying the methodology used to conduct the risk assessment, and report thereon in accordance with Article 5;

(b) to implement, review, modify, discontinue or expand some or all of the risk mitigation measures taken in accordance with Article 4;

(c) to introduce additional risk mitigation measures in accordance with Article 4.

The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to require pursuant to the first subparagraph.

POLITICO

2. **A provider that is required to perform the actions specified in points (b) or (c) of paragraph 1 shall re-conduct or update the risk assessment in accordance with Article 3 so as to take account of those actions, and report thereon in accordance with Article 5. In the report on the re-conducted or updated risk assessment the provider shall also specify and explain the actions performed pursuant to paragraph 1, within a time period set by the Coordinating Authority. That time period shall be reasonable, taking into account the complexity of the required actions.**

3. **The Coordinating Authority of establishment shall, by deviation from the time periods specified in Articles 3(4) and 5(1), set a reasonable time period for the performance of the actions pursuant to paragraph 1 and for the reporting pursuant to paragraph 2. That time period shall be reasonable, taking into account the complexity of the required actions.**

4. **The Coordinating Authority of establishment may recommend to a provider offering a service or parts or components of a service classified as low risk to carry out one or several of the actions listed in paragraph 1, with respect to those parts or components of a service classified as low risk, as appropriate.**

Article 5b

Sign of reduced risk

1. **Where both of the following conditions have been met, the Coordinating Authority of establishment shall authorise a provider of hosting services or a provider of interpersonal communications services, upon its reasoned and voluntary request, as referred to in point (d) of Article 5(1), to publicly display a distinctive sign of reduced risk as a clear visual representation to users indicating that the service concerned meets those conditions:**

(a) **the Coordinating Authority considers that the provider has carried out the risk assessment in accordance with Article 3 and has taken all reasonable risk mitigation measures in accordance with Article 4, including where applicable pursuant to Article 5a;**

(b) **the Coordinating Authority considers that there is no need to initiate the process for the issuance of a detection order in accordance with Article 7, having regard in particular to the nature and extent of any remaining risk referred to in Article 5(2) and the conditions set out in Article 7(4).**

POLITICO

2. **The sign shall only be displayed upon receiving the authorisation referred to in paragraph 1. The provider shall not display the sign where the authorisation has been suspended or withdrawn in accordance with paragraph 4, in which case the provider shall stop displaying it within 24 hours.**

3. **Providers authorised in accordance with paragraph 1 shall, for as long as the authorisation is not withdrawn or suspended, do both of the following:**

(a) **prominently display the sign on the service concerned;**

(b) **include, in a clear and easily understandable manner, the necessary explanations regarding the sign in their terms and conditions, including about the conditions met to be authorised to display the sign and the fact that the authorisation does not mean that the risk of online child sexual abuse is completely eliminated.**

4. **The Coordinating Authority that issued an authorisation in accordance with paragraph 1 shall regularly, and at least every six months, review whether the conditions set out in that paragraph continue to be met, taking due account of the risk reporting in accordance with Article 5 and all other relevant information. Where necessary to that aim, it may require the provider concerned to do one or both of the following:**

a) **conduct or update a risk assessment, take the necessary risk mitigation measures and report thereon in accordance with Articles 3, 4 and 5 respectively;**

b) **provide any other relevant information.**

The Coordinating Authority shall immediately suspend the authorisation where it has reasonable doubts about the provider's continued compliance with the conditions of paragraph 1. During the suspension, the Coordinating Authority shall review such compliance, including by requiring the provision of information pursuant to the first subparagraph where appropriate and giving the provider an opportunity to comment on its findings and its intended next steps within a reasonable time period. It shall conclude the review, without undue delay and taking into account any comments received within the time period set, either by terminating the suspension or by withdrawing the authorisation.

The Coordinating Authority shall withdraw the authorisation where it considers that the provider no longer meets the conditions of paragraph 1. It shall also withdraw the authorisation upon request of the provider.

Public

5. Coordinating Authorities shall immediately inform the provider concerned and the EU Centre about each authorisation granted, suspended or withdrawn in accordance with paragraphs 1 and 4. The EU Centre shall maintain a publicly available registry of that information.

6. The issuance of an authorisation in accordance with paragraph 1 shall not affect the Coordinating Authority's possibility to initiate the process for the issuance of a detection order in accordance with Article 7.

7. 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 requests for authorisation to display the sign, on the issuance, suspension and withdrawal of the authorisation, on the design of the sign, on the display of the sign and the provision of information to users relating thereto, on the regular review of continued compliance with the conditions and on the registry of information.

Article 6

Obligations for software application stores

1. Providers of software application stores shall:

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

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

   (c) take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the measures referred to in point (b). **Those age verification and age assessment measures shall be privacy preserving, proportionate, transparent, effective, accurate, non-discriminatory, accessible and take as a primary consideration the best interest of the child.**

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

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

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

Section 2

Detection obligations

Article 7

Issuance of detection orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or an~~other~~ independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services **that are classified as high risk in accordance with Article 5(2) or parts or components of the services classified as high risks that fall** under the jurisdiction of that Member State to take the measures specified in Article 10 **for the sole purpose of** ~~to~~ detect**ing** the dissemination of online child sexual abuse **material** on a specific service **or parts or components of the service, classified as high risk in accordance with Article 5(2), for a limited period of time as specified in paragraph 9**. **Member States may decide that detection orders can be issued by the Coordinating Authority of establishment subject to prior authorisation by a judicial authority or an independent administrative authority.**

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

   To that end, it may~~, where appropriate,~~ require the provider to submit the necessary information, additional to the report and the further information referred to in Article 5(1) and (3), **and Article 5a(2),** 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. **It may also request the assistance of the EU Centre to conduct simulation tests in accordance with Article 47a on the service in question to verify whether there are objective indications, as referred to in point (a) of paragraphs 5 or 6, as applicable.**

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

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

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

(c) afford the provider an opportunity to comment on the draft request, within a reasonable time period set by that Coordinating Authority;

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

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

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

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

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

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

Where, having regard to the implementation plan of the provider and the **received** opinion**s** of the data protection authority **and the EU Centre, where applicable**, 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 **or for the authorisation of 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 **and, when appropriate, the reasons for diverging from the opinions received**.

POINTO

4. The Coordinating Authority of establishment shall request the issuance of **or the authorisation for issuing** the detection order **substantiated by its motivated reasoning and relevant justifications**, and the competent judicial authority or independent administrative authority **may** ~~shall~~ issue **or authorise the issuing by the Coordinating Authority of establishment of** the detection order where it considers that the following conditions are met:

(a) there is evidence of a significant and present or foreseeable risk of the **high-risk** service **or parts or components of the service** being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5~~,~~ **and** 6 ~~and 7~~, as applicable;

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

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

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

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

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

(ca) the necessity and proportionality in terms of the period of application, the intrusiveness of the technologies, approved by implementing act in line with Article 10(2), the impact on fundamental rights, and the possibility to limit the scope to parts or components of a service and other safeguards provided for in accordance with paragraph 8;

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

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

POLITO

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

(a) ~~it is likely,~~ **there are objective indications that,** despite any mitigation measures that the provider may have taken or will take, ~~that~~ the service **or parts or components of the high-risk service** is used, to an appreciable extent for the dissemination of known child sexual abuse material**;**

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

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~~, **there are objective indications that,** despite any mitigation measures that the provider may have taken or will take, ~~that~~ the service **or parts or components of the high-risk 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.

6a. Providers of hosting services and providers of interpersonal communications services shall carry out the detection orders concerning the dissemination of new child sexual abuse material in a way that the material is reported in accordance with Articles 12 and 13 under the conditions outlined in sub-paragraphs 2 to 4.

The detection of potential new child sexual abuse material shall result in a hit to be flagged in the affected service, without the provider getting knowledge of, or control over, that information. Providers shall preserve the information about the existence of the hit for at least twelve months or the duration of the respective detection order, whatever is longer.

POLITO

Once potential new child sexual abuse material has been flagged in a service twice, or once a user has notified the provider about potential new child sexual abuse material within a service, the provider shall report that material to the EU Centre in such a manner that the personal data cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separate and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Where the EU Centre considers, after human verification, that a report on potential new child sexual abuse material submitted by a provider is not manifestly unfounded, it shall require the provider to re-submit the report without the limitations outlined in sub-paragraph 3.

The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to increase, where necessary, the number of hits required to trigger the reporting of potential new child sexual abuse referred to in sub-paragraph 3.

~~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, despite any mitigation measures that the provider may have taken or will take, that 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 **or the authorisation to issue** detection orders, and the competent judicial or independent administrative authority when issuing **or authorising the issuing by the Coordinating Authority of establishment of** the detection order, shall target and specify it in such a manner that the negative consequences referred to in paragraph 4, first subparagraph, point (b), remain limited to what is strictly necessary to effectively address the significant risk referred to in point (a) thereof.

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

In particular, they shall ensure that:

(a) where that risk is limited to an identifiable part or component of a service, the required measures are 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), (5) and (6) are provided for;

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

(d) detection does not apply to accounts used by the State for national security purposes, maintaining law and order or military purposes.

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

Article 8

Additional rules regarding detection orders

1. The competent judicial authority **or independent administrative authority, or the Coordinating Authority of establishment subject to prior authorisation by a judicial authority or an 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 measures to be taken to execute the detection order, including the indicators to be used and the safeguards to be provided for, including the reporting requirements set pursuant to Article 9(3) and, where applicable, any additional safeguards as referred to in Article 7(8);

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

POLITO

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

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

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

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

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

(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.

1a. If a detection order is issued by an independent administrative authority or by the Coordinating Authority of establishment with the prior authorisation by an independent administrative authority, that independent administrative authority must have a status enabling it to act objectively, impartially and free from any external influence when carrying out its duties.

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

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

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

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

3. If the provider cannot execute the detection order because it contains manifest errors or does not contain sufficient information for its execution, the provider shall, without undue delay, **inform** ~~request the necessary clarification to~~ the Coordinating Authority of establishment, using the template set out in Annex II. **That Coordinating Authority shall assess the matter and request the competent judicial authority or independent administrative authority that issued or authorised the issuing of the detection order the modification or revocation of such order, where necessary in the light of the outcome of that assessment.**

The competent authority that issued the detection order shall inform the provider of the outcome of and the reasons leading to that assessment.

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

Article 9

Redress, information, reporting and modification of detection orders

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

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

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

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

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

POLITO

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 **or authorised the issuing of** the detection order the modification or revocation of such order, where necessary in the light of the outcome of that assessment. The provisions of this Section shall apply to such requests, *mutatis mutandis*.

Article 10

Technologies and safeguards

1. Providers of hosting services and providers of interpersonal communication**s** services that have received a detection order shall execute it by installing and operating technologies **approved by the Commission** 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 Commission shall adopt implementing acts to approve the technologies referred to in paragraph 1 and Article 10a, after consulting the EU Centre, using the criteria set out in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87.**

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 **referred to in paragraph 1 and Article 10a approved by the Commission** ~~made available by the EU Centre~~ shall not affect the responsibility of the provider to comply with ~~those~~ **the** requirements **set out in this Article** 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) **be** effective **and suitable** in detecting the dissemination of known or new child sexual abuse material ~~or the solicitation of children~~, as applicable;

(aa) not introduce cybersecurity risks for which it is not possible to take any effective measures to mitigate such risk;

(ab) if applied in services using end-to-end encryption, be certified by the EU Centre following tests conducted with the support of its Technology Committee, that their use could not lead to a weakening of the protection provided by the encryption;

(b) **be limited to detect visual content and URLs, and** shall not be able to **deduce the substance of the content of the communications nor to** extract any other information from the relevant communications than the information strictly necessary to detect, using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new child sexual abuse material ~~or the solicitation of children~~, as applicable;

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

(d) **be** ~~sufficiently~~ reliable **and accurate**, in that they limit to the maximum extent possible the rate of errors regarding the detection **and, where such errors occur, enable the correction of errors without undue delay**.

4. The provider shall:

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

(i) diligently identify, analyse and assess the cybersecurity risks that could be introduced by the technologies used for the execution of the detection orders;

(ii) take all reasonable mitigation measures, tailored to the possible cyberscurity risk identified, to minimise that risk;

(aa) upon receiving a detection order in interpersonal communications services, limit the functionalities of that service to prevent the transmission of visual content and URLs absent the user consent pursuant to paragraph 5(aa);

(b) establish effective internal procedures to prevent and, where necessary, detect and remedy any misuse**, including misuses caused by breaching cybersecurity measures,** of the technologies, indicators and personal data and other data referred to in point (a), and 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 are detected, human intervention**;

(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, 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), **(aa),** (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~~ **request the consent of** users **to detect the dissemination of known or new child sexual abuse material for the purpose of executing detection orders after informing them in the terms and conditions of use** in a clear, prominent and comprehensible way of the following:

(a) the fact that, **upon receiving a detection order, the provider** ~~it~~ operates technologies to detect online child sexual abuse **material** to execute the detection order, the ways in which it operates those technologies, **meaningful information about the logic involved**, and the impact on the confidentiality of users' communications;

(aa) the fact that, upon receiving a detection order in interpersonal communications services, it is required to limit the functionalities of the service to prevent the transmission of visual content and URLs absent the user consent;

(b) the fact that **the provider** ~~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.

POLITICO

Article 10a

Technologies for upload moderation

In order to implement this Regulation, providers of interpersonal communications services shall install and operate technologies to detect, prior to transmission, the dissemination of known child sexual abuse material or of new child sexual abuse material.

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, may issue 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.

Section 3

Reporting obligations

Article 12

Reporting obligations

1. **Without prejudice to Article 7(6a),** where a provider of hosting services or a provider of interpersonal communications services becomes aware in any manner other than through a removal order issued in accordance with this Regulation of any information ~~indicating~~ **that indicate** potential online child sexual abuse on its service~~s~~, it shall promptly submit a report thereon to the EU Centre in accordance with Article 13. It shall do so through the system established in accordance with Article 39(2).

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

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

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

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

The mechanisms shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices. To that end, the providers shall take the necessary measures, with particular attention to the needs of the child, to enable and to facilitate the submission of notices, with a view to receiving:

(a) the reasons why the user alleges that the material or conversation at issue constitutes online child sexual abuse;

(b) a clear indication of the online location of the alleged online child sexual abuse and, where necessary, information specific to a service that enables the identification of its online location.

4. The Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, shall issue guidelines on the application of paragraph 3, having due regard in particular to the child's age, maturity, views, needs and concerns.

Article 13

Specific requirements for reporting

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

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

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

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

(c) ~~all~~ content data **related to the reported potential online child sexual abuse**~~, including images, videos and text~~;

(d) ~~all~~ **other** available data related to the **reported** potential online child sexual abuse**, including metadata related to media files and communications**;

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

POLITO

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

(g) information concerning the identity of any user involved in the potential online child sexual abuse, **including unique identifiers of the user**;

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

(i) where the **information that indicate** potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material, whether the provider has removed or disabled access to the material**, and, where relevant, whether it has been done on a voluntary basis**;

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

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

1a. By deviation from paragraph 1, where the information referred to in Article 12(1) reasonably justifies the conclusion that there is likely to be an imminent threat to the life or safety of a child or when the information indicates ongoing abuse, the report referred to in paragraph 1 of this Article shall include:

(a) in any event, the information referred to in points (a), (b), (f), (j) and (k) of paragraph 1 of this Article;

(b) the information referred to in the other points of paragraph 1 of this Article, only insofar as that information is immediately available and the inclusion thereof in the report does not delay the submission of the report.

Where the report referred to in the first subparagaph does not contain all information referred to in paragraph 1 of this Article in accordance with point (b) of the first subparagraph, the provider of hosting services or of interpersonal communications services concerned shall promptly submit an additional report containing all that information, updated or completed where relevant. That additional report shall include a reference to the initial report submitted in accordance with the first subparagaph and shall indicate which information has been updated or completed.

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

Section 4
Removal obligations

Article 14

Removal orders

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

1a. By deviation from paragraph 1, and without causing undue delays in the process of issuance of those orders, Member States may decide that such orders can only be issued by or with the prior authorisation of a judicial authority, if necessary, at the request of another competent authority. Where a Member State makes use of this possibility, it shall inform the Commission thereof and maintain this information updated. The Commission shall make the information received publicly available and maintain this information updated.

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

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

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

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

   (c) the specific service **in respect** of ~~for~~ which the removal order is issued;

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

(e) ~~an exact uniform resource locator and, where necessary, additional~~ **clear** information ~~for the identification of~~ **enabling the provider to identify and locate** 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);

(fa) the information necessary for the application, where relevant, of paragraphs 5, 6 and 7;

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

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

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

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

~~It shall transmit~~ The removal order **shall be transmitted, where applicable in accordance with Article 14a,** to the **the provider's** point of contact referred to in Article 23(1) by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order, to the Coordinating Authority **of the Member State whose authority issued the order** and to the EU Centre, through the system established in accordance with Article 39(2).

~~It~~ **The removal order** shall ~~draft~~ **be transmitted** ~~the removal order~~ in **any of** the **official** language**s** declared by the provider pursuant to Article 23(3).

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

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

The time period set out in paragraph **2**~~1~~ shall start to run as soon as the reasons referred to in the first subparagraph have ceased to exist.

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

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

7. The provider shall, without undue delay and using the template set out in Annex VI, inform the **authority issuing the order,** ~~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 14a

Procedure for cross-border removal orders

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

2. The Coordinating Authority of establishment may, within 72 hours of receiving the copy of the removal order in accordance with paragraph 1, scrutinise the removal order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter.

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

3. Where a hosting service provider receives a removal order as referred to in paragraph 1, it shall take the measures provided for in Article 14 and take the necessary measures to be able to reinstate the content or access thereto, in accordance with paragraph 4 of this Article.

4. Upon receiving a decision finding an infringement communicated in accordance with paragraph 7, the provider of hosting services concerned shall without undue delay reinstate the content or access thereto, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.

5. **By deviation from Article 14(1) and from paragraphs 1 and 2 of this Article, where required by the constitutional law of the Member State where the provider of hosting services has its main establishment or where its legal representative resides or is established, that Member State may decide that removal orders issued by the competent authorities of other Member States are to be transmitted through the Coordinating Authority of that Member State. That Member State shall inform the Commission of its decision and of its reasons for taking the decision. The Commission shall make publicly available, and keep up-to-date, a list of Member States that took the decision referred to in this subparagraph.**

The Coordinating Authority of establishment shall as soon as possible and in any event within 72 hours of receiving the removal order transmit the removal order covered by the first subparagraph to the provider of hosting services, unless it adopts a reasoned decision within these 72 hours that the removal order seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter. The removal order shall only have legal effect upon the transmission thereof to the provider of hosting services.

6. **The Coordinating Authority of establishment shall, before adopting a decision pursuant to the second subparagraph of paragraph 2 or the second subparagraph of paragraph 5, inform the Coordinating Authority of the Member State whose authority issued the removal order of its intention to adopt the decision and of its reasons for doing so.**

7. **Where the Coordinating Authority of establishment adopts a reasoned decision in accordance with the second subparagraph of paragraph 2, it shall, without delay, transmit that decision, to the Coordinating Authority of the Member State whose authority issued the removal order, the provider of hosting services and the EU Centre.**

Where the Coordinating Authority of establishment adopts a reasoned decision in accordance with the second subparagraph of paragraph 5, it shall, without delay, transmit that decision to the Coordinating Authority of the Member State whose authority issued the removal order and the EU Centre.

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.

POLITICO

1a. **If the order is reversed as a result of a redress procedure, the provider shall without undue delay reinstate the material or access thereto, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.**

2. When the removal order becomes final, the ~~competent judicial authority or independent administrative~~ authority that issued the removal order shall, without undue delay, transmit a copy thereof **and copies of the information it has received pursuant to Article 14(5) to (7)** to the Coordinating Authority **of the Member State of the authority issuing the removal order** ~~of establishment~~. Th**at**~~e~~ Coordinating **Authority** shall then, without undue delay, transmit ~~a copy~~ **copies** thereof to all other Coordinating Authorities **and to the EU Centre** 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 user's right to judicial redress referred to in paragraph 1 and the user's right to submit complaints to the Coordinating Authority in accordance with Article 34.

3a. **The provider shall establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it complaints about alleged infringements of its obligations under this Section. It shall process such complaints in an objective, effective and timely manner.**

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

POLITICO

In such a case:

(a) the ~~judicial authority or independent administrative~~ authority issuing the removal order shall **inform the provider of its decision specifying the applicable time period that shall be** ~~set the time period~~ no~~t~~ longer than necessary and not exceeding **twelve** ~~six~~ weeks, during which the provider is not to disclose such information;

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

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

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

4a. Where Article 14a(5) applies, the issuing authority shall inform the provider of the decision referred to in paragraph 4 through the Coordinating Authority of establishment.

Section 5
Blocking obligations

Article 16

Blocking orders

1. The **competent authority of establishment** ~~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**, subject to any requirements of national law as referred to in paragraph 1a,** 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~~. **The competent authorities may make use of 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.**

1a. By deviation from paragraph 1, and without causing undue delays in the process of issuance of those orders, Member States may decide that such orders can only be issued by or with the prior authorisation of a judicial authority at the request of another competent authority. Where a Member State makes use of this possibility, it shall inform the Commission thereof and maintain this information updated. The Commission shall make the information received publicly available and maintain this information updated.

POLITICO

1b. The provider shall execute the blocking order as soon as possible and in any event within a reasonable time period set by the issuing authority. The provider shall take the necessary measures to ensure that it is capable of reinstating access in accordance with Article 18(1a).

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

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

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

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

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

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

~~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~~ **A** blocking order **shall be issued**~~,~~ where ~~it considers that~~ the following conditions are met:

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

POLITICO

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

~~(c) 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~~ **A** blocking order~~,~~ shall:

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

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

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

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

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

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

Article 17

Additional rules regarding blocking orders

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

   (a) **where applicable,** 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) **clear information enabling the provider to identify and locate the child sexual abuse material and** the specific service in respect of which the ~~detection~~ **blocking** order is issued;

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

   (ea) the limits referred to in Article 16(5);

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

   (fa) the information necessary for the application, where relevant, of paragraphs 4a, 5, and 5a;

   (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~~ **competent** 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~~ **competent** 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.

POLITICO

3. The blocking order shall be transmitted to the provider's point of contact referred to in Article 23(1) **by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order**, to the Coordinating Authority **in the Member State in which the order was issued** ~~of establishment~~ and to the EU Centre, through the system established in accordance with Article 39(2).

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

4a. If the provider cannot execute the blocking order on grounds of force majeure or de facto impossibility not attributable to it, including for objectively justifiable technical or operational reasons, it shall, without undue delay, inform the authority issuing the order of those grounds, using the template set out in Annex VIII.

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~~ **from** the **authority issuing the order** ~~Coordinating Authority of establishment~~ using the template set out in Annex VIII.

5a. The provider shall, without undue delay and using the template set out in Annex IX, inform the issuing authority of the measures taken to execute the blocking order, indicating, in particular, whether the provider has prevented access to child sexual abuse material.

The authority issuing the order shall require the provider to report to it at regular intervals on the measures taken and their functioning to execute a blocking order, including the effective and proportionate limitations and safeguards provided for.

Upon request of the issuing authority, the provider shall also provide, without undue delay, such reports or any other information relating to the execution of the blocking order needed for the purpose of the assessment referred to in Article 16(7).

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

Article 18

*Redress **and provision of information**~~, information and reporting of blocking orders~~*

1. Providers of internet access services that have received a blocking order~~, as well as~~ **and** users who provided ~~or were prevented from accessing a specific item of~~ **blocked** 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.

POLITICO

1a. **If the order is reversed as a result of a redress procedure, the provider shall without undue delay reinstate access to the material, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.**

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 **and copies of information it has received pursuant to Article 17 (4a) to (5a)** the Coordinating Authority. The Coordinating Authority shall then, without undue delay, transmit ~~a copy~~ **copies** thereof to all other Coordinating Authorities **and the EU Centre** through the system established in accordance with Article 39(2).

   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 content** ~~the uniform resource locators~~ pursuant to a blocking order ~~issued in accordance with Article 17~~, it shall take reasonable measures to inform ~~the~~ **those** users of the following:

   (a) the fact that it does so pursuant to a blocking order **and the reasons for doing so**;

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

   (c) the right of **users who provided the blocked material to** judicial redress referred to in paragraph 1, the~~ir~~ right~~s~~ **of users** 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.~~

POLITICO

~~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 5a
Delisting obligations

Article 18a

Delisting orders

1. The competent authority of each Member State shall have the power to issue a delisting order, subject to any requirements of national law as referred to in the paragraph 1a, requiring a provider of an online search engine to take reasonable measures to delist an online location where child sexual abuse material can be found from appearing in search results in all Member States. The competent authorities may make use of 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.

1a. By deviation from paragraph 1, and without causing undue delays in the process of issuance of those orders, Member States may decide that such orders can only be issued by or with the prior authorisation of a judicial authority at the request of another competent authority. Where a Member State makes use of this possibility, it shall inform the Commission thereof and maintain this information updated. The Commission shall make the information received publicly available and maintain this information updated.

2. The provider shall execute the delisting order as soon as possible and in any event within 24 hours of receipt thereof. The provider shall take the necessary measures to ensure that it is capable of reinstating the delisted online location to appear in search results in accordance with Article 18c(2).

3. A delisting order shall be issued where the following conditions are met:

(a) the delisting is necessary to prevent the dissemination of the child sexual abuse material in the Union, having regard in particular to the need to protect the rights of the victims;

(b) URLs specified in the delisting order correspond, in a sufficiently reliable manner, to online locations where child sexual abuse material can be found.

4. The issuing authority shall specify in the delisting order the period during which it applies, indicating the start date and the end date.

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

5. **The Coordinating Authority or the issuing authority shall, where necessary and at least once every year, assess whether any substantial changes to the grounds for issuing the delisting orders have occurred and whether the conditions of paragraph 4 continue to be met.**

Where necessary in the light of the outcome of that assessment or information of the reports referred to in Article 18b(6) an order may be modified or reversed by the issuing authority, where relevant at the request of the Coordinating Authority.

Article 18aa

Procedure for cross-border delisting orders

1. **Subject to Article 18a, where the provider of an online search engine does not have its main establishment or legal representative in the Member State of the authority that issued the delisting order, that authority shall, simultaneously submit through the Coordinating Authority a copy of the delisting order to the Coordinating Authority of establishment.**

2. **The Coordinating Authority of establishment may, within 72 hours of receiving the copy of the delisting order in accordance with paragraph 1, scrutinise the delisting order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter.**

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

3. **Where a provider of an online search engine receives a delisting order as referred to in paragraph 1, it shall take the measures provided for in Article 18a and take the necessary measures to be able to reinstate the delisted online location to appear in search results, in accordance with paragraph 4 of this Article.**

4. **Upon receiving a decision finding an infringement communicated in accordance with paragraph 7, the provider of an online search engine concerned shall without undue delay reinstate the delisted online location to appear in search results, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.**

POLITICO

5. **By deviation from Article 18a(1) and from paragraphs 1 and 2 of this Article, where required by the constitutional law of the Member State where the provider of an online search engine has its main establishment or where its legal representative resides or is established, that Member State may decide that delisting orders issued by the competent authorities of other Member States are to be transmitted through the Coordinating Authority of that Member State. That Member State shall inform the Commission of its decision and of its reasons for taking the decision. The Commission shall make publicly available, and keep up-to-date, a list of Member States that took the decision referred to in this subparagraph.**

The Coordinating Authority of establishment shall as soon as possible and in any event within 72 hours of receiving the delisting order transmit the delisting order covered by the first subparagraph to the provider of the online search engine, unless it adopts a reasoned decision within these 72 hours that the delisting order seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter. The delisting order shall only have legal effect upon the transmission thereof to the provider of the online search engine.

6. **The Coordinating Authority of establishment shall, before adopting a decision pursuant to the second subparagraph of paragraph 2 or the second subparagraph of paragraph 5, inform the Coordinating Authority of the Member State whose authority issued the delisting order of its intention to adopt the decision and of its reasons for doing so.**

7. **Where the Coordinating Authority of establishment adopts a reasoned decision in accordance with the second subparagraph of paragraph 2, it shall, without delay, transmit that decision, to the Coordinating Authority of the Member State whose authority issued the delisting order, the provider of the online search engine and the EU Centre.**

Where the Coordinating Authority of establishment adopts a reasoned decision in accordance with the second subparagraph of paragraph 5, it shall, without delay, transmit that decision to the Coordinating Authority of the Member State whose authority issued the delisting order and the EU Centre.

POLITICO

Article 18b

Additional rules regarding delisting orders

1. A delisting order shall be issued using the template set out in Annex X. Delisting orders shall include:

(aa) where applicable, the reference to the list of uniform resource locators, provided by the EU Centre,

(a) identification details of the authority issuing the delisting order and authentication of the order by that authority;

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

(c) clear information enabling the provider to identify and locate the child sexual abuse material and the specific service in respect of which the delisting order is issued;

(d) the start and end date of the delisting;

(e) a sufficiently detailed statement of reasons explaining why the delisting order is issued;

(f) the information necessary for the application, where relevant, of paragraphs 4, 5, and 6;

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

(h) the date, time stamp and electronic signature of the competent authority issuing the delisting order;

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

POLITICO

2. **The competent authority issuing the delisting 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 delisting order shall be transmitted to the provider's point of contact referred to in Article 23(1) by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order to the Coordinating Authority in the Member State in which the order was issued and to the EU Centre, through the system established in accordance with Article 39(2).

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

4. **If the provider cannot execute the delisting order on grounds of force majeure or de facto impossibility not attributable to it, including for objectively justifiable technical or operational reasons, it shall, without undue delay, inform the authority issuing the order of those grounds, using the template set out in Annex XI.**

5. **If the provider cannot execute the delisting 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 from the authority issuing the order, using the template set out in Annex XI.**

6. **The provider shall, without undue delay and using the template set out in Annex XII, inform the issuing authority of the measures taken to execute the delisting order, indicating, in particular, whether the provider has prevented search results for the online location with child sexual abuse material to appear.**

The authority issuing the order may require the provider to report to it regularly on the measures taken to execute a delisting order.

7. **The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annexes X, XI and XII where necessary to improve the templates in view of relevant technological developments or practical experiences gained.**

POLITO

Article 18c

Redress and provision of information

1. **Providers of online search engines that have received a delisting order and users that provided the material to a delisted online location shall have a right to effective redress. That right shall include the right to challenge the delisting order before the courts of the Member State of the authority that issued the delisting order.**

2. **If the order is reversed as a result of a redress procedure, the provider shall without undue delay reinstate the delisted online location to appear in search results, without prejudice to the possibility to enforce its terms and conditions in accordance with Union and national law.**

3. **When the delisting order becomes final, the issuing authority shall, without undue delay, transmit a copy thereof and information it has received pursuant to Article 18b (4) to (6) to the Coordinating Authority. The Coordinating Authority shall then, without undue delay, transmit copies thereof to all other Coordinating Authorities and the EU Centre through the system established in accordance with Article 39(2).**

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

3a. **The provider shall establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it 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 obtaining search results for child sexual abuse material corresponding to an online location pursuant to a delisting order, it shall take reasonable measures to inform those users of the following:**

(a) **the fact that it does so pursuant to a delisting order and the reasons for doing so;**

(b) **the right of users that provided the material to a delisted online location to judicial redress referred to in paragraph 1 and users' right to submit complaints to the Coordinating Authority in accordance with Article 34.**

POLITICO

Section 6
Additional provisions

Article 19

Liability of providers

Providers of relevant information society services shall not be liable for child sexual abuse offences **if and insofar as** ~~solely because~~ they carry out, in good faith, ~~the necessary~~ activities to comply with ~~the requirements of~~ this Regulation, in particular activities aimed at **assessing and mitigating risk**, detecting, identifying, **reporting**, removing, disabling ~~of~~ access to, blocking **or delisting from search results** ~~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~~ **in** 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).

POLITICO

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 **support from the EU Centre**~~,~~ upon their request, **to and via** ~~from~~ the Coordinating Authority ~~designated by~~ **in** the Member State where the**y** ~~person~~ reside~~s~~, ~~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.

POLITICO

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 **that is necessary for taking** ~~in connection to~~ the measures ~~taken~~ to comply with this Regulation and the personal data generated through such processing, when the following measures have been taken or for the purposes of complaints or redress procedures ~~complaints only for one or more of the following purposes~~, as applicable:

(xa) insofar as strictly necessary for using the technologies referred to in Article 10, involving in particular the automatic, intermediate and temporary preservation of such data for the use of the indicators provided by the EU Centre, as well as for applying the safeguards referred to in Article 10, when executing a detection order issued pursuant to Article 7;

(a) executing ~~a detection order issued pursuant to Article 7, or~~ a removal order issued pursuant to Article 14 **or a blocking order pursuant to Article 16 or a delisting order pursuant to Article 18a;**

(b) reporting **information that indicate** 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~~;~~**.**

1a. **Upon a request** ~~responding to requests~~ issued by **a** competent ~~law enforcement~~ authorit**y**~~ies and judicial authorities~~ **, providers shall** ~~with a view to~~ provid~~e~~ing th~~em~~ **requesting authority** with the necessary information for the prevention, detection, investigation or prosecution of child sexual abuse offences~~,~~ **or the handling of complaints or admininstrative or judicial redress proceedings,** insofar as the content data and other data **have been preserved for one of the purposes in paragraphs 1(a) to (d)**. ~~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.

POLITICO

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 **measures taken that led to the obligation to preserve the information** ~~reporting or of the removal or disabling of access, whichever occurs first~~. **They shall subsequently irrevocably delete the information.**

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

3. 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 22a

Keeping of logs

1. Providers of hosting services and providers of interpersonal communications services shall record, in respect of any processing of content and other data in connection with the execution of detection order pursuant to Article 7, the time and duration of the processing and, where applicable, the person performing the processing.

2. The logs shall only be used for the verification of the lawfulness of the processing, for self-monitoring, for ensuring data integrity and data security as well as for the purposes of criminal or disciplinary proceedings.

3. Providers shall keep the information contained in the logs referred to in paragraph 1 for no longer than necessary for the applicable purpose and, in any event, no longer than five years from the date of the measures taken that led to the obligation to preserve the information recorded in those logs. They shall subsequently irrevocably delete the information.

They shall, upon request from the competent national authority or court, keep the information for a further specified period, set by that the requesting authority or court, where and to the extent necessary for one of the purposes referred to in paragraph 2.

Article 23

Points of contact

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

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

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

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

Article 24

Legal representative

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

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 **orders and** decisions issued in relation to this Regulation, including detection orders, removal orders and**,** blocking orders **and delisting orders**.

POLITICO

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 **to** comply with the **orders and** 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, 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. **The provider or the legal representative** ~~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.

POLITICO

CHAPTER III

SUPERVISION, ENFORCEMENT AND COOPERATION

Section 1
~~Coordinating~~ Authorities of the Member States ~~for child sexual abuse issues~~

Article 25

Coordinating Authorities ~~for child sexual abuse issues~~ and other competent authorities

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

1a. Where a Member State designates more than one competent authority, it shall appoint one of those competent authorities as Coordinating Authority. Where it designates only one competent authority, that competent authority shall be the Coordinating Authority.

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 **the** 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~~ **all** matters **relating to the application, supervision and enforcement of this Regulation** ~~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~~ **including those 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 **competent authorities, including the** Coordinating Authorities ~~and other competent authorities~~ ~~pursuant to paragraph 1~~, Member States shall make publicly available, and communicate to the Commission and the EU Centre, the name**s** of ~~their Coordinating Authority~~ **those authorities as well as their respective tasks or sectors**. They shall keep that information updated.

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

6. **The EU Centre shall, by [*eighteen months and two weeks from the date of entry into force of this Regulation*]**~~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 competent authorities, including** the Coordinating Authorities and their contact points, **designated pursuant to paragraphs 1, 1a, 2 and 5**. The EU Centre shall regularly publish any modification thereto.

7. **Competent authorities** ~~Coordinating Authorities~~ may, where necessary for the performance of their tasks under this Regulation, request **through the Coordinating Authority,** 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**s** services under the jurisdiction of the Member State that designated the requesting **competent authority** ~~Coordinating Authority~~;

   (c) **provide an opinion on** ~~verify~~ the possible need to request ~~competent national authorities to issue~~ **the issuance of** 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) **provide an opinion on** ~~verify~~ the effectiveness of a detection order ~~or a removal order issued upon the request of the requesting Coordinating Authority;~~.]

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

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

POLITICO

Article 26

*Requirements for ~~Coordinating~~ **competent** ~~A~~**a**uthorities*

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

Those authorities shall not seek or take instructions from any other body in relation to carrying out their tasks under this Regulation.

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

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

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

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

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

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

2 ~~3~~. Paragraph ~~2~~ **1** shall not prevent supervision of the ~~Coordinating~~ **competent a**~~A~~uthorities in accordance with national ~~constitutional~~ law~~, to the extent that such supervision does not affect their independence as required under this Regulation~~.

3 4. The ~~Coordinating Authorities~~ **competent authorities** shall ensure that **their** ~~relevant members of~~ staff have the required qualifications, experience**,** and technical skills to ~~perform~~ **carry out the application, supervision and enforcement under this Regulation** ~~duties~~.

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

POLITICO

Section 2
Powers of ~~Coordinating Authorities~~ competent authorities of Member States

Article 27

*Investigatory **and enforcement** powers*

1. Where needed **in order to** ~~for~~ carrying out their tasks **under this Regulation**, **competent authorities** ~~Coordinating Authorities~~ shall have the following powers of investigation, in respect of **conduct by** providers of relevant information society services under the jurisdiction of ~~the~~ **their** 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 **without undue delay** ~~within a reasonable time period~~;

   (b) the power to carry out**, or to request a judicial authority to order,** ~~on-site~~ inspections of any premises that those providers or ~~the other~~ **those** 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~~ **those persons** to give explanations in respect of any information relating to a suspected infringement of this Regulation and to record the answers **by any technical means**;

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

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

POLITICO

~~*Article 28*~~

~~*Enforcement powers*~~

2. ~~1.~~ Where needed for carrying out their tasks **under this Regulation**, **competent authorities** ~~Coordinating Authorities~~ shall have the following enforcement powers, in respect of providers of relevant information society services under the jurisdiction of ~~the~~ **their** 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 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 **or to request a judicial authority to do so;**

(c) the power to impose fines, or request a judicial authority in their Member State to do so, in accordance with Article 35 for **failure to comply with** ~~infringements of~~ this Regulation, including ~~non-compliance with~~ any of the orders issued pursuant to **paragraph 1 of this** Article ~~27 and to point (b) of this paragraph~~;

(d) the power to impose a periodic penalty payment**, or to request a judicial authority to do so,** 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 **sub**paragraph or for failure to comply with any of the orders issued pursuant to **paragraph 1 of this** Article. ~~27 and to point (b) of this paragraph~~;

(e) the power to adopt interim measures **or to request the competent national judicial authority to do so,** to avoid the risk of serious harm.

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

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

~~*Article 29*~~

~~*Additional enforcement powers*~~

3. ~~1.~~ Where needed for carrying out their tasks **under this Regulation**, **competent authorities** ~~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**ir** Member State**, where** ~~that designated them, provided that:~~

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

~~(b)~~ **and** the infringement **has not been remedied or is continuing and is** ~~persists;~~

~~(c) the infringement~~ ~~causes~~ **causing** serious harm which cannot be avoided through the exercise of other powers available under Union or national law**, also have the power to take the following measures:**

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

(a) **to** require the management body of the providers**, without undue delay,** 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; **and**

~~(iii)~~ report on the measures taken;

(b) **where the competent authorities consider that a provider of relevant information society services has not sufficiently complied with the requirements of point (a), that the infringement has not been remedied or is continuing and is causing serious harm, and that that infringement entails a criminal offence involving a threat to the life or safety of persons or the infringement results in the regular and structural facilitation of child sexual abuse offences,** to request **that** the competent judicial authority or **other** independent administrative authority of its ~~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~~ **competent authorities** shall, prior to submitting the request referred to in **this** paragraph ~~2~~, point (b), invite interested parties to submit written observations **within a period that shall not be less than two weeks, describing the measures that it intends to request and identifying 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 before the competent judicial authority or other independent administrative authority.**

~~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 **of access** shall **be** ~~apply~~ for a period of four weeks, subject to the possibility for the competent judicial authority **or other independent administrative authority of the Member State**, in its order, to allow the ~~Coordinating Authority~~ **competent authorities** to extend that period for further periods of the same lengths, subject to a maximum number of extensions set by **that** judicial authority **or other independent administrative authority**.

The ~~Coordinating Authority~~ **competent authorities referred to in the second subparagraph** shall only extend the period where ~~it considers~~, having regard to the rights and ~~legitimate~~ interests of all parties affected by ~~the~~ **that** 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, **it considers** that both of the following conditions have been met:

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

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

Where the ~~Coordinating Authority~~ **competent authority,** considers that **the conditions set out in the fifth subparagraph, points (a) and (b)** ~~those two conditions~~ have been met but it cannot further extend the period pursuant to the **fourth** ~~second~~ subparagraph, it shall submit a new request to the ~~competent~~ judicial authority **or other independent administrative authority**, as referred to in **the first sub**paragraph ~~2~~, point (b).

~~*Article 30*~~

~~*Common provisions on investigatory and enforcement powers*~~

4. ~~1.~~ The measures taken by the ~~Coordinating Authorities~~ **competent authorities** in the exercise of their investigatory and enforcement powers **listed in paragraphs 1, 2 and 3** ~~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 **relevant** ~~applicable~~.

5. ~~2.~~ Member States shall **lay down specific rules and procedures for the exercise of the powers pursuant to paragraphs 1, 2 and 3 and shall** ensure that any exercise of **those** ~~the investigatory and enforcement~~ powers ~~referred to in Articles 27, 28 and 29~~ is subject to adequate safeguards laid down in the applicable national law **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 **parties**.

Article 31

Searches to verify compliance

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

POLITICO

~~*Article 32*~~

~~*Notification of known child sexual abuse material*~~

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

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

Section 3

Other provisions on enforcement

Article 33

Jurisdiction

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

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

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

Article 34

Right ~~of users of the service~~ to lodge a complaint

1. Users **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 **against providers of relevant information society services** alleging an infringement of this Regulation ~~affecting them~~ ~~against providers of relevant information society services~~ with the Coordinating Authority ~~designated by~~ **in** the Member State where the user **is located** ~~resides~~ or ~~is~~ established.

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

3. The Coordinating Authority ~~receiving the complaint~~ shall assess the complaint and, where appropriate, transmit it to the Coordinating Authority of establishment**, accompanied, where appropriate, by its reasoning**.

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

4. 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.

Article 34a

Representation

1. Without prejudice to Directive (EU) 2020/1828 or to any other type of representation under national law, users of relevant information society services shall at least have the right to mandate a body, organisation or association to exercise the rights conferred by this Regulation on their behalf, provided the body, organisation or association meets all of the following conditions:

(a) it operates on a non-profit basis;

(b) it has been properly constituted in accordance with the law of a Member State;

(c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.

2. Providers of relevant information society services shall take the necessary technical and organisational measures to ensure that complaints submitted by bodies, organisations or associations referred to in paragraph 1 of this Article on behalf of users through the mechanisms referred to in Article 34 are processed and decided upon with priority and without undue delay.

POLITO

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 **in accordance with Article 27**.

   ~~The p~~**P**enalties shall be effective, proportionate and dissuasive**, taking into account the risk categorisation of services laid down in Article 5(2)**. 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 **fines that may be** ~~penalties~~ imposed for ~~an~~ a **failure to comply with an obligation laid down in** ~~infringement of~~ this Regulation shall ~~be~~ not exceed 6 % of the annual **worldwide** ~~income or global~~ turnover of the **providers concerned in the** preceding financial ~~business~~ year ~~of the provider~~. ~~3.~~ **Member States shall ensure that the maximum amount of the fine that may be imposed** ~~Penalties~~ for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information ~~or~~ **and failure** to submit to an ~~on site~~ inspection shall ~~be~~ not exceed 1% of the annual income or worldwide ~~global~~ turnover of the ~~preceding business year of the~~ provider or ~~the other~~ person concerned in the preceeding financial year ~~referred to in Article 27~~.

3~~4~~. Member States shall ensure that the maximum amount of a periodic penalty payment shall ~~be~~ not exceed 5 % of the average daily **worldwide** ~~global~~ turnover **or income** of the provider ~~or the other person referred to in Article 27~~ in the preceding financial year per day, calculated from the date specified in the decision concerned.

4~~5~~. Member States shall ensure **that the competent authorities**, when deciding whether to impose a penalty and when determining the type and level of penalty, account is taken of all relevant circumstances, including:

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

   (b) whether the infringement was intentional or negligent;

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

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

POLITO

(e) the level of cooperation of the provider or the other person **with the competent authorities**;

(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**, taking into account the technical and organisational measures taken by **the provider** ~~it~~ to comply with this Regulation.

Section 4

Cooperation

Article 36

Identification and submission of online child sexual abuse

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

(a) specific items of material and ~~transcripts~~ **extracts** of conversations that **competent authorities** ~~Coordinating Authorities~~ ~~or that the competent judicial authorities or other independent administrative authorities~~ of a Member State have identified, after a diligent assessment, **subject to adequate oversight by judicial authorities,** 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 **the electronic location of the information** ~~specific items of material~~ that **competent authorities** ~~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 material identified as child sexual abuse material, the ~~transcripts~~ **extracts** of conversations identified as the solicitation of children, and the uniform resource locators, identified by **a competent authority** ~~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.

1a. By deviation from paragraph 1, last subparagraph, Member States may decide that the submission to the EU Centre, in accordance with the requirements specified in points (a) and (b) of paragraph 1, can be carried out by the competent authorities without undue delay and through the system established in accordance with Article 39(2). Where a Member State is making use of this possibility, the competent authority shall inform the Coordinating Authority of all the correspondence with the EU Centre.

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~~ **competent 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~~ **competent authority** submits the material to the EU Centre, in accordance with that paragraph, within ~~one~~ **two** month**s** from the date of reception of the report or, where the assessment is particularly complex, ~~two~~ **six** 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 **in a manner negatively affecting the users of the service in the Member State of that Coordinating Authority**, it **may** ~~shall~~ request the Coordinating Authority of establishment to assess the matter and **to** take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

POLITICO

~~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~~ **A** request ~~or recommendation~~ **pursuant** ~~referred~~ to ~~in~~ paragraph 1 shall **be duly reasoned and** 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 **including the description of the negative effects of the alleged infringement**;

(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~~ **or** suggestions for specific investigatory or enforcement measures to be taken**, including interim measures**.

3. The Coordinating Authority of establishment shall **take utmost account of the requests pursuant to paragraph 1 of this Article** ~~assess the suspected infringement, taking into utmost account the request or recommendation referred to in paragraph 1~~. Where it considers that it has insufficient information to ~~asses the suspected infringement or to~~ act upon the request ~~or recommendation~~ and has reasons to consider that the Coordinating Authority that sent the request~~, or the Commission,~~ could provide additional information, it may request such information. The time period laid down in paragraph 4 shall be suspended until that additional information is provided.

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

Article 38

Joint investigations

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

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

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

Article 38a

Mutual assistance

1. The Coordinating Authorities and the other competent authorities of the Member States shall cooperate closely and provide each other with mutual assistance in order to apply this Regulation in a consistent and efficient manner. Mutual assistance shall include, in particular, exchange of information in accordance with this Article and the duty of the Coordinating Authority to inform all the other Coordinating Authorities about the opening of an investigation and the intention to take a final decision, including its assessment, in respect of a specific provider of a relevant information society service.

2. For the purpose of an investigation, a Coordinating Authority may request a Coordinating Authority in another Member State to provide specific information in their possession as regards a specific provider of relevant information society services or to exercise their investigative powers referred to in Article 27(1) with regard to specific information located in their Member State. Where appropriate, the Coordinating Authority receiving the request may involve other competent authorities or other public authorities of the Member State in question.

3. The Coordinating Authority receiving the request pursuant to paragraph 2 shall comply with such request and inform the requesting Coordinating Authority about the action taken, without undue delay, unless:

   (a) the scope or the subject matter of the request is not sufficiently specified, justified or proportionate in view of the investigative purposes; or

(b) neither the requested Coordinating Authority nor other competent authority or other public authority of that Member State is in possession of the requested information nor can have access to it; or

(c) the request cannot be complied with without infringing Union or national law.

The Coordinating Authority receiving the request shall justify its refusal by submitting a reasoned reply, within the period set out in the first subparagraph.

Article 39

*~~General c~~Cooperation**, coordination** and information-sharing system*

1. **Competent authorities** ~~Coordinating Authorities~~ shall **sincerely** cooperate with each other, ~~other competent authorities of the Member States that designated the Coordinating Authority~~, the Commission, the EU Centre and other relevant Union agencies, including Europol, to facilitate the performance of their respective tasks under this Regulation and **to** ensure its effective, efficient and consistent application and enforcement**, without prejudice to the possibility for Member States to provide for cooperation mechanisms and regular exchanges of views between the competent authorities where relevant for the performance of their respective tasks in accordance with this Regulation**.

1a. The authorities and agencies referred to in paragraph 1 shall, including with the support from the EU Centre, coordinate their work for the performance of their respective tasks under this Regulation, with a view to ensuring its effective, efficient and consistent application and enforcement and avoiding interference with criminal investigations in different Member States and duplication of efforts.

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

2a. The information sharing system or systems referred to in paragraph 2 shall facilitate compliance with the obligations set out in Article 83(2) by enabling automated collection and easy retrieval of relevant statistical information.

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

4. The Commission shall adopt implementing acts laying down the practical and operational arrangements for the functioning of the information-sharing **system or** 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~~**]**.

POLITICO

Section 2

Tasks

Article 43

Tasks of the EU Centre

The EU Centre shall:

1. facilitate the risk assessment **and risk mitigation** 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) **and assisting in identifying and assessing technical aspects of specific mitigation measures pursuant to Article 4(3a)**;

   (c) upon request from the Coordinating Authority of establishment, providing an opinion on technical aspects of the possible actions that it intends to require pursuant to Article 5a(1), first subparagraph;~~.~~

   (d) upon request from the Coordinating Authority of establishment, assisting in evaluating the mitigation measures taken by the provider, evaluating the level of the remaining risk and evaluating the self-assessment by the provider for the risk categorisation pursuant to Article 5(2);

   (e) keep a record of the decisions by the Coordinating Authorities of establishment on the risk categorisation of services notified to the EU Centre pursuant to Article 5(2).

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);

   (aa) conducting simulation tests in connection to the possible issuance of detection orders, in accordance with Article 47a;

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

POLITICO

(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**, 5a** 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);

(aa) receiving decisions on a cross-border removal order transmitted to it pursuant to Article 14a(5);

(ab) receiving copies of final removal orders and thereto connected information transmitted to it pursuant to Article 15(2);

~~(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);

(ca) receiving copies of final blocking orders and thereto connected information transmitted to it pursuant to Article 18(2);

(cb) receiving the delisting orders transmitted to it pursuant to Article 18b(2);

(cc) receiving copies of final delisting orders and thereto connected information transmitted to it pursuant to Article 18c(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 **competent authorities, including 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:

POLITICO

(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 **competent authorities** ~~Coordinating Authorities~~ **free of charge and in accordance with its tasks under this Regulation** ~~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, **competent authorities including** 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 **and by inviting other Union institutions, bodies, offices and agencies, competent authorities including Coordinating Authorities, or other relevant authorities of the Member States to share information about relevant prevention initiatives**;

(ba) making available the knowledge referred to in paragraphs (a) and (b) in the database referred to in Article 50(4), and in accordance with Article 51;

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

7. develop or facilitate the further development of technologies to detect online child sexual abuse in accordance with Article 50 (1a);

8. advise the Commission with a view of preparing implementing acts for the approval of technologies used to detect the dissemination of known or new child sexual abuse material or the solicitation of children in accordance with Article 10 (2);

9. certify technologies that are intended to be used to detect the dissemination of known or new child sexual abuse material in services using end-to-end encryption following tests conducted with the support of its Technology Committee that their use could not lead to a weakening of the protection provided by the encryption in accordance with Article 10(3)(ab).

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**s** of uniform resource locators compiled by the EU Centre in accordance with paragraph 3 **for the purpose of, respectively, the issuance of blocking orders in accordance with Article 16 and the issuance of delisting orders in accordance with Article 18a**;

   (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~~ **competent** authorities of the Member States, submitted to it by the Coordinating Authorities pursuant to Article 36(1), point (a), **or by other competent authorities pursuant to Article 36(1a)**.

POLITICO

The EU Centre shall compile ~~the~~ list**s** 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) **for the purpose of, respectively, the issuance of blocking orders in accordance of Article 16 and the issuance of delisting orders in accordance with Article 18a.**

4. The EU Centre shall keep records of the submissions and of the process applied to generate the indicators and compile the list**s** referred to in the first and second subparagraphs. It shall keep those records for **no longer than** ~~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~~ **competent 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.

POLITICO

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 **and providers of online search engines** 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~~ **competent 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.

POLICO

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~~ lists 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).

POLITICO

Article 47a

Simulation tests to assist in connection to the possible issuance of detection orders

1. Where requested by the Coordinating Authority of establishment, the EU Centre shall conduct the tests referred to in Article 7(2), last subparagraph. Those tests shall, in particular, consist of the EU Centre engaging in the exchange of simulated child sexual abuse material so as to determine whether and if so, to which extent and in which manner the service in question, or certain identifiable parts or components thereof, can be used, where relevant by certain specific users or groups or types of users, for the purpose of child sexual abuse.

2. The tests referred to in paragraph 1 shall:

(a) only be conducted involving accounts specifically set up and solely operated by the EU Centre for the purpose of those tests;

(b) only be conducted by duly authorised staff of the EU Centre, subject to adequate safeguards and supervision, and be duly documented;

(c) be designed and conducted by the EU Centre in an accurate and objective manner, so as to lead to non-biased and representative outcomes.

(d) not involve any exchange of child sexual abuse material, nor involve or otherwise affect communications, with or between any users other than the relevant staff of the Centre;

(e) be conducted without the knowledge of the service provider concerned.

3. The EU Centre shall design and prepare conduct the test referred to in paragraph 1 in cooperation with the Coordinating Authority of establishment that made the request and, where so requested, also with the relevant law enforcement authorities indicated in the request. That Coordinating Authority shall in any event inform the relevant law enforcement authorities of the tests in due time prior to the beginning of the tests.

4. The EU Centre shall, without undue delay, report to the Coordinating Authority of establishment that made the request on the outcomes of the tests referred to in paragraph 1. Those reports shall not contain any personal data.

The EU Centre shall store those reports. It may make those reports or some or all of the outcomes of the tests available to other Coordinating Authorities and it may use those reports or outcomes for the performance of its other tasks under this Regulation, subject to the protection of confidential information.

POLITICO

5. **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 the tests referred to in paragraph 1, in particular as regards procedural aspects, the design and conduct of those tests, the necessary safeguards and supervision, cooperation, reporting and storage, as well as the making available and further use of the reports or their outcomes.**

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~~ **there are reasonsable grounds for the EU Centre to consider that the** ~~a~~ report is **not manifestly un**founded, 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.~~

The EU Centre shall perform the assessment and processing referred to in paragraphs 1, 2 and 3 of this Article as a matter of priority in respect of reports submitted in accordance with Article 13(2), first subparagraph. In particular, where there are reasonable grounds for the EU Centre to consider that the report is founded and that there is likely to be an imminent threat to the life or safety of a child including when the report indicates ongoing abuse, it shall immediately forward the report in accordance with paragraph 3, marking it as requiring urgent action.

In other cases, it shall forward the report in accordance with paragraph 3 without such marking and inform the provider that submitted the report and the competent authority, indicating in all cases the outcome of the assessment and the reasons explaining that outcome.

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, **as well as constitute necessary and proportionate restrictions and respect the essence of the rights of the victims**.

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);

POLITO

(b) where so requested to assist a ~~Coordinating Authority~~ **competent 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), point~~s~~ (c) ~~and (d), respectively~~;

(c) where so requested to assist a Coordinating Authority, by verifying the effectiveness of a detection order that the competent authorities issued, in accordance with Article 25(7), point (d).

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**s** 10(1) **and 10a**.

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.

1a. **The EU Centre shall, in cooperation with Coordinating Authorities, providers of hosting services and providers of interpersonal communications services and, where relevant, independent experts, develop or facilitate the further development of technologies to detect online child sexual abuse, in such a manner as to ensure that those technologies are capable of meeting the requirements of this Regulation, in particular Article 10(3).**

1b. **Where the EU Centre has been requested, in accordance with this Regulation, to provide an opinion, information or other assistance on technologies, including a functional and security audit at the source code level, that may be used for the execution of a specific order issued under this Regulation, it may, in accordance with Article 66, request the Technology Committee for its opinion thereon. In that case, the rules of the third paragraph on the time period for providing that opinion shall apply.**

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~~ **3a**. **The EU Centre shall keep a database encompassing all research, surveys and studies, involving public EU or national resources, as referred to in paragraphs 2 and 3 and the information resulting thereof. That database shall not contain any personal data other than information identifying the authors and any other persons having contributed to the research, survey and studies.**

POLITICO

The competent authorities may consult this database where necessary for the performance of their tasks under this Regulation.

The EU Centre may decide to provide the appropriate level of access for consultation of this database to other entities and individuals upon reasoned request, if the requesting entities and individuals can justify that such access could contribute to the achievement of the objectives of this Regulation.

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**s** 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;

POLITICO

(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.

POLITICO

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.

POLITICO

Article 53a

Cooperation with other Union agencies and bodies

1. In addition to the obligation to cooperate with Europol in accordance with Article 53, where necessary for the performance of its tasks under this Regulation, the EU Centre may cooperate with other Union agencies and bodies, in particular the EU Agency for Fundamental Rights, the European Union Agency for Cybersecurity, the European Data Protection Supervisor and the European Data Protection Board in accordance with the respective mandates of the EU Centre and those other Union agencies and bodies.

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

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**, including on data sharing**.

Article 54a

Cooperation with third countries and international organisations

1. In so far as is necessary in order to achieve the objectives set out in this Regulation, and without prejudice to the respective competences of the Member States and the institutions of the Union, the EU Centre may cooperate with, the competent authorities of third countries or with international organisations.

To this end, the EU Centre may, subject to prior approval by the Commission, establish working arrangements with the authorities of third countries or international organisations. These arrangements shall not create legal obligations incumbent on the Union and its Member States.

POLITICO

2. The EU Centre shall be open to the participation in its work of third countries that have entered into agreements with the Union to this effect.

Under the relevant provisions of the agreements referred to in the first subparagraph, arrangements shall be developed specifying, in particular, the nature, extent and manner in which the third countries concerned will participate in the work of the EU Centre, including provisions relating to participation in the initiatives undertaken by the EU Centre, financial contributions and staff. As regards staff matters, those arrangements shall, in any event, comply with the Staff Regulations.

3. The Management Board shall adopt a strategy for relations with third countries or international organisations concerning matters for which the EU Centre is competent. The Commission shall ensure that the EU Centre operates within its mandate and the existing insitutional framework by concluding an appropriate working arrangement with the EU Centre's Executive Director.

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.

POLITICO

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 **one** ~~two~~ representative~~s~~ 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, **without the right to vote,** 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~~ **competencies**. 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;

   (aa) be responsible for the overall planning and the execution of the tasks conferred on the EU Centre pursuant to Article 43, and it shall adopt all the decisions of the EU Centre;

POLITO

(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;

(fa) consult the Victims Board in all cases where, in the performance of its tasks pursuant to points (a) and (h), interests of victims are concerned;

(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;

(i) adopt, by 30 November of each year, 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;

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

(k) 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 of each year, to the European Parliament, the Council, the Commission and the Court of Auditors and make the consolidated annual activity report public;

(l) 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;

(m) 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[27] ("the appointing authority powers");

(n) 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;

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

(p) 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;

(q) 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);

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

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

(t) appoint a Data Protection Officer;

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

(v) authorise the conclusion of memoranda of understanding referred to in Articles 53(3), 53a(2) and 54(2).

2. With respect to the powers mentioned in paragraph 2 point (m) and (n), the Management 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.

[27] 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)

POLITICO

3. In exceptional circumstances, the Management 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.

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.

3. The detailed procedure for the election of the Chairperson and the Vice-Chairperson shall be set out in the rules of procedure of the Management Board.

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**, including representatives of the Victims Board**.

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**, including representatives of the Victims Board**.

6. The EU Centre shall provide the secretariat for the Management Board.

POLITO

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 **with voting rights**.

2. Each member shall have one vote. In the absence of a member **with the right to vote**, 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.~~

POLITICO

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[28] ("the appointing authority powers");

[28] 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)

(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;

(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.

POLITICO

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.

POLITICO

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~~ **Management** Board after consulting the Commission;

(e) implementing the Single Programming Document and reporting to the ~~Executive~~ **Management** Board on its implementation;

(f) preparing the Consolidated Annual Activity Report ~~(CAAR)~~ on the EU Centre's activities and presenting it to the ~~Executive~~ **Management** 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 **by reporting any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 24 of Regulation (EU) 2017/1939.**~~, where appropriate, by imposing effective, proportionate and dissuasive administrative, including financial penalties;~~

POLITICO

(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~~ **Management** 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~~ **Management** 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.

6. Without prejudice to the powers of the Commission and of the Management Board, the Executive Director shall be independent in the performance of the duties and shall neither seek nor take instructions from any government nor from any other body.

POLITICO

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~~ **Management** 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~~ **Management** 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~~ **Management Board, with the support of 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~~ **Management** 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~~ **Management** Board ~~acting on a proposal from the Commission~~.

8. The ~~Executive~~ **Management** 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.

POLITICO

Subsection 5: Technology Committee and Victims Board

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, their independence, and particular area of expertise, to ensure a complete and varied set of skills and expertise** ~~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. **Member States may nominate up to four technical experts each, of which the Management Board shall select a maximum of two per Member State while the Commission and Europol may nominate up to two technical experts each, from which the Management Board shall select one of each. The Management Board may appoint up to eleven additional experts beyond those nominated by Member States, or appointed by the Commission and Europol. These experts nominated by Member States are not seconded national experts but experts mandated by Member States to perform technical expertise missions on an ad hoc basis upon request by the Management Board.**

   The experts of the Technology Committee shall act in the general interest, observing the principles of neutrality and transparency.

1a. **The Technology Committee shall be divided in working groups specialised in assessing specific categories of technologies or types of technologies used to prevent and combat online child sexual abuse. Those working groups may call on external experts on an ad hoc basis.**

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 **acting in the general interest, neutrality or transparency in the framework of his/her mandate** ~~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 the member appointed** by ~~of~~ the Commission, ~~a lack of independence~~ **that the member is no longer acting in the general interest, or that he or she does not meet the neutrality or transparency criteria** and revoke the **appointment of that member**. ~~The Management Board shall appoint a new member~~ **In that case, a replacement shall be appointed** for the ~~remaining term of office~~ **remainder of the mandate of the member concerned** in accordance with the procedure **described in paragraph 1** ~~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);

(aa) contribute to the EU Centre's activities related to the development, or facilitation of the development, of technologies to detect online child sexual abuse, in accordance with Article 50(1a);

(ab) contribute to the EU Centre's activities related to the advice provided to the Commission with a view of preparing implementing acts for the approval of technologies used to detect the dissemination of known or new child sexual abuse material in accordance with Article 10(2);

(ac) contribute to the EU Centre's activities related to the testing of technologies that are intended to be used to detect the dissemination of known or new child sexual abuse material in services using end-to-end encryption with a view of excluding that their use could lead to a weakening of the protection provided by the encryption in accordance with Article 10(3)(ab);

(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;

(d) provide internally expertise after having involved the relevant working group or groups, on an ad hoc basis and at the request of the Management Board.

Article 66a

Appointment and tasks of the Victims ~~and Survivors~~ Board

1. The Victims Board shall be comprised of adult victims of child sexual abuse and recognised experts in providing assistance to victims who, following a call for expressions of interest published in *the Official Journal of the European Union,* shall be appointed by the Management Board on the basis of their personal experience, expertise and independence.

2. The procedures governing the appointment of the members of the Victims Board, its functioning and the conditions governing the transmission of information to the Victims Board shall be laid down in the Management Board's rules of procedure, and shall be published.

POLITO

3. The members of the Victims Board shall be independent in carrying out their tasks as members thereof and shall act in the interest of victims of online child sexual abuse. The EU Centre shall publish on its website and maintain updated the list of the members of the Victims Board.

4. Members who cease to be independent shall inform the Management Board accordingly. In addition, the Management Board, at the proposal of at least one third of its members or of the member appointed by the Commission, may determine that a given member lacks sufficient independence and revoke the appointment. The Management Board shall appoint a replacement for the remainder of mandate of the member concerned, following the procedure referred to in paragraph 1.

5. The mandate of members of the Victims Board shall be four years. It may be renewed once by the Management Board.

6. The Executive Director and the Management Board may consult the Victims Board in connection with all matters concerning victims of online child sexual abuse.

7. The Victims Board has the following tasks:

(a) make the concerns of victims heard and represent their interests in connection to the work of the EU Centre;

(b) advise the Management Board in matters referred to in Article 57 (1)(fa);

(c) advise the Executive Director and the Management Board when consulted in accordance with paragraph 6;

(d) contribute their experience and expertise to the work of the EU Centre as a knowledge hub as regards preventing and combating online child sexual abuse and assisting and supporting victims;

(e) contribute to the work of the EU Centre in connection to European networks of victims of child sexual abuse.

POLITICO

Section 6

Establishment and Structure of the Budget

Subsection 1

Single Programming Document

Article 67

Establishment of the budget ~~*Budget establishment and implementation*~~

1. Each year the Executive Director shall draw up a **provisional** draft ~~statement of~~ estimate~~s~~ of the EU Centre's revenue and expenditure for the following financial year, including ~~an~~ **the** establishment plan, and shall send it to the ~~Executive~~ **Management** Board.

2. The provisional draft estimate shall be based on the objectives and expected results of the annual programming document, and shall take into account the financial resources necessary to achieve those objectives and expected results, in accordance with the principle of performance-based budgeting.

~~2~~**3**. The ~~Executive~~ **Management** Board shall, on the basis of the **provisional** draft ~~statement of~~ estimate~~s~~, 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.

4. The Commission shall send the draft estimate to the budgetary authority together with the draft general budget of the Union. The draft estimate shall also be made available to the EU Centre.

5. On the basis of the draft estimate, 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 budgetary authority in accordance with Articles 313 and 314 TFEU.

6. The budgetary authority shall authorise the appropriations for the contribution from the general budget of the Union to the EU Centre.

7. The budgetary authority shall adopt the EU Centre's establishment plan.

8. The Management Board shall adopt the EU Centre's budget. It shall become final following the final adoption of the general budget of the Union and, if necessary, it shall be adjusted accordingly.

POLITO

9. For any building project likely to have significant implications for the budget of the EU Centre, Delegated Regulation (EU) 2019/715 shall apply.

~~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 Management 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.~~

POLITICO

Subsection 2

Presentation, implementation and control of the budget of the EU Centre

*Article **68** ~~69~~*

Structure of the ~~B~~budget

1. Estimates of all revenue and expenditure ~~for~~ **of** 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.~~ **and shall be shown in the EU Centre's budget. The financial year shall correspond to the calendar year.**

2. The EU Centre's budget shall be balanced in terms of revenue and of expenditure.

3. Without prejudice to other resources, the EU Centre's revenue shall comprise:

(a) a contribution from the Union entered in the general budget of the Union;

(b) any voluntary financial contribution from the Member States;

(c) any contribution from third countries participating in the work of the EU Centre, as provided for in Article 54a;

(d) possible Union funding in the form of delegation agreements or ad hoc grants in accordance with the EU Centre's financial rules referred to in Article 70 and with the provisions of the relevant instruments supporting the policies of the Union;

(e) charges for publications and any service provided by the EU Centre.

4. The expenditure of the EU Centre shall include staff remuneration, administrative and infrastructure expenses, and operational 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.~~

POLITICO

*Article **69** ~~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).

1a. The EU Centre's accounting officer shall also provide the required accounting information for consolidation purposes to the Commission's accounting officer, in the manner and format required by the latter by 1 March of year N + 1.

2. The EU Centre shall send ~~a~~ **the** report on the budgetary and financial management for year N to the European Parliament, the Council**, the Commission** 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.~~ **On receipt of the Court of Auditor's observations on the EU Centre's provisional accounts for year N, the EU Centre's accounting officer shall draw up the EU Centre's final accounts under his or her own responsibility. The Executive Director shall submit them to the Management Board for an opinion.**

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~~,~~ **and** the Court of Auditors ~~and national parliaments~~, together with the Management Board's opinion.

6. **A link to the pages of the website containing** ~~T~~the final accounts **of the EU Centre** ~~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~~ **The Executive Director** shall also send ~~the~~ **this** reply to the Management Board **and to the Commission**.

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**, in accordance with Article 261(3) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council.**

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

*Article **70** ~~68~~*

Financial rules

The financial rules applicable to the EU Centre shall be adopted by the ~~Executive~~ **Management** Board after consultation with the Commission. They shall not depart from Delegated Regulation (EU) 2019/715[29] unless such a departure is specifically required for the operation of the EU Centre and the Commission has given its prior consent.

The EU Centre shall establish and implement its budget in line with its financial rules and the Financial Regulation (EU) 2018/1046.

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~~ **Management** 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~~ **Management** 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~~ **Management** Board shall aim to ensure consistency with the rules applicable to reimbursement of the mission expenses of the statutory staff.

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

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~~ **Management** 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~~ **Management** 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[30].

[30] 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).

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[31] 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~~ **Management** 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[32] 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.

Article 77

Transparency and communication

1. Regulation (EC) No 1049/2001[33] 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.

POLITICO

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

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

33 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.

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[34] 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**, within the scope of its mandate,** carry out investigations, ~~including~~ **which may also include** 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[35].

POLITO

34 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).

35 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~~ **Management** Board and no later than *[2 years after the entry into force of this Regulation]*.

POLITICO

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~~ **Management** 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 **and national experts seconded to the Commission** 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~~ **Management** Board and may conclude contracts, including staff contracts, following the adoption of the EU Centre's establishment plan.

POLITICO

CHAPTER V

DATA COLLECTION AND TRANSPARENCY REPORTING

Article 83

Data collection

1. **Providers of relevant information society services that were subject to orders issued under Articles 7, 14, 16 and 18a** ~~Providers of hosting services, providers of interpersonal communications services, providers of internet access services~~ shall collect data on the following topics and make that information available to the EU Centre upon request:

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

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

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

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

   (b) the number of removal orders issued to the provider in accordance with Article 14, **indicating the number of those orders that were subject to the procedure for cross-border removal orders referred to in Article 14a**. ~~and the average time needed for removing or disabling access to the item or items of child sexual abuse material in question~~;

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

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

(da) the number of delisting orders issued to the provider in accordance with Article 18a, indicating the number of those orders that were subject to the procedure for cross-border delisting orders referred to in Article 18aa;

(e) the number of instances in which the provider invoked Article 8(3), Article 14(5) or (6)**,** ~~or~~ Article 17**(4a)** or (5) **or Article 18b(4) or (5)**, together with the **reasons** ~~grounds~~ therefor**e**;

2. **Relying to the extent possible on information collected in an automated manner by means of the information sharing system or systems referred to in Article 39(2a), as well as on any similar system that might be used for the exchange of information at national level, t**he Coordinating Authorities shall collect data on the following topics and make that information available to the EU Centre upon request:

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

– whether the report led to the launch of a criminal investigation or **contributed to an ongoing investigation,** ~~led to taking any other action 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, as reported by providers of hosting services and providers of interpersonal communications services in accordance with Article **5** ~~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 **was issued** in accordance with Article 14;

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

(g) the number of blocking orders issued in accordance with Article 16, broken down by provider, and the number of instances in which the provider invoked Article 17**(4a) or** (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;.~~

(ha) the number of complaints received in accordance with Article 34 broken down by what the alleged infringement of this Regulation was concerned with.

3. The EU Centre shall collect data and generate statistics on the detection, reporting, removal of or disabling of access to, **blocking and delisting of** online child sexual abuse under this Regulation. The data shall ~~be~~ **constitute** in particular ~~on~~ the following ~~topics~~.

(a) the number of indicators in the databases of indicators referred to in Article 44 and the development 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 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 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);

POLICE

(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 **included in the reports** ~~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 manifestly unfounded, as referred to in Article 48(2);

(f) the number of reports relating to potential new 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;

(k) a report describing and analysing the relevant technologies, including the published opinions of the European Data Protection Board pursuant to Article 50(1) on the technologies made available by the EU Centre.

4. **Providers of relevant information society services that were subject to orders issued under Articles 7, 14, 16 and 18a** ~~The providers of hosting services, providers of interpersonal communications services and providers of internet access services~~, the Coordinating Authorities **or other competent authorities** and the EU Centre shall ensure that the data referred to in paragraphs 1, 2 and 3, respectively, is stored no longer than is necessary for for the transparency reporting referred to in Article 84. The data ~~stored~~ **referred to in paragraphs 1 to 3** 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.

5~~6~~. 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 the process of data collection and categorisation of the data to be collected pursuant to paragraphs 1 to 4 for the purposes of follow up of the reports and the application of the Regulation.

Article 84

Transparency reporting

1. Each provider of relevant information society services **that was subject to orders issued under Articles 7, 14, 16 and 18a during the relevant calendar year** shall draw up an annual report on its activities under this Regulation. That report shall compile the information referred to in Article 83(1).

   The providers shall, by 31 January of every year subsequent to the year to which the report relates, make the report available to the public and communicate it to the Coordinating Authority of establishment, the Commission and the EU Centre.

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

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

4. The EU Centre~~, working in close cooperation with the Coordinating Authorities,~~ shall draw up an annual report on its activities under this Regulation. That report shall ~~also~~ compile and analyse the information contained in the reports referred to in paragraph~~s~~ 2 and **Article 83(**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.

POLITO

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.

In this report, the Commission shall consider, in particular:

(a) the effectiveness of this Regulation in achieving its objective to prevent and combat in a targeted, carefully balanced and proportionate manner the use of relevant information society services for online child sexual abuse in the internal market;

(b) the impact of the application of this Regulation on fundamental rights, notably:

i. children's rights to physical and mental integrity, the prohibition of torture and inhuman and degrading treatment, their right to respect for private and family life and their right to protection of personal data, and their right to such protection and care as is necessary for their well-being, laid down in Articles 3, 4, 7, 8 and 24 of the Charter respectively;

ii. users' rights to respect for private and family life, to protection of personal data, and the freedom of expression and information, laid down in Articles 7, 8 and 11 of the Charter respectively; and

iii. providers of relevant information society services' freedom to conduct a business, laid down in Article 16 of the Charter;

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.

POLICO

3. On the occasion of every second evaluation referred to in paragraph 2, the results achieved by the EU Centre shall be assessed **by the Commission**, having regard to **the EU Centre's** 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, **4, 5, 5b**, **7,** 8, 13, 14, 17, **18b**, 47, **47a**, **83** and 84 shall be conferred on the Commission for an indeterminate period of time from [*date of adoption of the Regulation*].

3. The delegation of power referred to in Articles 3, **4, 5, 5b**, **7,** 8, 13, 14, 17, **18b**, 47, **47a, 83** 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, **4, 5, 5b**, **7,** 8, 13, 14, 17, **18b**, 47, **47a, 83** 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**s 10(2) and** 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.

1a. With regard to the implementing acts referred to in Article 10(2), Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), the third subparagraph, of Regulation (EU) No 182/2011 shall apply.

2. ~~Where reference is made to this paragraph~~**With regard to the implementing acts referred to in Article 39(4),** Article 4 of Regulation (EU) No 182/2011 shall apply.

Article 88

Amendment and** repeal **of Regulation (EU) 2021/1232

1. In Article 10 of Regulation (EU) 2021/1232, the second paragraph is deleted.

2. Regulation (EU) 2021/1232 is repealed from *[date of application **54 months after entry into force** of this Regulation]*.

POLITICO

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~~ ***[24** months after ~~its~~ entry into force **of this Regulation]*.** **However:**

- **Article 88(1) shall apply from [*date of entry into force of this Regulation];***
- **Articles 7 to 13, Articles 20 to 22a, Article 25(7)(d), Articles 43(2), (3) and 6(ba), Articles 44 to 50, and Articles 83(3) and 84(4) shall apply from [*date 48 months after entry into force of this Regulation];***

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*

POLITICO

ANNEX I

TEMPLATE FOR DETECTION ORDERS

referred to in Article 8(1) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

DETECTION ORDER ISSUED IN ACCORDANCE WITH REGULATION (EU) …/… LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE ('THE REGULATION')

SECTION 1: Authorities having requested and issued the detection order:

Name of the Coordinating Authority having requested the issuance of the detection order:

(Text)

Name of the competent judicial authority or the independent administrative authority having issued **or having authorised the issuing by the Coordinating Authority of** the detection order:

(Text)

Reference of the detection order:

(Text)

SECTION 2: Addressee of the detection order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point of the provider:

(*Text*)

POLITICO

SECTION 3: Relevant service, targeting and specification

The detection order applies to the following service provided by the provider in the Union:

(Text)

Further information regarding the targeting and specification of the detection order, in accordance with Article 7(7) of the Regulation:

(Text)

SECTION 4: Measures to execute the detection order, including additional safeguards

In accordance with Article 8(1) of the Regulation, the provider is to take the measures specified in Article 10 of the Regulation to execute the detection order including the safeguards specified therein.

The provider is to take those measures to detect the following:

☐ The dissemination of known child sexual abuse material as defined in Article 2, letter (m), of the Regulation

☐ The dissemination of new child sexual abuse material as defined in Article 2, letter (n), of the Regulation

~~☐ The solicitation of children as defined in Article 2, letter (o), of the Regulation~~

~~Where the detection order concerns the solicitation of children, in accordance with Article 7(7), last subparagraph, of the Regulation, the detection order applies only to publicly available interpersonal communications where one of the users is a child user, as defined in Article 2, point (i), of the Regulation.~~

The provider is to execute the detection order using the following indicators made available by the EU Centre on Child Sexual Abuse ('the EU Centre'), in accordance with Article 37 of the Regulation.

☐ The indicators contained in the database referred to in Article 44(1), point (a), of the Regulation

☐ The indicators contained in the database referred to in Article 44(1), point (b), of the Regulation

~~☐ The indicators contained in the database referred to in Article 44(1), point (c), of the Regulation~~

In order to obtain access to the relevant indicators, the provider is to contact the EU Centre at the following address:

(*Contact information and contact point of EU Centre)*

POLITICO

Where applicable, information regarding the additional safeguards that the provider is to put in place, in accordance with Article 7(8) of the Regulation:

(*Text*)

Where relevant, additional information regarding the measures that the provider is to take to execute the detection order:

(Text)

SECTION 5: Reasons, period of application and reporting

The reasons for issuing the ~~removal~~ **detection** order are as follows:

(Sufficiently detailed statement of reasons for issuing the detection order)

The detection order applies from …….. (*date*) to ……. (*date*).

The following reporting requirements apply, in accordance with Article 9(3) of the Regulation:

(*Text*)

SECTION 6: Contact details for follow-up

Contact details of the Coordinating Authority having requested the issuance of the detection order for feedback on the execution of the detection order or further clarification, including the communications referred to in Article 8(3) of the Regulation:

(*Text*)

POLITICO

SECTION 7: Information about redress

Competent court before which the detection order can be challenged, in accordance with Article 9(1) of the Regulation:

(*Text*)

Time periods for challenging the detection order (*days/months starting from*):

(*Text*)

References or links to provisions of national law regarding redress:

(*Text*)

Where relevant, additional information regarding redress:

(Text)

A lack of compliance with this detection order may result in penalties pursuant to Article 35 of the Regulation.

SECTION 8: Date, stamp and signature

Date of issuance of the detection order:

(*Text*)

Time stamp:

(*Text*)

Electronic signature of the competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the detection order:

POLITICO

ANNEX II

TEMPLATE FOR INFORMATION ABOUT THE IMPOSSIBILITY TO EXECUTE THE DETECTION ORDER

referred to in Article 8(3) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the detection order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point of the provider:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the provider:

(*Text*)

SECTION 2: Information regarding the detection order

Name of the Coordinating Authority having requested the issuance of the detection order:

(*Text*)

Name of the competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the detection order:

(*Text*)

Reference of the detection order:

(*Text*)

Date and time of receipt of the detection order, including time zone:

(*Text*)

POLITICO

SECTION 3: Non-execution

The provider cannot execute the detection order within the mandatory time period for the following reasons (tick the relevant box(es)):

☐ The detection order contains one or more manifest errors
☐ The detection order does not contain sufficient information

Specify the manifest error(s) and/or the further information or clarification necessary, as applicable:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX III

TEMPLATE FOR REPORTS

referred to in Article 13(2) of Regulation (EU) .../…[laying down rules to prevent and combat child sexual abuse]

REPORT OF POTENTIAL ONLINE CHILD SEXUAL ABUSE ISSUED IN ACCORDANCE WITH REGULATION (EU) …/… LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE ('THE REGULATION')

SECTION 1: Reporting provider

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point of the provider:

(Text)

Contact information of the provider and, where applicable, of its legal representative:

(*Text*)

SECTION 2: Information on the report

1) Does the report require urgent action, notably because of an imminent threat to the life or safety of the child or children appearing to be victim of the potential online child sexual abuse:

☐ Yes
☐ No

Reasons for urgent action

(*Text – attach data as necessary*)

2) Type of potential online child sexual abuse to which the report relates:

☐ Known child sexual abuse material, as defined in Article 2, letter (m), of the Regulation
☐ New child sexual abuse material, as defined in Article 2, letter (n), of the Regulation
☐ Solicitation of children, as defined in Article 2, letter (o), of the Regulation

POLITICO

3) Content data related to the reported potential online child sexual abuse, including images, videos and texts, as applicable:

(*Text – attach data as necessary*)

4) Other available data related to the reported potential online child sexual abuse, including metadata related to media files **and communications** (date, time, time zone):

(*Text – attach data as necessary*)

5) Information concerning the geographic location related to the potential online child sexual abuse:

- IP address of upload, with associated date and time **stamp, including time** zone, and port number:

  (*Text*)

- Where available, other information concerning the geographical location (postal code, GPS data of media files, etc.):

  (*Text*)

6) Information concerning the identity of any user or users involved in the potential online child sexual abuse, including:

- Username:

  (*Text*)

- Email address:

  (*Text*)

- Phone number:

  (*Text*)

- Other information (mailing address, profile information, other email addresses, other phone numbers, billing information, last login date, other user information or unique user identifier):

  (*Text*)

POLITICO

7) Type of service provided by the provider:

☐ hosting service, as defined in Article 2, point a, of the Regulation
☐ interpersonal communication service, as defined in Article 2, point (b), of the Regulation

Addition information about the service, including webpage/URL:

(*Text*)

8) Manner in which the provider became aware of the potential child sexual abuse:

☐ Measures taken to execute a detection order issued in accordance with Article 7 of the Regulation
☐ Notification by a public authority~~, including notification by the Competent Authority of establishment in accordance with Article 32 of the Regulation~~
□ Notification by a hotline, including a trusted flagger within the meaning of Article **22** ~~19~~ of Regulation (EU) **2022/2065** ~~…/…~~ [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~]
☐ Flagged by a user
☐ Measures taken on the provider's own motion
☐ Other

In accordance with Article 12(1) of the Regulation, providers are not to report potential online child sexual abuse detected through a removal order issues in accordance with the Regulation.
Specification of details regarding the manner in which the provider became aware, as indicated above:

(Text)

9) Has the provider reported, or will it report, the potential online child sexual abuse to a public authority or to another entity competent to receive such reports of a third country?

☐ Yes
☐ No

If yes, indicate the following:

- name of the public authority or other entity:

  (*Text*)

- reference number of the case reported to the public authority or other entity:

  (*Text*)

POLITICO

10) If the report concerns the dissemination of potential known or new child sexual abuse material, has the provider removed or disabled access to the material?

☐ Yes
☐ No

11) Has the provider taken any decision in respect of the user or users involved in relation to the potential online child sexual abuse (blocking account, suspending or terminating the provision of the service)?

☐ Yes
☐ No

If yes, specify decision:

(Text)

12) Where available, information about the child or children appearing to be victim of the potential online child sexual abuse:

- Username:

  (*Text*)

- Email address:

  (*Text*)

- Phone number:

  (*Text*)

- Other (mailing address, profile information, other email addresses, other phone numbers, billing information, last login date, other user information or unique user identifier):

  (*Text*)

13) Where relevant, other information related to the potential online child sexual abuse:

(*Text – attach data as necessary*)

POLITICO

SECTION 3: Date, time and signature

Date and time of issuance of the report, including time zone:

(*Text*)

Time stamp:

(Text)

Signature:

(*Text*)

POLITICO

ANNEX IV

TEMPLATE FOR REMOVAL ORDERS

referred to in Article 14(3) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

REMOVAL ORDER ISSUED IN ACCORDANCE WITH REGULATION (EU) …/… LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE ('THE REGULATION')

SECTION 1: Authorities having ~~requested and~~ issued the removal order

~~Name of the Coordinating Authority having requested the issuance of the removal order:~~

~~*(Text)*~~

Name of the competent ~~judicial~~ authority ~~or the independent administrative authority~~ having issued the removal order:

(Text)

Reference of the removal order:

(*Text*)

SECTION 2: Addressee of the removal order and service concerned

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point:

(*Text*)

Specific service for which the removal order is issued:

(Text)

POLITICO

SECTION 3: Child sexual abuse material concerned and temporary non-disclosure

The provider is to remove or disable access in all Member States, as soon as possible and in any event within 24 hours of receipt of this removal order, the following the child sexual abuse material:

(Exact URL and, where necessary, additional information)

The material constitutes child sexual abuse material, as defined in Article 2, point (l), of the Regulation, as it constitutes material that meets one or more of the following elements of the definition of child pornography and/or of the definition of pornographic performance, set out in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU of the European Parliament and of the Council[41] (tick the relevant box(es)):

- ☐ Any material that visually depicts a child engaged in real or simulated sexually explicit conduct
- ☐ Any depiction the sexual organs of a child for primarily sexual purposes
- ☐ Any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes
- ☐ Realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes
- ☐ Material that visually depicts a live exhibition aimed at an audience of a child engaged in real or simulated sexually explicit conduct
- ☐ Material that visually depicts a live exhibition aimed at an audience of the sexual organs of a child for primarily sexual purposes

Tick, where applicable:

- ☐ To avoid interference with activities for the prevention, detection, investigation, and prosecution of child sexual abuse offences, the provider is not to disclose any information regarding the removal of or disabling of access to the child sexual abuse material in accordance with Article 15(4) of the Regulation, during the following period:

  (*Text*)

[41] 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 of 17.12.2011, p.1).

SECTION 3a: Information to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established

Please tick the relevant box(es):

□ **The Member State where the hosting service provider has its main establishment or where its legal representative resides or is established is other than the Member State of the issuing competent authority**

□ **A copy of the removal order is sent to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established**

□ **The removal order is sent through the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established**

SECTION 4: Contact details for follow-up

Contact details of the ~~Coordinating~~ **competent** ~~A~~**a**uthority having ~~requested the issuance of~~ **issued** the removal order for feedback on the execution of the removal order or further clarification, including the communications referred to in Article 14(5), (6) and (7) of the Regulation:

(*Text*)

SECTION 5: Reasons

The reasons for issuing the removal order are as follows:

(Sufficiently detailed statement of reasons for issuing the removal order)

POLITICO

SECTION 6: Information about redress

Competent court before which the removal order can be challenged, in accordance with Article 15(1) of the Regulation:

(*Text*)

Time periods for challenging the ~~detection~~ **removal** order (days/months starting from):

(*Text*)

References or links to provisions of national law regarding redress:

(*Text*)

Where relevant, additional information regarding redress:

(*Text*)

A lack of compliance with this removal order may result in penalties pursuant to Article 35 of the Regulation.

SECTION 7: Date, stamp and electronic signature

Date of issuance of the removal order:

(*Text*)

Time stamp:

(Text)

Electronic signature of the competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the removal order:

(Text)

POLITICO

ANNEX V

TEMPLATE FOR INFORMATION ABOUT THE IMPOSSIBILITY TO EXECUTE THE REMOVAL ORDER

referred to in Article 14(5) and (6) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the removal order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the provider:

(*Text*)

SECTION 2: Information regarding the removal order

~~Name of the Coordinating Authority having requested the issuance of the removal order:~~

~~*(Text)*~~

Name of the competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the removal order

(*Text*)

Reference of the removal order

(*Text*)

Date and time of receipt of the removal order, including time zone:

(*Text*)

POLITICO

SECTION 3: Non-execution

The provider cannot execute the removal order within the mandatory time period for the following reasons (tick the relevant box(es)):

☐ Force majeure or de facto impossibility not attributable to the provider of hosting services, including for objectively justifiable technical or operational reasons
☐ The removal order contains one or more manifest errors
☐ The removal order does not contain sufficient information

Provide further information regarding the reasons for non-execution, specifying the reasons of force majeure or de facto impossibility, the manifest error(s) and/or the further information or clarification necessary, as applicable:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX VI

TEMPLATE FOR INFORMATION ON THE EXECUTION OF THE REMOVAL ORDER

referred to in Article 14(7) of Regulation (EU) .../…[*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the removal order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Point of contact:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the provider:

(*Text*)

SECTION 2: Information regarding the removal order

~~Name of the Coordinating Authority having requested the issuance of the removal order:~~

~~*(Text)*~~

Competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the removal order:

(*Text*)

Reference of the removal order:

(*Text*)

Date and time of receipt of the removal order, including time zone:

(*Text*)

POLITICO

SECTION 3: Measures taken to execute the removal order

To execute the removal order, the provider has taken the following measure (tick the relevant box):

- ☐ Removed the child sexual abuse material
- ☐ Disabled access to the child sexual abuse material in all Member States

Date and time of taking of the measure, including time zone:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX VII

TEMPLATE FOR BLOCKING ORDERS

referred to in Article 17(1) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

BLOCKING ORDER ISSUED IN ACCORDANCE WITH REGULATION (EU) …/… LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE ('THE REGULATION')

SECTION 1: Authorities having ~~requested and~~ issued the blocking order

~~Name of the Coordinating Authority having requested the issuance of the blocking order:~~

~~*(Text)*~~

Name of the competent ~~judicial~~ authority ~~or the independent administrative authority~~ having issued the blocking order:

(Text)

Reference of the blocking order:

(Text)

SECTION 2: Addressee of the blocking order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point:

(*Text*)

POLITICO

SECTION 3: Measures to execute the blocking order, including additional safeguards:

The provider is to take the necessary measures to prevent users in the Union from having access to the known child sexual abuse material indicated by the following URLs:

(*Text*)

The blocking order applies to the following service provided by the provider in the Union:

(*Text*)

When executing the blocking order, the provider is to respect the following limits and/or to provide for the following safeguards, as referred to in Article 16(5) of the Regulation:

(*Text*)

SECTION 4: Reasons, period of application and reporting

The reasons for issuing the blocking order are as follows:

(Sufficiently detailed statement of reasons for issuing the blocking order)

The blocking order applies from … (*date*) to ……. (*date*)

~~The following reporting requirements apply, in accordance with Article 18(6) of the Regulation:~~

~~*(Text)*~~

SECTION 5: Contact details for follow-up

Contact details of the ~~Coordinating Authority~~ **competent authority** having ~~requested the issuance of~~ **issued** the order for feedback on the execution of the blocking order or further clarification, including the communications referred to in Article 17(5)**, (4a) and (5a)** of the Regulation:

(*Text*)

POLITICO

SECTION 6: Information about redress

Competent court before which the blocking order can be challenged, in accordance with Article 18(1) of the Regulation:

(*Text*)

Time periods for challenging the blocking order (days/months starting from):

(*Text*)

References or links to provisions of national law regarding redress:

(*Text*)

Where relevant, additional information regarding redress:

(Text)

A lack of compliance with this blocking order may result in penalties pursuant to Article 35 of the Regulation.

SECTION 7: Date, time and electronic signature:

Date of issuance of the blocking order:

(*Text*)

Time stamp:

(Text)

Electronic signature of the competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the blocking order:

(*Text)*

POLITICO

ANNEX VIII

TEMPLATE FOR INFORMATION ABOUT THE IMPOSSIBILITY TO EXECUTE THE BLOCKING ORDER

referred to in Article 17(4a) and (5) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the blocking order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Point of contact:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the addressee

(*Text*)

SECTION 2: Information regarding the blocking order

~~Name of the Coordinating Authority having requested the issuance of the blocking order:~~

~~*(Text)*~~

Competent ~~judicial~~ authority ~~or independent administrative authority~~ having issued the blocking order

(*Text*)

Reference of the blocking order

(*Text*)

Date and time of receipt of the blocking order, including time zone:

(*Text*)

POLITICO

SECTION 3: Non-execution

The provider cannot execute the blocking order within the mandatory time period for the following reasons (tick the relevant box(es)):

- ☐ **Force majeure or de facto impossibility not attributable to the provider of hosting services, including for objectively justifiable technical or operational reasons**
- ☐ The blocking order contains one or more manifest errors
- ☐ The blocking order does not contain sufficient information

~~Specify the manifest error(s) and/or the further information or clarification necessary, as applicable: (*Text*)~~

Provide further information regarding the reasons for non-execution, specifying the reasons of force majeure or de facto impossibility, the manifest error(s) and/or the further information or clarification necessary, as applicable:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX IX

TEMPLATE FOR INFORMATION ON THE EXECUTION OF THE BLOCKING ORDER

referred to in Article 17(5a) of Regulation (EU) .../…[*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the blocking order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Point of contact:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the provider:

(*Text*)

SECTION 2: Information regarding the blocking order

Competent authority having issued the blocking order:

(*Text*)

Reference of the blocking order:

(*Text*)

Date and time of receipt of the blocking order, including time zone:

(*Text*)

POLITICO

SECTION 3: Measures taken to execute the blocking order

To execute the blocking order, the provider has taken the following measures, indicating in particular whether the provider has prevented access to child sexual abuse material:

(*Text*)

Date and time of taking of the measure, including time zone:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX X

TEMPLATE FOR DELISTING ORDERS

referred to in Article 18b(1) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

DELISTING ORDER ISSUED IN ACCORDANCE WITH REGULATION (EU) …/… LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE ('THE REGULATION')

SECTION 1: Authorities having issued the delisting order

Name of the competent authority having issued the delisting order:

(Text)

Reference of the delisting order:

(Text)

SECTION 1a: Information to the competent authority of the Member State where the provider has its main establishment or where its legal representative resides or is established

Please tick the relevant box(es):

□ **The Member State where the provider has its main establishment or where its legal representative resides or is established is other than the Member State of the issuing competent authority**

□ **A copy of the delisting order is sent to the competent authority of the Member State where the provider has its main establishment or where its legal representative resides or is established**

□ **The delisting order is sent through the competent authority of the Member State where the provider has its main establishment or where its legal representative resides or is established**

POLITICO

SECTION 2: Addressee of the delisting order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Contact point:

(*Text*)

SECTION 3: Measures to execute the delisting order, including additional safeguards:

The provider is to take the necessary measures to prevent the dissemination of known child sexual abuse material in the Union, indicated by the following URLs:

(*Text*)

The delisting order applies to the following service provided by the provider in the Union:

(*Text*)

SECTION 4: Reasons, period of application and reporting

The reasons for issuing the delisting order are as follows:

(*Text*)

The delisting order applies from … (*date*) to ……. (*date*)

The following reporting requirements apply, in accordance with Article 18a(5) of the Regulation:

(*Text*)

SECTION 5: Information about redress

Competent court before which the delisting order can be challenged, in accordance with Article 18c(1) of the Regulation:

(*Text*)

POLITICO

Time periods for challenging the delisting order (days/months starting from):

(*Text*)

References or links to provisions of national law regarding redress:

(*Text*)

Where relevant, additional information regarding redress:

(Text)

SECTION 6~~7~~: Date, time and electronic signature:

Date of issuance of the delisting order:

(*Text*)

Time stamp:

(Text)

Electronic signature of the competent authority having issued the delisting order:

(*Text)*

A lack of compliance with this delisting order may result in penalties pursuant to Article 35 of the Regulation.

POLITICO

ANNEX XI

TEMPLATE FOR INFORMATION ABOUT THE IMPOSSIBILITY TO EXECUTE THE DELISTING ORDER

referred to in Article 18b(4) and (5) of Regulation (EU) .../… [*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the delisting order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Point of contact:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the addressee:

(*Text*)

SECTION 2: Information regarding the delisting order

Competent authority having issued the delisting order:

(*Text*)

Reference of the delisting order:

(*Text*)

Date and time of receipt of the delisting order, including time zone:

(*Text*)

POLITICO

SECTION 3: Non-execution

The provider cannot execute the delisting order within the mandatory time period for the following reasons (tick the relevant box(es)):

- ☐ **Force majeure or de facto impossibility not attributable to the provider, including for objectively justifiable technical or operational reasons**
- ☐ **The delisting order contains one or more manifest errors**
- ☐ **The delisting order does not contain sufficient information**

Provide further information regarding the reasons for non-execution, specifying the reasons of force majeure or de facto impossibility, the manifest error(s) and/or the further information or clarification necessary, as applicable:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX XII

TEMPLATE FOR INFORMATION ON THE EXECUTION OF THE DELISTING ORDER

referred to in Article 18b(6) of Regulation (EU) .../…[*laying down rules to prevent and combat child sexual abuse*]

SECTION 1: Addressee of the delisting order

Name of the provider and, where applicable, of its legal representative:

(*Text*)

Point of contact:

(Text)

Contact details of the provider and, where applicable, of its legal representative:

(*Text*)

File reference of the provider:

(*Text*)

SECTION 2: Information regarding the delisting order

Competent authority having issued the delisting order:

(*Text*)

Reference of the delisting order:

(*Text*)

Date and time of receipt of the delisting order, including time zone:

(*Text*)

POLITICO

SECTION 3: Measures taken to execute the delisting order

To execute the delisting order, the provider has taken the following measures, indicating in praticular whether the provider has prevented search results for the online location with child sexual abuse material to appear:

(*Text*)

Date and time of taking of the measure, including time zone:

(*Text*)

SECTION 4: Date, time and signature

Date and time, including time zone:

(*Text*)

Signature:

(*Text*)

POLITICO

ANNEX XIII

CORRELATION TABLE

Chapters	Articles	Recitals
I	Article 1 (Subject matter and scope)	Recitals 1-12
	Article 2 (Definitions)	Recital 13
II	Article 3 (Risk Assessment)	Recital 14-15
	Article 4 (Risk Mitigation)	Recital 16
	Article 5 (Risk Reporting)	Recitals 17-18
	Article 6 (Obligations for software application stores)	Recitals 19
	Article 7 (Issuance of detection orders)	Recitals 20-22
	Article 8 (Additional rules regarding detection orders)	Recitals 20-22
	Article 9 (Redress, information, reporting and modification of detection orders)	Recital 23
	Article 10 (Technologies and safeguards)	Recitals 24-26
	Article 11 (Guidelines regarding detection obligations)	Recital 27-28
	Article 12 (Reporting obligations)	Recital 29
	Article 13 (Specific requirements of reporting)	Recital 29
	Article 14 (Removal orders)	Recitals 30 - 31
	Article 15 (Redress and provision of information)	Recitals 30, 32
	Article 16 (Blocking orders)	Recitals 33-34
	Article 17 (Additional rules regarding blocking orders)	Recitals 33-34
	Article 18 (Redress, information and reporting blocking orders)	Recital 33
	Article 19 (Liability of providers)	Recital 34
	Articles 20 (Victims' rights to information)	Recital 35
	Article 21 (Victims' rights of assistance and support for removal	Recitals 36-38
	Article 22 (Preservation of information)	Recital 39
	Article 23 (Points of contact)	Recital 40
	Article 24 (Legal Representative)	Recitals 41-42
III	Article 2 (Coordinating Authorities for child sexual abuse issues and other competent authorities)	Recitals 43-45
	Article 26 (Requirements for coordinating authorities)	Recital 46
	Article 27 (Investigatory powers)	Recitals 47-48
	Article 28 (Enforcement powers)	Recitals 47-48
	Article 29 (Additional enforcement powers)	Recitals 47-48
	Article 30 (Common provisions on investigatory and enforcement powers)	Recitals 47-48
	Article 31 (Searches to verify compliance)	Recital 49
	Article 32 (Notification of known child sexual abuse material)	Recital 50
	Article 33 (Jurisdiction)	Recital 51
	Article 34 (Right of users of the service to lodge a complaint)	Recital 52
	Article 35 (Penalties)	Recital 53
	Article 36 (Identification and submission of online child sexual abuse)	Recitals 54-56
	Article 37 (Cross-border cooperation among coordinating authorities)	Recital 57
	Article 38 (Joint investigations)	Recital 57
	Article 39 (General cooperation and information sharing system)	Recital 58

Chapters	Articles	Recitals
IV	Article 40 (Establishment and scope of action of the EU Centre)	Recital 59
	Article 41 (Legal status)	Recital 59
	Article 42 (Seat)	Recital 59
	Article 43 (Tasks of the EU Centre)	Recital 60
	Article 44 (Databases of indicators)	Recital 61
	Article 45 (Database of reports)	Recitals 62-63
	Article 46 (Access, accuracy and security)	Recital 64
	Article 47 (Delegated acts related to the databases)	Recital 64
	Articles 48 (Reporting)	Recital 65
	Article 49 (Searches and notifications)	Recital 66
	Article 50 (Technologies, information and expertise)	Recital 67
	Article 51 (Processing activities and data protection)	Recital 68
	Article 52 (Contact officers)	Recitals 69-72
	Article 53 (Cooperation with Europol)	Recitals 69-72
	Article 54 (Cooperation with partner organisations)	Recitals 69-72
	Article 55 (Administrative and management structure)	Recitals 73
	Article 56 (Composition of the Management Board)	-
	Article 57 (Functions of the Management Board)	-
	Article 58 (Chairperson of the Management Board)	-
	Article 59 (Meetings of the Management Board)	-
	Article 60 (Voting rules of the Management Board)	-
	Article 61 (Composition and appointment of the Executive Board)	-
	Article 62 (Tasks of the Executive Board)	-
	Article 63 (Voting rules of the Executive Board)	-
	Article 64 (Responsibilities of the Executive Director)	-
	Article 65 (Executive Director)	-
	Article 66 (Establishment and tasks of the Technology Committee)	Recital 74
	Article 67 (Budget establishment and implementation)	ANNEX to the Legislative Financial Statement
	Article 68 (Financial rules)	ANNEX to the Legislative Financial Statement
	Article 69 (Budget)	ANNEX to the Legislative Financial Statement
	Article 70 (Presentation of accounts and discharge)	ANNEX to the Legislative Financial Statement
	Article 71 (General Provisions)	ANNEX to the Legislative Financial Statement
	Article 72 (Seconded national experts and other staff)	-
	Article 73 (Privileges and immunities)	-
	Article 74 (Obligation of professional secrecy)	-
	Article 75 (Security rules on the protection of classified and	-

POLITO

Chapters	Articles	Recitals
	sensitive non-classified information	
	Article 76 (Language arrangements)	-
	Article 77 (Transparency and communication)	-
	Article 78 (Anti-fraud measures)	ANNEX to the Legislative Financial Statement
	Article 79 (Liability)	-
	Article 80 (Administrative inquires)	-
	Article 81 (Headquarters agreement and operating conditions)	-
	Article 82 (Start of the EU Centre's activities)	-
V	Article 83 (Data collection)	-
	Article 84 (Transparency reporting)	-
VI	Article 85 (Evaluation)	Recitals 75-77
	Article 86 (Exercise of the delegation)	-
	Article 87 (Committee procedure)	Recitals 79-82
	Article 88 (Repeal)	Recital 88
	Article 89 (Entry into force and application)	Recitals 83-84

POLITICO

ANNEX XIV

METHODOLOGY AND CRITERIA FOR THE RISK CATEGORISATION OF SERVICES

POLITICO

POLITICO

1. Scoring based on the size of the service

A. Services defined as "VLOPs" (= very large online platforms), and services defined as "VLOSEs" (very large online search engines)[42].

a. Definition: Online platforms and online search engines which have several average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines

B. Other services

2. Scoring based on the type of service

Is the service one or more of the following service types?

A. Social media platform (services that connect users and enable them to build communities around common interests or connections)

B. Electronic messaging service *(service that is typically centered around allowing users to send messages that can only be viewed or read by a specific recipient or group of people)*

C. Online gaming service *(services that allow users to interact within partially or fully simulated virtual environments)*

D. Adult service[43] *(services that are primarily used for the dissemination of user-generated adult content)*

a. For instance, adult services could comprise one or more of the following services:
   i. Camming Services: These platforms facilitate the live streaming or webcam performances by individuals typically engaged in adult-oriented activities such as explicit conversations, striptease, or sexual acts for an audience.
   ii. Pornographic Websites: These are platforms that primarily host or distribute sexually explicit videos, images, or other adult content for viewing or downloading.

POLITICO

---

42 Art. 33 and 34 of Regulation (EU) 2022/2065 (Digital Services Act).

43 An "adult service" typically refers to an online platform or service that primarily deals with or facilitates the dissemination of adult content. This content may include, but is not limited to, explicit imagery, videos, or text that is intended for mature audiences and may contain nudity, sexual content, or explicit language. Adult services encompass a wide range of platforms, including adult websites, adult social media networks, adult chat rooms, adult streaming services, and adult dating or hookup platforms. These platforms are designed to cater to individuals seeking adult-oriented content, entertainment, or interactions. Note that adult services may vary in terms of the types of content they offer, the audience they target, and the services they provide. However, they share a common characteristic of providing access to adult-oriented material and often require users to confirm their age before accessing such content.

iii. Adult Gambling Services: These services involve online betting or gambling activities that are explicitly geared towards adults and may include adult-themed games or gambling content.

iv. Escort Services: These services connect individuals with escorts or companions for adult-oriented activities, which may include companionship, intimacy, or sexual services in exchange for payment.

v. Adult Social Networking Sites: These are platforms like mainstream social networking sites but cater specifically to adults interested in connecting with others for adult-oriented interactions, such as dating, casual encounters, or discussions about sexual topics.

vi. Adult Dating Services: These mobile applications focus on facilitating connections between adults interested in casual or intimate relationships, often emphasizing physical attraction and sexual compatibility, typically through profile creation, matching algorithms, and messaging features.

vii. Adult Content Subscription Services: These platforms offer access to exclusive or premium adult content through subscription-based models, providing users with a variety of adult-oriented media such as videos, images, or stories.

E. Discussion forum or chat room service *(services that allow users to send or post messages that can be read by the public or an open group of people)*

F. Marketplace or listing service *(services that allow users to buy and sell their goods or services)*

G. File-storage and file-sharing service *(services whose primary functionalities involve enabling users to store digital content and share access to that content through links)*

H. Web and server hosting services[44] *(services that provide individuals or organisations with the infrastructure and technology needed to host websites or web applications on the internet, including server space, bandwidth, and technical support).*

I. Online search engines[45]

J. Services directly targeting children

K. Other information society services[46]

POLITICO

44 See also article 3 (g), point (iii) of Regulation (EU) 2022/2065.

45 See article 3 (j) of Regulation (EU) 2022/2065.

46 'Information society service' means a 'service' as defined in Article 1(1), point (b), of Directive (EU) 2015/1535.

3. Scoring based on the core architecture of the service.

A. Does the service allow child[47] *users to access a part or the entirety of the service?*

YES/NO

B. User identification

1. Can users display identifying information through a user profile that can be viewed by others (e.g. images, usernames, age)?

   YES/NO

2. Can the platform be used anonymously?

   YES/NO

3. Can users share content anonymously (e.g. anonymous profiles or access without an account)?

   YES/NO

4. Are there functionalities that prevent users from accessing the website(s) in another geographic region where the legislation is less strict?

   YES/NO

5. Does the service require multi-factor authentication and user signup information, where users register for the service using a phone number, email address, or other identifiers?

   YES/NO

C. User connection

1. Can users connect with other users?

   YES/NO

2. Can users form closed groups or send group messages?

   YES/NO

3. Can users search for other users by specific categories (place, gender, hobbies, etc.)?

   YES/NO

POLITICO

[47] Users not having reached the age of adulthood in the country of establishment of the service provider. The assessment of this criteria should consider not just whether children can access the site but whether they do access the site.

D. User communication[48]

1. Can users communicate via livestreaming?

   YES/NO

2. Can users communicate via direct messaging (including ephemeral direct messaging)?

   YES/NO

3. Can users communicate via encrypted messaging (YES/ NO) and are there functionalities to "opt-in/opt-out"? [49]

   YES/NO

4. Can users post or send images or videos (either open or closed channels)?

   YES/NO

5. Can users re-post and forward content (either open or closed channels)?

   YES/NO

6. Can users share content via hyperlinks and plain-text URLs?

   YES/NO[50]

7. Can users comment on content (open and/or closed channels)?

   YES/NO

8. Can users post/share (visible) location information?

   YES/NO

9. Can users search for user-generated content?

   YES/NO

POLITICO

---

48 These criteria have been presented ranked to help for the future scoring system (to be developed). These ranking places activities involving direct real-time communication (livestreaming, messaging) at the highest risk due to their immediate and potentially unfiltered nature. Encrypted messaging follows closely due to privacy concerns and the potential for misuse. Posting and sharing of multimedia content are also high-risk activities, as they can easily disseminate harmful material. Reposting, forwarding, and sharing via hyperlinks carry a moderate risk, while commenting, sharing location information, and searching for user-generated content are deemed lower risk, though they still warrant attention in terms of potential risks.

49 Making design choices such as ensuring that E2EE is opt-in by default, rather than opt-out would require people to choose E2EE should they wish to use it, therefore allowing certain detection technologies to work for communication between users that have not opted in to E2EE.

50 Link to encrypted services is often shared on unencrypted online spaces to facilitate the exchange of CSAM.

E. Does the service allow users to post goods and services for sale?

1. Does the service allow the use of cryptocurrency to buy service/material (promotes anonymity)?

   YES/NO

2. Does the service allow for gift-card-related transactions?

   YES/NO

F. Does the service allow payments through its system?

YES/NO

G. Can users download/save/screenshot/screen video content?

YES/NO

H. Does the service apply recommendation algorithms?[51]

YES/NO

I. In case the service applies recommendation algorithms, can the recommendation algorithms used by the service be modified to limit illegal content?

YES/NO

J. Possibility to limit the number of downloads per user to reduce the distribution of illegal content

- Absent
  - The platform lacks functionalities to limit the number of downloads per user to reduce the dissemination of harmful content.
- Basic
  - The platform has basic functionalities in place to limit the number of downloads per user to reduce the dissemination of harmful content. Their scope and effectiveness are limited.
- Effective
  - The platform has effective functionalities in place to limit the number of downloads per user to reduce the dissemination of harmful content. They significantly reduce the risk of the dissemination of harmful content, contributing to a safer online environment.

[51] Algorithms that recommend content like that already viewed may potentially expose users to inappropriate content if they have already been exposed to child pornography.

POLITICO

- Comprehensive
    - The platform has comprehensive functionalities in place to limit the number of downloads per user to reduce the distribution of harmful content. These robust measures leave minimal to no room for the dissemination of harmful content, thereby ensuring a safe online environment for users.

K. Storage functionalities

- Absent
    - The platforms' storage functionalities and/or the legal framework of the country of storage do not allow sharing information with law enforcement authorities.
- Basic
    - The platforms' storage functionalities and/or the legal framework of the country of storage allow sharing information with law enforcement authorities, but only for a limited amount of information and for a limited amount of time.
- Effective
    - The platforms' storage functionalities and/or the legal framework of the country of storage allow sharing information with law enforcement authorities for a large amount of information and for a long time.
- Comprehensive
    - The platforms' storage functionalities and/or the legal framework of the country of storage allow sharing information with law enforcement authorities for all information and for an indefinite period.

L. Functionalities preventing users from making recordings and screenshots of shared content or saving a local copy of shared content

- Absent
    - The platform lacks functionalities to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof (such as for example not allowing recording and screenshotting content shared by minors).

POLITICO

- Basic
    - The platform has basic functionalities in place to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof, but their scope and effectiveness are limited.
- Effective
    - The platform has effective functionalities in place to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof. These measures significantly reduce the risk of the dissemination of harmful content, contributing to a safer online environment.
- Comprehensive
    - The platform has comprehensive functionalities in place to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof. These robust measures leave minimal to no room for the dissemination of harmful content through saving, thereby ensuring a safe online environment for users.

4. Scoring based on policies and safety by design functionalities in place to address identified risks.

A. Effectiveness of CSA Risk Policies

- Absent
    - The platform lacks explicit policies specifically addressing child sexual abuse risks.
- Basic
    - While the platform has policies related to CSA risks, they are not regularly updated, and users find them unclear.
- Effective
    - Clear policies addressing CSA risks are in place, updated regularly, and users understand them.
- Comprehensive
    - The platform boasts explicit and user-friendly policies on CSA risks, which are not only regularly updated, but also enforced in a manner that users can easily comprehend.

POLITICO

B. Measures for Promoting Users' Media Digital Literacy and Safe Usage Scoring System

- Absent/limited
    - The platform does not offer (or only to a limited extent) educational materials dedicated to promoting media digital literacy (for example, links to educational information). The materials do not contribute to an observable user awareness of CSA risks.
- Basic
    - The platform offers some educational content dedicated to promoting media digital literacy. The materials only contribute to a limited extent to an observable adequate level of user awareness of CSA risks.
- Effective
    - The platform offers a robust set of educational content dedicated to promoting media digital literacy. The materials lead to an observable improvement in user awareness of CSA risks.
- Comprehensive
    - The platform offers a robust set of educational content dedicated to promoting media digital literacy. The materials lead to an observable improvement in user awareness and engagement. The commitment to fostering a deep recognizing of safe media usage is evident.

C. Definition of CSA in Terms of Services

- Absent/limited
    - Terms and conditions related to CSA risks are lacking or unclear, leading to potential misinterpretation by users.
- Basic
    - While terms are clear, the enforcement mechanisms related to CSA risks are weak and may not deter violations effectively.
- Effective
    - The platform has comprehensive terms addressing CSA risks, and enforcement is moderate.
- Comprehensive.
    - Terms are strictly enforced, and the platform is transparent about the consequences for violating CSA-related terms.

POLITICO

D. Functionalities enabling Users to Share Potentially Harmful Content

- Absent/Very Limited
    - Platforms lack adequate functionalities (for example: Hashing/photo DNA) to prevent the sharing of potentially harmful content by users. This absence raises concerns about the platform's ability to mitigate the dissemination of harmful material effectively.
- Limited
    - Platforms have limited functionalities to prevent users from sharing potentially harmful content. While some measures may be in place, they are not comprehensive, leaving room for the dissemination of harmful material.
- Effective
    - Platforms in this category demonstrate effective functionalities to prevent users from sharing potentially harmful content. These measures significantly reduce the risk of harmful material dissemination, contributing to a safer online environment.
- Comprehensive
    - Platforms in this category have comprehensive functionalities in place to prevent users from sharing potentially harmful content. These robust measures leave minimal to no room for the dissemination of harmful material, ensuring a safe online environment for users.

E. Possibility to use peer-to-peer downloading (allows direct sharing of content without using centralised servers)

- Absent
    - Platforms offer comprehensive support for peer-to-peer downloading, allowing seamless and efficient direct sharing of content among users, promoting decentralised distribution, and reducing reliance on central servers for content dissemination.
- Limited
    - Platforms provide effective support for peer-to-peer downloading, enabling users to directly share content without dependence on centralised servers, enhancing efficiency and user autonomy.
- Effective
    - Platforms offer limited support for peer-to-peer downloading, but it may not be widely available or may come with significant limitations, potentially increasing the risk associated with centralised content distribution.

POLITICO

- Comprehensive
    - Platforms lack the option for users to utilise peer-to-peer downloading, restricting direct sharing of content without relying on centralised servers.

F. Functionalities Assessment of Potential Dissemination Risks

- Absent
    - Platforms fail to assess potential dissemination risks associated with shared content adequately. This lack of assessment raises concerns about the platform's ability to proactively identify and mitigate dissemination risks, potentially exposing users to harmful content.
- Limited
    - Platforms conduct partial assessments of potential dissemination risks related to shared content. While efforts are made to evaluate risks, the assessment may not be comprehensive, leading to gaps in identifying and mitigating dissemination risks.
- Effective
    - Platforms conduct effective assessments of potential dissemination risks related to shared content. Through proactive evaluation mechanisms, these platforms identify and mitigate dissemination risks, contributing to a safer content-sharing environment.
- Comprehensive
    - Platforms conduct comprehensive assessments of potential dissemination risks related to shared content. With thorough evaluation processes in place, these platforms effectively identify and mitigate dissemination risks, ensuring a safe content-sharing environment for users.

G. Possibility to delete shared content for all users it has been shared with

- Absent
    - The service provider lacks the ability for children to delete shared content.
- Limited
    - The service provider has a limited functionality for children to delete shared content. Only for a certain period and under certain circumstances, avoiding the proper possibility of children to delete shared content when necessary.
- Effective
    - The service provider has a limited functionality for children to delete shared content. For an extensive period and under relevant circumstances, succeeding in allowing deleting shared content in most of the cases.

POLITICO

- Comprehensive
    - The service provider has an efficient functionality for children to delete shared content when necessary. For an extensive period and under every circumstance, succeeding in allowing deleting shared content in all relevant cases.

H. Systems for selecting and presenting advertisements

- Absent
    - The platform does not propose any safety by design functionalities on advertisement systems, like age-based ad filtering or parental control, allowing potentially harmful content to be shown to children.
- Limited
    - The platform proposes limited safety-by-design functionalities on advertisement systems, but it is not comprehensive enough to effectively prevent harmful content to be shown to children.
- Effective
    - The platform proposes effective safety by design functionalities that reduces the likelihood of harmful content being shown to children.
- Comprehensive
    - The platform provides comprehensive safety by design functionalities on advertisement systems that thoroughly prevent harmful content from being displayed to children.

I. Usage of Premoderation functionalities

- Absent
    - Platforms lack a premoderation system, allowing potentially harmful content to be posted without oversight or moderation.
- Limited
    - Platforms have a limited premoderation system in place, but it is not comprehensive enough to effectively filter out all inappropriate content.
- Effective
    - Platforms utilise an effective premoderation system that significantly reduces the likelihood of inappropriate content being posted, enhancing user safety.
- Comprehensive
    - Platforms have a comprehensive premoderation system in place that thoroughly screens all content before it is posted, minimising the risk of harmful content reaching users.

POLITICO

J. Usage of Delisting Content System

- Absent
    - Platforms lack a delisting content system, making it challenging to remove harmful or inappropriate content once posted.
- Limited
    - Some platforms have a limited delisting content system, but it is not consistently applied or may not effectively remove all inappropriate content.
- Effective
    - Platforms utilise an effective delisting content system that promptly removes harmful or inappropriate content upon identification, reducing its visibility to users.
- Comprehensive
    - Platforms have a comprehensive delisting content system that efficiently identifies and removes harmful or inappropriate content, ensuring a safer online environment for users.

K. Usage of Image Masking

- Absent
    - Platforms lack image masking capabilities, potentially exposing users to sensitive or explicit content without adequate protection.
- Limited
    - Platforms have limited image masking capabilities, but they may not be consistently applied or may not effectively conceal sensitive or explicit content.
- Effective
    - Platforms utilise effective image masking techniques that appropriately conceal sensitive or explicit content, enhancing user privacy and safety.
- Comprehensive
    - Platforms have comprehensive image masking capabilities in place that consistently and effectively conceal sensitive or explicit content, providing robust protection for users.

POLITICO

5. Mapping of user tendencies

A. Assessing User Patterns

- Absent
    - A portion of users demonstrate frequent engagement with content that could pose risks. This includes but is not limited to content that may be inappropriate, harmful, or potentially unsafe. A high frequency of user interaction with such content raises concerns about the overall safety of the platform.
- Limited
    - Platforms falling within this range demonstrate a certain level of user engagement with potentially risky content. While harmful activities are not widespread, occasional instances raise concerns about the need for enhanced moderation and content filtering mechanisms to ensure a safer environment for users.
- Effective
    - Users in this category engage with risky content in a limited manner. Instances of harmful activities are infrequent, suggesting a healthy user environment. However, ongoing monitoring and preventive measures are still essential to maintain this positive trend and further reduce potential risks.
- Comprehensive
    - This represents the most favourable scenario where users rarely engage in activities that pose risks. The platform enjoys an elevated level of user responsibility, and harmful content is a rare occurrence. This indicates a strong community's commitment to maintaining a safe and secure online environment.

B. Service's Popularity Among Different Age Groups

- Absent
    - The platform lacks adequate monitoring and assessment of its popularity among different age groups. There is a lack of data collection and analysis regarding user demographics, particularly related to age groups, raising concerns about the platform's understanding of potential vulnerabilities.
- Limited
    - Platforms have limited data on the popularity among different age groups. While there may be efforts to collect and analyse user demographics, the data may not provide an understanding of potential vulnerabilities associated with age groups.

POLITICO

- Effective
    - Platforms in this category effectively monitor and analyse the service's popularity among different age groups. Through comprehensive data collection and analysis, these platforms gain insights into user demographics, allowing for targeted risk assessment and mitigation strategies.
- Comprehensive
    - Platforms in this category have comprehensive monitoring and analysis of the service's popularity among different age groups. With data collection and analysis mechanisms in place, these platforms possess detailed insights into user demographics, facilitating targeted risk assessment and effective mitigation strategies.

C. Analysis of Grooming Risks Based on User Mapping

- Ineffective
    - Platforms fail to conduct a comprehensive analysis of solicitation risks based on functionalities and user mapping. This lack of assessment raises concerns about the platform's ability to proactively identify and mitigate solicitation risks, potentially exposing users to harmful interactions.
- Limited
    - Platforms conduct a partial analysis of solicitation risks based on functionalities and user mapping. While efforts are made to evaluate risks, the analysis may not be comprehensive, leading to gaps in identifying and mitigating solicitation risks.
- Effective
    - Platforms conduct an effective analysis of solicitation risks based on functionalities and user mapping. Through proactive evaluation mechanisms, these platforms identify and mitigate solicitation risks, contributing to a safer online environment.
- Comprehensive
    - Platforms conduct a comprehensive analysis of solicitation risks based on functionalities and user mapping. With thorough evaluation processes in place, these platforms effectively identify and mitigate solicitation risks, ensuring a safe online environment for users.

POLITICO

D. Analysis of tendencies based on account's information:

Use of Anonymous Account:

- **Frequent use of anonymous accounts**
  - Less than 25% of accounts have identifiable information.
- **Moderate instance of anonymous accounts.**
  - 25 to 60% of accounts have identifiable information.
- **Minimal or no use of anonymous accounts**
  - More than 60% of accounts have identifiable information

Multiple accounts under different names

- **Frequent use of multiple accounts under different names**
  - More than 60% of accounts are linked to 2 or more accounts of the same person
- **Moderate use of multiple accounts under different names**
  - 25% to 60% of accounts are linked to 2 or more accounts of the same person
- **Minimal or no use of multiple accounts under different names**
  - Less than 25% of accounts are linked to 2 or more accounts of the same person

Consecutive and Repetitive De- and Re-Activation of Accounts

- **Frequent de- and re-activation patterns observed.**
  - More than 60 % of accounts undergo repetitive activation and deactivation.
- **Moderate instances of de- and re-activation**
  - 25 to 60 % of accounts undergo repetitive activation and deactivation.
- **Minimal or no repetitive de- and re-activation**
  - Less than 25% of accounts undergo repetitive activation and deactivation.

POLITICO

Fake or Imposter Accounts

- **Frequent fake or imposter accounts identified.**
  - Less than 25% are genuine accounts.
- **Moderate instances of fake or imposter accounts**
  - 25 to 60% are genuine accounts.
- **Minimal or no fake or imposter accounts**
  - More than 60 % are genuine accounts.

Identity Verification Tools for Opening Accounts

- **Lack of identity verification tools**
  - More than 60% of accounts can be created without verifying identity.
- **Moderate identity verification measures**
  - 25 to 60% of accounts can be created without verifying identity.
- **Comprehensive identity verification tools**
  - Less than 25% of accounts can be created without verifying identity.

Pseudonymity

- **Frequent Pseudonymous behavior**
  - More than 60% of users use aliases or pseudonyms.
- **Moderate instances of pseudonymity**
  - 25 to 60% of users use aliases or pseudonyms.
- **Minimal or no pseudonymous behavior:**
  - Less than 25% of users use aliases or pseudonyms.

Temporary Accounts

- **Frequent creation of temporary accounts:**
  - More than 60% of accounts are created for short-term use.
- **Moderate instances of temporary account:**
  - 25 to 60% of accounts are created for short-term use.
- **Minimal or no temporary account creation:**
  - Less than 25% of accounts are created for short-term use.

POLITICO

Frequent Changing of Account(s) or Profile Details:

- **High frequency of changing accounts or profile details:**
  - More than 60% of users update account(s) information/ details at least every 7 days.
- **Moderate instances of changes:**
  - 25 to 60% of users update account(s) information/ details at least every 7 days.
- **Minimal instances or no changes of accounts:**
  - Less than 25% of users update account(s) information/ details at least every 7 days.

Unmatching or Defriending Victims on Social Media Accounts

- **Frequent unmatching or defriending of victims observed:**
  - More than 60% of users maintain consistent social connections.
- **moderate instances of unmatching or defriending:**
  - 25 to 60 % of users maintain consistent social connections.
- **Minimal or no unmatching or defriending:**
  - Less than 25% of users maintain consistent social connections.

Switching Between Private and Public Platforms

- **Frequent switching between private and public platforms:**
  - More than 60% of accounts switch between private and public settings.
- **Moderate instances of platform switching:**
  - 25 to 60 % of accounts switch between private and public settings.
- **Stable behavior with minimal platform changes:**
  - Less than 25% of accounts switch between private and public settings.

POLITICO

Moving Public Conversations to Private Channels

- **Frequent movement from public to private channels:**
  - More than 60% of users often transition discussions from public to private spaces.
- **Moderate instances of conversation shifts:**
  - *25 to 60 % of* users often transition discussions from public to private spaces.
- **Minimal or no movement to private channels:**
  - Less than 25% of users often transition discussions from public to private spaces.

Obfuscation of I.P. Addresses

- **Frequent use of VPN or proxy servers to mask IP addresses:**
  - More than 60 % of users employ VPNs or proxies and don't typically use their real IP addresses.
- **Moderate instances of IP address obfuscation:**
  - 25 to 60% of users employ VPNs or proxies and don't typically use their real IP addresses.
- **Minimal or no obfuscation of IP addresses:**
  - Less than 25% of users employ VPNs or proxies and don't typically use their real IP addresses.

Use of Unsecure Public WIFI Hotspots

- **Frequent use of unsecure public WIFI hotspots:**
  - More than 60% of users connect from unsecured public networks.
- **Moderate instances of connecting to unsecure WIFI:**
  - 25 - 60 % of users connect from unsecured public networks.
- **Minimal or no use of unsecure public WIFI:**
  - Less than 25% of users connect from unsecured public networks.

POLITICO

Creation of Private Group or Chatboxes

- **Frequent creation of private groups or chatboxes:**
  - More than 60% of users create private communication spaces and groups.
- **Moderate instances of creating private spaces or chatboxes:**
  - 25 to 60 % of users create private groups for communication.
- **Minimal or no creation of private groups or chatboxes:**
  - 25% of users predominantly engage in public communication.

"Cyber Flashing" (Unsolicited Intimate Messages)

- **Frequent incidents of cyber flashing:**
  - More than 60% of users report to be victim of unsolicited intimate messages.
- **Moderate instances of unsolicited intimate messages:**
  - 25 to 60% of users report to be victim of unsolicited intimate messages.
- **Minimal or no incidents of cyber flashing:**
  - Less than 25% of users report to be victim of unsolicited intimate messages.

POLITICO