EUROPEAN
COMMISSION

Brussels, XXX
COM(2022) 209/2

2022/0155 (COD)
SENSITIVE[*]
UNTIL ADOPTION

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)

{SEC(2022) 209} - {SWD(2022) 209-210}

[*] Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions https://europa.eu/!db43PX

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The United Nations Convention on the Rights of the Child (UNCRC) and Article 24(2) of the Charter of Fundamental Rights of the European Union ('the Charter')[1] enshrine as rights the protection and care of children's best interests and well-being. In 2021, the United Nations Committee on the Rights of the Child underlined that these rights must be equally protected in the digital environment[2]. The protection of children, both offline and online, is a Union priority.

At least one in five children falls victim to sexual violence during childhood[3]. A 2021 global study found that more than one in three respondents had been asked to do something sexually explicit online during their childhood, and over half had experienced a form of child sexual abuse online[4]. Children with disabilities face an even higher risk of experiencing sexual violence: up to 68% of girls and 30% of boys with intellectual or developmental disabilities will be sexually abused before their 18th birthday[5]. Child sexual abuse material is a product of the physical sexual abuse of children. Its detection and reporting is necessary to prevent its production and dissemination, and a vital means to identify and assist its victims. The pandemic has exposed children to a significantly higher degree of unwanted approaches online, including solicitation into child sexual abuse. Despite the fact that the sexual abuse and sexual exploitation of children and child sexual abuse materials are criminalised across the EU by the Child Sexual Abuse Directive[6], adopted in 2011, it is clear that the EU is currently still failing to protect children from falling victim to child sexual abuse, and that the online dimension represents a particular challenge.

Therefore, on 24 July 2020, the European Commission adopted the EU Strategy for a More Effective Fight Against Child Sexual Abuse,[7] which sets out a comprehensive response to the growing threat of child sexual abuse both offline and online, by improving prevention, investigation, and assistance to victims. It includes eight initiatives to put in place a strong legal framework for the protection of children and facilitate a coordinated approach across the many actors involved in protecting and supporting children. These initiatives aim to identify legislative gaps and ensure that EU laws enable an effective response, strengthen law enforcement efforts at national and EU level, enable EU countries to better protect children through prevention, galvanise industry efforts to ensure the protection of children when using

---

1 UN Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26 October 2012.

2 UN General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment.

3 One in Five Campaign, Council of Europe, 2010-2015.

4 Economist Impact survey of more than 5,000 18-20 year olds in 54 countries, published in the Global Threat Assessment, WeProtect Global Alliance, 2021.

5 UN Special Representative of the Secretary-General on Violence Against Children, Children with Disabilities.

6 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.

7 EU strategy for a more effective fight against child sexual abuse, COM(2020) 607, 24 July 2020, p. 2.

the services they offer, and improve protection of children globally through multi-stakeholder cooperation. This dedicated strategy is flanked by other complementary efforts. On 24 March 2021, the European Commission adopted its comprehensive EU Strategy on the Rights of the Child, which proposes reinforced measures to protect children against all forms of violence, including online abuse. In addition, it invites companies to continue their efforts to detect, report and remove illegal online content, including online child sexual abuse, from their platforms and services. The proposed European Declaration on Digital Rights and Principles for the Digital Decade[8] also includes a commitment to protect all children against illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes.[9]

In this context, providers of hosting or interpersonal communication services ('providers') play a particularly important role. Their responsible and diligent behaviour is essential for a safe, predictable and trusted online environment and for the exercise of fundamental rights guaranteed in the Charter. The circulation of images and videos of child sexual abuse, which has increased dramatically with the development of the digital world, perpetuates the harm experienced by victims, while offenders have also found new avenues through these services to access and exploit children.

Certain providers already voluntarily use technologies to detect, report and remove online child sexual abuse on their services. Yet the measures taken by providers vary widely, with the vast majority of reports coming from a handful of providers, and a significant number take no action. The quality and relevance of reports received by EU law enforcement authorities from providers also varies considerably. Still, organisations such as the National Centre for Missing and Exploited Children ('NCMEC') to whom US providers are obliged to report under US law when they become aware of child sexual abuse on their services, received over 21 million reports in 2020, of which over 1 million related to EU Member States. The most recent reporting figure for 2021 shows a further increase, approaching the 30 million mark[10].

Despite the important contribution made by certain providers, voluntary action has thus proven insufficient to address the misuse of online services for the purposes of child sexual abuse. As a consequence, several Member States have started preparing and adopting national rules to fight against online child sexual abuse. As the Impact Assessment Report accompanying this proposal demonstrates, this results in the development of divergent national requirements, in turn leading to an increase in the fragmentation of the Digital Single Market for services[11]. Against this background, uniform Union rules on the detection, reporting and removal of online child sexual abuse are necessary to complement the Digital Services Act, remove existing barriers to the Digital Single Market and prevent their

---

8 Proposed European Declaration on Digital Rights and Principles for the Digital Decade. COM(2022) 28, 26 January 2022.

9 EU strategy on the rights of the child, COM(2021) 142, 24 March 2021.

10 The 2021 reporting figure of approximately 29.4 million represents a 35% year-on-year increase, EU Cybertipline data snapshot NCMEC, accessed 11 March 2022.

11 Illustrated by the setting up of diverse new or existing authorities responsible for monitoring and enforcing different obligations applicable to varying service provider types as constrained by the national laws of the Member States. See section 3 of Annex 5 of the Impact Assessment Report accompanying this proposal for further detail.

proliferation.[12] Addressing the risk of fragmentation through this proposal must take account of the need to guarantee children's fundamental rights to care and to protection of their well-being, mental health and best interest, and support the general public interest to effectively prevent, investigate and prosecute the perpetration of the serious crime of child sexual abuse.

To address these challenges and in response to calls by the Council and the European Parliament, this proposal therefore seeks to establish a clear and harmonised legal framework on preventing and combating online child sexual abuse. It seeks to provide legal certainty to providers as to their responsibilities to assess and mitigate risks and, where necessary, to detect, report and remove such abuse on their services in a manner consistent with the fundamental rights laid down in the Charter and as general principles of EU law. In combating child sexual abuse as it manifests itself online, there are important rights and interests at stake on all sides. It is therefore particularly important to establish a fair balance between measures to protect child victims of sexual abuse and their fundamental rights and thus to achieve important objectives of general societal interest, and the fundamental rights of other users and of the providers.

This proposal therefore sets out targeted measures that are proportionate to the risk of misuse of a given service for online child sexual abuse and are subject to robust conditions and safeguards. It also seeks to ensure that providers can meet their responsibilities, by establishing a European Centre to prevent and counter child sexual abuse ('the EU Centre') to facilitate and support implementation of this Regulation and thus help remove obstacles to the internal market, especially in connection to the obligations of providers under this Regulation to detect online child sexual abuse, report it and remove child sexual abuse material. In particular, the EU Centre will create, maintain and operate databases of indicators of online child sexual abuse that providers will be required to use to comply with the detection obligations. These databases should therefore be ready before the Regulation enters into application. To ensure that, the Commission has already made funding available to Member States to help with the preparations of these databases. The EU Centre should also carry out certain complementary tasks, such as assisting competent national authorities in the performance of their tasks under this Regulation and providing support to victims in connection to the providers' obligations. It should also use its central position to facilitate cooperation and the exchange of information and expertise, including for the purposes of evidence-based policy-making and prevention. Prevention is a priority in the Commission's efforts to fight against child sexual abuse.

- **Consistency with existing policy provisions in the policy area**

This proposal delivers on commitments made in the EU Strategy for a More Effective Fight Against Child Sexual Abuse, notably to propose legislation to tackle child sexual abuse online effectively, including by requiring providers to detect known child sexual abuse materials, and to work towards the creation of a European Centre to prevent and counter child sexual abuse. The current EU legal framework in this area consists of Union legislation relating to child sexual abuse, such as the Child Sexual Abuse Directive, and Regulation (EU)

[12] See section 4, *Fragmentation of rules for digital services*, in Business Journeys on the Single Market: Practical Obstacles and Barriers, SWD(2020)54, 10 March 2020.

2021/1232 on combating online child sexual abuse[13], which applies until 3 August 2024 ('the interim Regulation').

By introducing an obligation for providers to detect, report, block and remove child sexual abuse material from their services, the proposal enables improved detection, investigation and prosecution of offences under the Child Sexual Abuse Directive. The proposed legislation complements the new European Strategy for a Better Internet for Children[14], which aims to create safe digital experiences for children and to promote digital empowerment.

The EU Centre should work closely with Europol. It will receive the reports from providers, check them to avoid reporting obviously false positives and forward them to Europol as well as to national law enforcement authorities. A representative from Europol will be part of the management board of the EU Centre. In turn, a representative from the EU Centre could be part of the management board of Europol, to further ensure effective cooperation and coordination.

The proposed legislation also contributes to the achievement of the objectives set in several international law instruments. Relevant in this respect are the Council of Europe's Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[15], ratified by all EU Member States, which establishes minimum requirements regarding substantive criminal law, assistance to victims, and intervention programmes, and the Council of Europe's Budapest Convention on Cybercrime[16], ratified by almost all EU Member States, which requires parties to establish certain criminal offences relating to child sexual abuse material.

- **Consistency with other Union policies**

The proposal builds on the General Data Protection Regulation[17] (GDPR). In practice, providers tend to invoke various grounds for processing provided for in the GDPR to carry out the processing of personal data inherent in voluntary detection and reporting of child sexual abuse online. The proposal sets out a system of targeted detection orders and specifies the conditions for detection, providing greater legal certainty for those activities. As regards the mandatory detection activities involving processing of personal data, the proposal, in particular the detection orders issued on the basis thereof, thus establishes the ground for such processing referred to in Article 6(1)(c) GDPR, which provides for the processing of personal data that is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject.

---

13 Regulation 2021/1232/EU 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 (Text with EEA relevance).

14 COM(2022) 212, 11 May 2022.

15 Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, 25 October 2997.

16 Council of Europe Convention on Cybercrime, ETS No. 185, 23 November 2001.

17 Regulation (EU) 2016/679 of the *European* Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The proposal covers inter alia providers that offer interpersonal electronic communications services and hence are subject to national provisions implementing the ePrivacy Directive[18] and its proposed revision currently in negotiations[19]. The measures set out in the proposal restrict in some respects the scope of the rights and obligations under the relevant provisions of that Directive, namely, in relation to activities that are strictly necessary to execute detection orders. In this regard, the proposal involves the application, by analogy, of Article 15(1) of that Directive.

The proposal is also coherent with the e-Commerce Directive and the Proposal for a Digital Services Act (DSA)[20], on which provisional political agreement between the co-legislators has recently been reached[21]. In particular, the proposal lays down specific requirements for the combating of particular forms of illegal activities conducted and illegal online exchanged online, coupled with a set of safeguards. In that manner, it will complement the general framework provided for by the DSA, once adopted. The proposal builds on the horizontal framework of the DSA relying on it as a baseline where possible and setting out more specific rules where needed for the particular case of combating online child sexual abuse. For example, some providers may be subject to a more general obligation to assess systemic risks related to the use of their services under the DSA, and a complementary obligation to perform a specific assessment of risks of child sexual abuse online in the present proposal. Those providers can build on the more general risk assessment in performing the more specific one, and in turn, specific risks identified for children on their services pursuant to the specific risk assessment under the present proposal can inform more general mitigating measures that also serve to address obligations under the DSA.

The e-Commerce Directive and the DSA prohibit Member States from imposing on providers of intermediary services general obligations to monitor or to actively seek facts or circumstances indicating illegal activity. Whilst the precise contours of that prohibition addressed to Member States are only gradually becoming clear, the proposed Regulation aims to comply with the underlying requirement of fairly balancing the various conflicting fundamental rights at stake that underlies that prohibition, taking into account the specific context of combating online child sexual abuse and the importance of the public interest at stake. It does so, in particular, by targeting the scope of the obligations imposed on providers at risk and by setting out a set of clear and carefully balanced rules and safeguards, including through a clear definition of the objectives pursued, the type of material and activities concerned, a risk-based approach, the scope and nature of the relevant obligations, rules on redress and relevant supervision and transparency mechanisms. It also includes strong measures to facilitate and support implementation and hence reduce the burden on service providers.

---

18 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.

19 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).

20 Proposal for a regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final, 15 December 2020.

21 https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2545

In delivering on its main objectives, the proposal also helps victims. As such, the proposed Regulation is in coherence with the Victims' Rights Directive as a horizontal instrument to improve victims' access to their rights[22].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis to support action in this area is Article 114 of the Treaty on the Functioning of the European Union (TFEU). The article provides for the establishment of measures to ensure the functioning of the Internal Market. Article 114 is the appropriate legal basis for a Regulation that seeks to harmonise the requirements imposed on providers of relevant online services in the Digital Single Market. As mentioned above, barriers to the Digital Single Market for Services have started to emerge following the introduction by some Member States of diverging national rules to prevent and combat online child sexual abuse.

The proposed Regulation seeks to eliminate those existing divergences and prevents the emergence of future obstacles which would result from the further development of such national rules. Given the intrinsic cross-border nature of the provision of online services, lack of EU action leaving space for a regulatory framework fragmented along national lines would result in a burden for providers having to comply with diverging sets of national rules and it would create unequal conditions for providers across the EU, as well as possible loopholes.

• Subsidiarity

According to the principle of subsidiarity, EU action may only be taken if the envisaged aims cannot be achieved by Member States alone, but can be better achieved at Union level.

The aim of ensuring a level playing field for providers across the Digital Single Market while taking measures to prevent and combat online child sexual abuse cannot be achieved by the Member States alone. As mentioned, Member States have started imposing requirements on providers to tackle online child sexual abuse. Even those Member States who have not yet introduced such requirements are increasingly considering national measures to that effect. However, the providers covered typically operate across borders, often on an EU-wide basis, or may wish to do so. Accordingly, national requirements imposed on such market players to address online child sexual abuse increase fragmentation in the Digital Single Market and entail significant compliance costs for providers, while being insufficiently effective by virtue of the cross-border nature of the services concerned.

Only EU level action can achieve the aim of eliminating barriers to the Digital Single Market for the services concerned, enhancing legal certainty for providers and reducing compliance costs, while at the same time ensuring that the requirements imposed on market players to tackle online child sexual abuse are effective by virtue of their uniform applicability across

[22] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

borders within the entire EU. Therefore, EU action is necessary to achieve the objectives of the proposed Regulation and it presents a significant added value compared to national action.

- **Proportionality**

This proposal aims at eliminating existing barriers to the provision of relevant services within the Digital Single Market and preventing the emergence of additional barriers, while allowing for an effective fight against online child sexual abuse in full respect of the fundamental rights under EU law of all parties affected. To achieve this objective, the proposal introduces narrowly targeted and uniform obligations of risk assessment and mitigation, complemented where necessary by orders for detection, reporting and removal of child sexual abuse content. These obligations are applicable to relevant providers offering services on the Digital Single Market regardless of where they have their principal establishment.

The proposed rules only apply to providers of certain types of online services which have proven to be vulnerable to misuse for the purpose of dissemination of child sexual abuse material or solicitation of children (known as 'grooming'), principally by reason of their technical features or of the age composition of their typical user base. The scope of the obligations is limited to what is strictly necessary to attain the objectives set out above. The obligations are accompanied by measures to minimise the burden imposed on such providers, as well as the introduction of a series of safeguards to minimise the interference with fundamental rights, most notably the right to privacy of users of the services.

To reduce the number of false positives and prevent erroneous reporting to law enforcement authorities, and to minimise the administrative and financial burden imposed on providers, among other reasons, the proposal creates the EU Centre as an essential facilitator of implementation of the obligations imposed on the providers. Among other tasks, the EU Centre should facilitate access to reliable detection technologies to providers; make available indicators created based on online child sexual abuse as verified by courts or independent administrative authorities of Member States for the purpose of detection; provide certain assistance, upon request, in connection to the performance of risk assessments; and provide support in communicating with relevant national authorities.

Finally, the proposed Regulation contains safeguards to ensure that technologies used for the purposes of detection, reporting and removal of online child sexual abuse to comply with a detection order are the least privacy-intrusive and are in accordance with the state of the art in the industry; they perform any necessary review on an anonymous basis and only take steps to identify any user in case potential online child sexual abuse is detected. It guarantees the fundamental right to an effective remedy in all phases of the relevant activities, from detection to removal, and it limits the preservation of removed material and related data to what is strictly necessary for certain specified purposes. Thereby, the proposed Regulation limits the interference with the right to personal data protection of users and their right to confidentiality of communications, to what is strictly necessary for the purpose of ensuring the achievement of its objectives, that is, laying down harmonised rules for effectively preventing and combating online child sexual abuse in the internal market.

- **Choice of the instrument**

Article 114 TFEU gives the Union's legislator the possibility to adopt Regulations and Directives. As the proposal aims at introducing uniform obligations on providers, which usually offer their services in more than one Member State or may wish to do so, a directive leaving a margin for divergent national transposition of EU rules would not be suitable to achieve the relevant objectives. Divergent national rules transposing the requirements imposed on providers by this instrument would lead to the continuation or reintroduction of those barriers to the Digital Single Market for services that this initiative aims at eliminating.

Unlike a Directive, a Regulation ensured that the same obligations are imposed in a uniform manner across the EU. A Regulation is also directly applicable, provides clarity and greater legal certainty and avoids divergent transposition in the Member States. For these reasons, the appropriate instrument to be used to achieve the objectives of this initiative is a Regulation. In addition, in view of the date of expiry of the interim Regulation, there would in this case be insufficient time to adopt a Directive and then transpose its rules at national level.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

The Commission consulted relevant stakeholders over the course of two years to identify problems and ways forward in the fight against child sexual abuse, both online and offline. This was done through surveys, ranging from open public consultations to targeted surveys of law enforcement authorities. Multiple group expert meetings and bilateral meetings were organised between the Commission and relevant stakeholders to discuss the potential impacts of legislation in this area, and the Commission participated in relevant workshops, conferences and events on the rights of the child.

The Commission published an Inception Impact Assessment in December 2020 with the aim of informing citizens and stakeholders about the planned initiative and seeking initial feedback. This feedback showed significant support for the objective of tackling online child sexual abuse. While the holistic approach of the potential Centre and expected improvements regarding legal clarity were welcomed, some industry stakeholders expressed concerns regarding the impact of mandatory detection and reporting of online child sexual abuse.

The Commission conducted an open public consultation in 2021. This process sought to gather the views from across a broad range of stakeholders such as public authorities and private citizens, industry and civil society. Despite efforts to ensure a balanced distribution of responses, a significant proportion of contributions were received from private individuals in Germany solely addressing questions relating to the subject of encryption. That apart, issues of better cooperation and coordination, and sufficient resourcing and expertise to meet continually increasing volumes of illegal content featured prominently across public authorities, industry and civil society contributions. There was also widespread support across all groups for swift takedown of reported child sexual abuse material, for action to reduce online 'grooming' (solicitation of children) and for improvements to prevention efforts and assistance to victims.

Regarding the possible imposition of legal obligations on providers to detect and report various types of online child sexual abuse in their services, the consultation revealed strong support from law enforcement authorities and organisations working in the area of children's rights, while privacy rights advocates and submissions from private individuals were largely opposed to obligations.

- **Collection and use of expertise**

Targeted surveys of law enforcement authorities in the Member States revealed that reports made by US providers currently constitute one of the most important sources of reports of child sexual abuse. However the quality and relevance of such reports is variable, and some reports are found not to constitute child sexual abuse material under the applicable national law.

These surveys also identified the elements necessary to ensure that a report is 'actionable', i.e., that it is of sufficient quality and relevance that the relevant law enforcement authority can take action. It is for this reason that harmonised reports at an EU level, to be coordinated and facilitated by the actions of the EU Centre, would be the best strategy to maximise the use of expertise to counter online child sexual abuse.

- **Impact assessment**

Following a previous first negative opinion of the Regulatory Scrutiny Board on the Impact Assessment, in February 2022, the Regulatory Scrutiny Board issued a positive opinion on the Impact Assessment with reservations and made various suggestions for improvement. The Impact Assessment report was further revised taking into account the relevant feedback, notably by clarifying the descriptions of the measures taken to ensure compatibility with fundamental rights and with the prohibition of general monitoring obligations and by providing more detailed descriptions of the policy options. The finalised Impact Assessment report examines and compares several policy alternatives in relation to online child sexual abuse and to the possible creation of an EU Centre to prevent and combat child sexual abuse.

The Impact Assessment shows that voluntary actions alone against online child sexual abuse have proven insufficient, by virtue of their adoption by a small number providers only, of the considerable challenges encountered in the context of private-public cooperation in this field, as well as of the difficulties faced by Member States in preventing the phenomenon and guaranteeing an adequate level of assistance to victims. This situation has led to the adoption of divergent sets of measures to fight online child sexual abuse in different Member States. In the absence of Union action, legal fragmentation can be expected to develop further as Member States introduce additional measures to address the problem at national level, creating barriers to cross-border service provision on the Digital Single Market.

Given the need to address the situation and with a view to ensuring the good functioning of the Digital Single Market for services while, at the same time, improving the mechanisms for prevention, detection, reporting and removal of online child sexual abuse and ensuring adequate protection and support for victims, EU level action was found to be necessary.

Five main policy options were considered besides the baseline scenario, with increasing levels of effectiveness in addressing the objectives set out in the impact assessment and the overall policy goal of ensuring the good functioning of the Digital Single Market for services while ensuring that online child sexual abuse is detected, reported and removed throughout the Union, thereby indirectly improving prevention, facilitating investigations and guaranteeing adequate assistance to victims.

All options focused on the objective of ensuring detection, removal and reporting of previously-known and new child sexual abuse material and grooming (material scope) by relevant online service providers (personal scope) established in the EU and in third countries - insofar as they offer their services in the Union (geographical scope).

The main differences between the five options relate to the scope of the obligations on providers and the role and form of the EU Centre. Option A would consist of non-legislative, practical measures to enhance prevention, detection and reporting of online child sexual abuse, and assistance to victims. These include practical measures to increase the implementation and efficiency of voluntary measures by providers to detect and report abuse, and the creation of a European Centre on prevention and assistance to victims in the form of a coordination hub managed by the Commission.

Option B would establish an explicit legal basis for voluntary detection of online child sexual abuse, followed by mandatory reporting and removal. In the context of Option B, the EU Centre would have been tasked with facilitating detection, reporting and removal and would have become a fundamental component of the legislation, serving as a key safeguard for service providers as well as a control mechanism to help ensuring the effective implementation of the proposal. After examining several options concerning the form that the EU Centre could take, the Impact Assessment reached the conclusion that the need for independence, own resources, visibility, staff and expertise needed to perform the relevant functions would be best met by setting up the EU Centre as an EU decentralised agency. This conclusion was confirmed and strengthened in relation to Options C to E, which adopt an incremental approach, building on one another.

Options C and D, while building on Option B, would impose legal obligations on providers to detect certain types of online child sexual abuse on their services. Option C would require providers to detect known child sexual abuse material (CSAM), namely copies of material that has previously been reliably verified as constituting CSAM. Option D would require providers to detect not only 'known' CSAM (material confirmed to constitute child sexual abuse material), but also 'new' CSAM (material that potentially constitutes child sexual abuse material, but not (yet) confirmed as such by an authority).

The retained Option (Option E) builds on Option D, and requires providers to also detect grooming, in addition to known and new CSAM.

The Impact Assessment concluded that Option E is the preferred option for several reasons. Obligations to detect online child sexual abuse are preferable to dependence on voluntary actions by providers (Options A and B), not only because those actions to date have proven insufficient to effectively fight against online child sexual abuse, but also because only uniform requirements imposed at Union level are suitable to achieve the objective of avoiding

the fragmentation of the Digital Single Market for services. Hence, Options A and B were discarded.

The level of the impact on the good functioning of the Digital Single Market for services and on the fight against online child sexual abuse increases progressively in line with the increasing obligations that would be imposed under each option. While an obligation to detect known CSAM (Option C) would help to reduce the recirculation of known material, such an obligation would have only a limited impact in terms of the goal of preventing abuse and providing assistance to victims of ongoing abuses, given that the material falling within the scope of such an obligation might have been in circulation for years. An obligation to detect both known and new CSAM (Option D) would allow for the identification and rescue of victims from ongoing abuse and it would do so based on uniform criteria established at EU level, thereby preventing the adoption of divergent national measures on this point. Mandatory detection also of grooming (Option E) would go further, and provide the greatest scope for preventing imminent abuse and guaranteeing a level playing field on the Digital Single Market for services.

Option E was therefore deemed to be the option which best achieves the policy objective in an effective and proportionate way, all the while ensuring proportionality through the introduction of rigorous limits and safeguards so as to ensure, in particular, the required fair balance of fundamental rights. In addition to the positive social impacts described above, the preferred option is expected to have an economic impact on the affected providers as a result of costs arising from compliance with their obligations, as well as on law enforcement authorities and other competent national authorities as a result of the increased volume of reports of potential online child sexual abuse. These are reduced as much as possible through the provision of certain support by the EU Centre.

In turn, the establishment of the Centre is also expected to incur one-off and ongoing costs. Quantitative estimates of the benefits and costs of each of the policy options were assessed in the Impact Assessment for the purposes of comparing them. The preferred option was found to lead to the greatest overall benefits, by virtue of the resulting improvement in the functioning of the Digital Single Market and reduction of the societal costs linked to online child sexual abuse.

To allow the EU Centre to achieve all of its objectives, it is of key importance that the EU Centre is established at the same location as its closest partner, Europol. The cooperation between the EU Centre and Europol will benefit from sharing location, ranging from improved data exchange possibilities to greater opportunities to create a knowledge hub on combatting CSAM by attracting specialised staff and/or external experts. This staff will also have more career opportunities without the need to change location. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol (HR, IT including cybersecurity, building, communication). Sharing such support services is more cost efficient and ensures a more professional service than duplicating them by creating them from scratch for a relatively small entity as the EU Centre will be.

The impact assessment analysed in detail the relevant impacts, i.e. social, economic and fundamental rights. It also considered the impact on competitiveness and SMEs. The Regulation incorporates some of the measures indicated in the impact assessment in relation to SMEs. These include notably the need for the competent national authorities to take into

account the size and financial and technological capabilities of the provider when enforcing the Regulation, including in relation to the risk assessment, detection obligations and penalties, as well as the possibility for SMEs to request free support from the EU Centre to conduct the risk assessment.

The impact assessment also considered the consistency with climate law, the 'do no significant harm' principle and the 'digital-by-default' principle. The impact assessment also analysed the application of the principle 'one in, one out' whereby each legislative proposal creating new burdens should relieve people and businesses of an equivalent existing burden at EU level in the same policy area, as well as the impacts in relation to the UN Sustainable Development Goals, where SDG 5.2 (eliminate all forms of violence against women girls) and SDG 16.2 (end abuse, exploitation, trafficking and all forms of violence against children) are particularly relevant for this Regulation.

- **Fundamental rights**

According to Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The proposal aims to harmonise the rules that apply to prevent and combat child sexual abuse, which is a particularly serious crime[23]. As such, the proposal pursues an objective of general interest within the meaning of Article 52(1) of the Charter[24]. In addition, the proposal seeks to protect the rights of others, namely of children. It concerns in particular their fundamental rights to human dignity and to the integrity of the person, the prohibition of inhuman or degrading treatment, as well as the rights of the child[25]. The proposal takes into account the fact that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. Furthermore, the types of child sexual abuse at issue here – notably, the exchange of photos or videos depicting such abuse – can also affect the children's rights to respect for private and family life and to protection of personal data[26]. In connection to combating criminal offences against minors, the Court of Justice of the EU has noted that at least some of the fundamental rights mentioned can give rise to positive obligations of the relevant public authorities, including the EU legislature, requiring them to adopt legal measures to protect the rights in question[27].

At the same time, the measures contained in the proposal affect, in the first place, the exercise of the **fundamental rights of the users** of the services at issue. Those rights include, in particular, the fundamental rights to respect for privacy (including confidentiality of communications, as part of the broader right to respect for private and family life), to

---

23 CSAM is also the only type of illegal content whose mere possession is illegal.

24 Cf. e.g. CJEU, *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12, Joined Cases C-511/18, C-512/18 and C-520/18, para. 42.

25 Art. 1, 3, 4 and 24 of the Charter, respectively.

26 Art. 7 and 8 of the Charter, respectively.

27 See in particular CJEU, *La Quadrature du Net*, Joined Cases C-511/18, C-512/18 and C-520/18, para. 126.

protection of personal data and to freedom of expression and information[28]. Whilst of great importance, none of these rights is absolute and they must be considered in relation to their function in society[29]. As indicated above, Article 52(1) of the Charter allows limitations to be placed on the exercise of those rights, subject to the conditions set out in that provision.

In addition, the **freedom to conduct a business** of the providers covered by the proposal comes into play as well[30]. Broadly speaking, this fundamental right precludes economic operators from being made subject to excessive burdens. It includes the freedom to choose with whom to do business and the freedom of contract. However, this right is not absolute either; it allows for a broad range of interventions that may limit the exercise of economic activities in the public interest[31]. Accordingly, the proposal seeks to achieve the abovementioned objective of general interest and to protect said fundamental rights of children, whilst ensuring proportionality and striking a fair balance between the fundamental rights of all parties involved. To that aim, the proposal contains a range of limits and safeguards, which are differentiated depending on the nature and level of the limit imposed on the exercise of the fundamental rights concerned.

Specifically, obliging detection of online child sexual abuse on both 'public-facing' and 'private' services, including interpersonal communication services, results in varying levels of intrusiveness in respect of the fundamental rights of users. In the case of material that is accessible to the public, whilst there is an intrusion, the impact especially on the right to privacy is generally smaller given the role of these services as 'virtual public spaces' for expression and economic transactions. The impact on the right to privacy in relation to private communications is greater.

Furthermore, the potential or actual removal of users' material, in particular erroneous removal (on the mistaken assumption that it concerns child sexual abuse material), can potentially have a significant impact on users' fundamental rights, especially to freedom of expression and information. At the same time, online child sexual abuse material that is not detected and left unremoved can have a significant negative impact on the aforementioned fundamental rights of the children, perpetuating harm for children and for society at large. Other factors to be taken into account in this regard include the nature of the users' material in question (text, photos, videos), the accuracy of the technology concerned, as well as the 'absolute' nature of the prohibition to exchange child sexual abuse material (which is in principle not subject to any exceptions and is not context-sensitive).

As a result of the measures obliging providers to detect and report known and new child sexual abuse material, the proposal would have a significantly positive impact on the fundamental rights of victims whose images are circulating on the internet, in particular on their right to respect for private and family life, right to protection of personal data and the right to the integrity of the person.

These measures would significantly reduce the violation of victims' rights inherent in the circulation of material depicting their abuse. These obligations, in particular the requirement

[28] Art. 7, 8 and 11 of the Charter, respectively.
[29] Cf. e.g. CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, para. 120.
[30] Art. 16 of the Charter.
[31] Cf. e.g. CJEU, *Sky Österreich*, Case C-283/11, para. 45-46.

to detect new child sexual abuse materials and 'grooming', would result in the identification of new victims and create a possibility for their rescue from ongoing abuse, leading to a significant positive impact on their rights and society at large.. The provision of a clear legal basis for the mandatory detection and reporting of 'grooming' would also positively impact these rights. Increased and more effective prevention efforts will also reduce the prevalence of child sexual abuse, supporting the rights of children by preventing them from being victimised. Measures to support victims in removing their images and videos would safeguard their rights to protection of private and family life (privacy) and of personal data.

As mentioned, the imposition of obligations on providers would affect their right to freedom to conduct a business, which can in principle be justified in view of the objective pursued, having regard also to the role that their services play in connection to the abuse. The impact on providers' rights nevertheless needs to be limited to the maximum extent possible to ensure that it is does not go beyond what is strictly necessary. This would be ensured, for instance, by providing certain forms of support to providers for the implementation of the obligations imposed, including access to reliable sets of indicators of online child sexual abuse that in turn provide means to use reliable automated detection technologies, and to free-of-charge automated detection technologies, reducing the burden on them. In addition, providers benefit from being subject to a single set of clear and uniform rules.

The processing of users' personal data for the purposes of detecting, reporting and removing online child sexual abuse has a significant impact on users' rights and can be justified only in view of the importance of preventing and combating online child sexual abuse. As a result, the decision of whether to engage in these activities in principle cannot be left to the providers; it rather pertains to the legislator. Nonetheless, any obligations need to be narrowly targeted both in their personal and material scope and be coupled with adequate safeguards, in order not to affect the essence of the rights and to be proportionate. This proposal therefore sets out rules that correspond to these requirements, setting out limits and safeguards that are differentiated in function of the potential impact on the fundamental rights at stake, increasing generally speaking depending on the types of services concerned and whether the measures aim to detect the dissemination of known child sexual abuse material, the dissemination of new child sexual abuse material or the solicitation of children ('grooming').

As mentioned, detecting 'grooming' would have a positive impact on the fundamental rights of potential victims especially by contributing to the prevention of abuse; if swift action is taken, it may even prevent a child from suffering harm. At the same time, the detection process is generally speaking the most intrusive one for users (compared to the detection of the dissemination of known and new child sexual abuse material), since it requires automatically scanning through texts in interpersonal communications. It is important to bear in mind in this regard that such scanning is often the only possible way to detect it and that the technology used does not 'understand' the content of the communications but rather looks for known, pre-identified patterns that indicate potential grooming. Detection technologies have also already acquired a high degree of accuracy[32], although human oversight and review remain necessary, and indicators of 'grooming' are becoming ever more reliable with time, as the algorithms learn.

[32] For example, Microsoft reports that the accuracy of its grooming detection tool is 88%, meaning that out of 100 conversations flagged as possible criminal solicitation of children, 12 can be excluded upon review and will not be reported to law enforcement; see annex 8 of the Impact Assessment.

Nonetheless, the interferences at stake remain highly sensitive. As a result, while robust limits and safeguards are already applied to the detection of known child sexual abuse material, they are more restrictive for new child sexual abuse materials and, especially, for the detection of 'grooming'. These include adjusted criteria for the imposition of the detection orders, a more limited period of application of those orders and reinforced reporting requirements during that period. In addition, the proposal also sets out strong oversight mechanisms, which include requirements regarding the independence and powers of the national authorities charged with issuing the orders and overseeing their execution, as well as an assisting and advising role for the EU Centre. The EU Centre also contributes by making available not only accurate and reliable indicators, but also suitable technologies to providers, and by assessing reports of potential online child sexual abuse made by providers. In this manner it helps the EU Centre minimise the risk of erroneous detection and reporting. In addition, various measures are taken to ensure effective redress for both providers and users.

Whilst different in nature and generally speaking less intrusive, the newly created power to issue removal orders in respect of known child sexual abuse material certainly also affects fundamental rights, most notably those of the users concerned relating to freedom of expression and information. In this respect, too, a set of limits and safeguards is provided for, ranging from setting clear and standardised rules to ensuring redress and from guaranteeing the issuing authorities' independence to transparency and effective oversight.

All references in the proposed Regulation to fundamental rights are to be understood as referring solely to the fundamental rights recognised under EU law, that is, those enshrined in the Charter and those recognised as general principles of EU law[33].

4. BUDGETARY IMPLICATIONS

The budgetary impact of the proposal will be covered by the allocations foreseen in the Multi-annual Financial Framework (MFF) 2021-27 under the financial envelopes of the Internal Security Fund as detailed in the legislative financial statement accompanying this proposal for a regulation, to the extent that it falls within the current budgetary perspective. These implications also require reprogramming of Heading 7 of the Financial Perspective.

The legislative financial statement accompanying this proposal for a Regulation covers the budgetary impacts for the Regulation itself.

5. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

The programme for monitoring the outputs, results and impacts of the proposed Regulation is set out in its Article 84 and outlined in more detail in the Impact Assessment. The programme sets out various indicators used to monitor the achievement of operational objectives and the implementation of the Regulation.

[33] See Art. 6 Treaty on European Union (TEU).

The Commission will carry out an evaluation and submit a report to the European Parliament and the Council at the latest five years after the entry into force of the Regulation, and every six years thereafter. Based on the findings of the report, in particular on whether the Regulation leaves any gaps which are relevant in practice, and taking into account technological developments, the Commission will assess the need to adapt the scope of the Regulation. If necessary, the Commission will submit proposals to adapt the Regulation.

- **Detailed explanation of the specific provisions of the proposal**

The proposed Regulation consists of two main building blocks: first, it imposes on providers obligations concerning the detection, reporting, removal and blocking of known and new child sexual abuse material, as well as solicitation of children, regardless of the technology used in the online exchanges, and, second, it establishes the EU Centre on Child Sexual Abuse as a decentralised agency to enable the implementation of the new Regulation.

Chapter I sets out general provisions, including the subject matter and scope of the Regulation (Article 1) and the definitions of key terms used in the Regulation (Article 2). The reference to 'child sexual abuse material' builds on the relevant terms as defined in the Child Sexual Abuse Directive, namely, child pornography and pornographic performance, and aims to encompass all of the material covered therein insofar as such material can be disseminated through the services in question (in practice, typically in the form of video and pictures). The definition is in line with the one contained in the interim Regulation. The same holds true in respect of the definition of 'solicitation of children' and 'online child sexual abuse'. For the definition of several other terms, the proposal relies on definition contained in other acts of EU law or proposal, in particular the European Electronic Communications Code (EECC)[34] and the DSA proposal.

Chapter II establishes uniform obligations, applicable to all providers of hosting or interpersonal communication service offering such services in the EU's digital single market, to perform an assessment of risks of misuse of their services for the dissemination of known or new child sexual abuse material or for the solicitation of children (together defined as 'online child sexual abuse'). It also includes targeted obligations for certain providers to detect such abuse, to report it via the EU Centre, to remove or disable access to, or to block online child sexual abuse material when so ordered.

Section 1 creates the aforementioned risk assessment obligations for hosting or interpersonal communication service providers (Article 3). It also requires providers to adopt tailored and proportionate measures to mitigate the risks identified (Article 4) and to report on the outcome of the risk assessment and on the mitigation measures adopted to the Coordinating Authorities designated by the Member States (Article 5). Finally, it imposes targeted obligations on software application stores to assess whether any application that they intermediate is at risk of being used for the purpose of solicitation and, if this is the case and the risk is significant, take reasonable measures to identify child users and prevent them from accessing it (Article 6).

[34] Directive (EU) 2018/1972 of the European Parliament and the Council of 11 December 2018 establishing the European Electronic Communications Code.

Section 2 empowers Coordinating Authorities which have become aware – through a risk assessment or other means – of evidence that a specific hosting or interpersonal communications service is at a significant risk of being misused for the purpose of online child sexual abuse to ask the competent judicial or independent administrative authority to issue an order obliging the provider concerned to detect the type of online child sexual abuse at issue on the relevant service (Articles 7 and 8). It contains a set of complementary measures, such as those ensuring that providers have a right to challenge orders received (Article 9). The section also establishes requirements and safeguards to ensure that detection is carried out effectively and, at the same time, in a balanced and proportionate manner (Article 10). Finally, it attributes to the Commission the power to adopt guidelines on the application of Articles 7 to 10 (Article 11).

Section 3 obliges providers of hosting or interpersonal communication services that have become aware, irrespective of the manner in which they have become aware, of any instance of potential online child sexual abuse on their services provided in the Union to report it immediately to the EU Centre (Article 12) and specifies the requirements that the relevant report has to fulfil (Article 13).

Section 4 empowers Coordinating Authorities to request the competent judicial or independent administrative authority to issue an order obliging a hosting service provider to remove child sexual abuse material on its services or to disable access to it in all Member States, specifying the requirements that the order has to fulfil (Article 14). Where providers detect online child sexual abuse, they are under no obligation under EU law to remove such material. Nonetheless, given the manifestly illegal nature of most online child sexual abuse and the risk of losing the liability exemption contained in the e-Commerce Directive and the DSA proposal, providers will regularly choose to remove it (or to disable access thereto). Where a provider does not remove online child sexual abuse material of its own motion, the Coordinating Authorities can compel removal by issuing an order to that effect. The article also requires providers of hosting services that have received such an order to inform the user who provided the material, subject to exceptions to prevent interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences. Other measures, such as redress, are also regulated (Article 15). The rules contained in this section have been inspired by those contained in the Terrorist Content Online Regulation (Regulation 2021/784).

Section 5 empowers Coordinating Authorities to request the competent judicial or independent administrative authority to issue an order obliging a provider of internet access services to disable access to uniform resource locators indicating specific items of child sexual abuse material that cannot reasonably be removed at source (Article 16 and 17). Article 18 ensures inter alia that providers that received such a blocking order have a right to challenge it and that users' redress is ensured as well, including through requests for re-assessment by the Coordinating Authorities. These Articles, in combination with the provisions on reliable identification of child sexual abuse material (Article 36) and data quality (Article 46), set out conditions and safeguards for such orders, ensuring that they are effective as well as balanced and proportionate.

Section 6 lays out an exemption from liability for child sexual abuse offenses for providers of relevant information society services carrying out activities to comply with this Regulation

(Article 19). This principally aims to prevent the risk of being held liable under national criminal law for conduct required under this Regulation.

Section 6 also creates specific rights for victims, whose child sexual abuse images and videos may be circulating online long after the physical abuse has ended. Article 20 gives victims of child sexual abuse a right to receive from the EU Centre, via the Coordinating Authority of their place of residence, information on reports of known child sexual abuse material depicting them. Article 21 sets out a right for victims to seek assistance from providers of hosting services concerned or, via the Coordinating Authority of their place of residence, the support of the EU Centre, when they seek to obtain the removal or disabling of access to such material.

This Section also exhaustively lists the purposes for which providers of hosting or interpersonal communication services are to preserve content data and other data processed in connection to the measures taken to comply with this Regulation and the personal data generated through such processing, setting out a series of safeguards and guarantees, including a maximum period of preservation of 12 months (Article 22).

Finally, it lays out the obligation for providers of relevant information society services to establish a single point of contact to facilitate direct communication with the relevant public authorities (Article 23), as well as the obligation for such providers not established in any Member State, but offering their services in the EU, to designate a legal representative in the EU, so as to facilitate enforcement (Article 24).

Chapter III contains provisions concerning the implementation and enforcement of this Regulation. Section 1 lays down provisions concerning national competent authorities, in particular Coordinating Authorities, which are the primary national authorities designated by the Member States for the consistent application of this Regulation (Article 25). Coordinating Authorities, like other designated competent authorities, are to be independent in all respects, akin to a court, and are to perform their tasks impartially, transparently and in a timely manner (Article 26).

Section 2 attributes specific investigatory and enforcement powers to Coordinating Authorities in relation to providers of relevant information society services under the jurisdiction of the Member State that designated the Coordinating Authorities (Articles 27 to 30). These provisions have mostly been inspired by the provisions in the DSA proposal. This section also provides for the power to monitor compliance with this Regulation by conducting searches of child sexual abuse material (Article 31) and to submit notices to providers of hosting services to flag the presence of known child sexual abuse material on their services (Article 32).

Section 3 includes further provisions on enforcement and penalties, by establishing that Member States of the main establishment of the provider of relevant information society services (or of its legal representative) have jurisdiction to apply and enforce this Regulation (Article 33). It also ensures that Coordinating Authorities can receive complaints against such providers for alleged breaches of their obligations laid down in this Regulation (Article 34). In addition, Member States are to lay down rules on penalties applicable to breaches of those obligations (Article 35).

Section 4 contains provisions on cooperation among Coordinating Authorities at EU level. It sets out rules on the assessment of material or conversations so as to confirm that it constitutes online child sexual abuse, which is a task reserved for Coordinating Authorities, other national independent administrative authorities or national courts, as well as for the submission of the outcomes thereof to the EU Centre for the generation of indicators or, where it concerns uniform resource locators, inclusion in the relevant list (Article 36). It also contains rules for cross-border cooperation among Coordinating Authorities (Article 37) and provides for the possibility that they undertake joint investigations, where relevant with the support of the EU Centre (Article 38). These provisions have also been inspired by the DSA proposal. Finally, this section provides for general rules on cooperation at EU level and on a reliable and secure information-sharing system to support communication among the relevant parties (Article 39).

Chapter IV concerns the EU Centre. Its provisions have been based on the Common Approach of the European Parliament, the Council and the Commission on decentralised agencies.

Section 1 establishes the EU Centre on Child Sexual Abuse (EUCSA) as a decentralised EU Centre (Article 40) and regulates the EU Centre's legal status and its seat (Articles 41 and 42). To allow the Centre to achieve all of its objectives, it is of key importance that the EU Centre is established at the same as its closest partner, Europol. The cooperation between the EU Centre and Europol will benefit from sharing location, ranging from improved data exchange possibilities to greater opportunities to create a knowledge hub on child sexual abuse by attracting specialised staff and/or external experts. This staff will also have more career opportunities without the need to change location. It would also allow the EU Centre, while being an independent entity, to rely on the support services of Europol (HR, IT including cybersecurity, communication). Sharing such support services is more cost efficient and ensures a more professional service than duplicating them by creating them from scratch for a relatively small entity as the EU Centre will be.

Section 2 specifies the tasks of the EU Centre under this Regulation. Those include support to Coordinating Authorities, facilitation of the risk assessment, detection, reporting, removal and blocking processes, and facilitating the generation and sharing of knowledge and expertise (Article 43). The EU Centre is mandated to create and maintain databases of indicators of online child sexual abuse (Article 44) and of reports (Article 45) and to grant relevant parties such access to the databases of indicators as required, respecting the conditions and safeguards specified (Article 46). The section also empowers the Commission to adopt delegated acts supplementing this Regulation in relation to those databases (Article 47).

In addition, this section clarifies that the EU Centre is intended to act as a dedicated reporting channel for the entire EU, receiving reports on potential online child sexual abuse from all providers of hosting or interpersonal communication services issued under this Regulation, assessing them to determine whether reports may be manifestly unfounded, and forwarding the reports that are not manifestly unfounded to Europol and competent law enforcement authorities of the Member States (Article 48). Finally, this section establishes that, to facilitate the monitoring of compliance with this Regulation, the EU Centre may under certain circumstances conduct online searches for child sexual abuse material or notify such material to the providers of hosting services concerned requesting removal or disabling of access, for their voluntary consideration (Article 49). The EU Centre is also mandated to make available

relevant technologies for the execution of detection orders and to act as an information and expertise hub, collecting information, conducting and supporting research and information-sharing in the area of online child sexual abuse (Article 50).

Section 3 allows the EU Centre to process personal data for the purposes of this Regulation in compliance with the rules on the processing of such data set by this Regulation and by other acts of EU law on this subject-matter (Article 51).

Section 4 establishes channels of cooperation linking the EU Centre to the Coordinating Authorities, through the designation of national contact officers (Article 52); to Europol (Article 53); and to possible partner organisations, such as the INHOPE network of hotlines for reporting child sexual abuse material (Article 54).

Section 5 sets out the administrative and management structure of the EU Centre (Article 55), establishing the composition, structure, tasks, meeting frequency and voting rules of its Management Board (Articles 56 to 60); the composition, appointment procedure, tasks and voting rules of its Executive Board (Articles 61 to 63); as well as the appointment procedure, and tasks of its Executive Director (Articles 64 and 65). In light of the technical nature and fast-paced evolution of the technologies used by providers of relevant information society services and to support the EU Centre's involvement in the monitoring and implementation of this Regulation in this regard, this section establishes a Technology Committee within the EU Centre, composed of technical experts and performing an advisory function (Article 66).

Section 6 provides for the establishment and structure of the budget (Article 67), the financial rules applicable to the EU Centre (Article 68), the rules for the presentation, implementation and control of the EU Centre's budget (Article 69), as well as presentation of accounts and discharge (Article 70).

Sections 7 and 8 contain closing provisions on composition and status of the EU Centre's staff, language arrangements, transparency and communications concerning its activities, measures to combat fraud, contractual and non-contractual liability, possibility for administrative inquires, headquarters agreement and operating conditions, as well as the start of the EU Centre's activities (Articles 71 to 82).

Chapter V sets out data collection and transparency reporting obligations. It requires the EU Centre, Coordinating Authorities and providers of hosting, interpersonal communications and internet access services to collect aggregated data relating to their activities under this Regulation and make the relevant information available to the EU Centre (Article 83), as well as to report annually on their activities to the general public and the Commission (Article 84).

Chapter VI contains the final provisions of this Regulation. Those relate to the periodic evaluation of this Regulation and of the activities of the EU Centre (Article 85); to the adoption of delegated and implementing acts in accordance with Articles 290 and 291 TFEU, respectively (Articles 86 and 87); to the repeal of the interim Regulation (Regulation 2021/1232) (Article 88) and finally to the entry into force and application of this Regulation (Article 89).

2022/0155 (COD)

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[35],

Having regard to the opinion of the Committee of the Regions[36],

Having regard to the opinion of the European Data Protection Supervisor[37],

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.

(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.

---

35 OJ C , , p. .

36 OJ C , , p. .

37 OJ C , , p. .

(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 as 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[38], Directive 2000/31/EC of the European Parliament and of the Council[39] and Regulation (EU) …/… of the European Parliament and of the Council[40] [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*],

[38] 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).

[39] 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).

[40] 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 ….).

Directive 2010/13/EU of the European Parliament and of the Council [41], Regulation (EU) 2016/679 of the European Parliament and of the Council[42], and Directive 2002/58/EC of the European Parliament and of the Council[43].

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

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

---

41 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).

42 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).

43 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).

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[44]. 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.

(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) …/… [*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.

(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

[44] 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).

an obligation to adopt mitigation measures pursuant to Regulation (EU) …/… [*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.

(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.

(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.

(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 mitigating measures are 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.

(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 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.

(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 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. 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.

(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. 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 the security and confidentiality of the communications of users.

(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.

(30) To ensure that online child sexual abuse material is removed as swiftly as possible after its detection, Coordinating Authorities of establishment should have the power to request competent judicial authorities or independent administrative authorities to issue a removal order addressed to providers of hosting services. As removal or disabling of access may affect the right of users who have provided the material concerned, providers should inform such users of the reasons for the removal, to enable them to exercise their right of redress, subject to exceptions needed to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

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

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

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

(34) 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.

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

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

(40) In order to facilitate smooth and efficient communications by electronic means, including, where relevant, by acknowledging the receipt of such communications, relating to matters covered by this Regulation, providers of relevant information society services should be required to designate a single point of contact and to publish relevant information relating to that point of contact, including the languages to be used in such communications. 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) …/… [*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) …/… [*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.

(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 Authorities should be able to request the assistance of the EU Centre in carrying out certain of their tasks. Such assistance should be without prejudice to the respective tasks and powers of the Coordinating Authorities requesting assistance and of the EU Centre and to the requirements applicable to the performance of their respective tasks and the exercise of their respective powers provided in this Regulation.

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

(47) The Coordinating Authority, as well as other competent authorities, play a crucial role in ensuring the effectiveness of the rights and obligations laid down in this Regulation and the achievement of its objectives. Accordingly, it is necessary to ensure that those authorities have not only the necessary investigatory and enforcement powers, but also 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 Authorities should be granted enforcement powers to address infringements of this

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

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

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

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

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

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

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

(55) It is essential for the proper functioning of the system of mandatory detection and blocking of online child sexual abuse set up by this Regulation that the EU Centre receives, via the Coordinating Authorities, 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, either by the Coordinating Authorities themselves or by a court or another independent administrative authority than the Coordinating Authority. Whilst the swift assessment, identification and submission of such material is important also in other contexts, it is crucial in connection to new child sexual abuse material and the solicitation of children reported under this Regulation, considering that this material can lead to the identification of ongoing or imminent abuse and the rescuing of victims. Therefore, specific time limits should be set in connection to such reporting.

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

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

(58) In particular, in order to facilitate the cooperation needed for the proper functioning of the mechanisms set up by this Regulation, the EU Centre should establish and maintain the necessary information-sharing systems. When establishing and maintaining such systems, the EU Centre should cooperate with the European Union Agency for Law Enforcement Cooperation ('Europol') and national authorities to build on existing systems and best practices, where relevant.

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

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

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

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

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

(64) Given the sensitivity of the data concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of indicators and databases of reports, on the data contained therein and on their security. In particular, the data concerned should not be stored for longer than is

strictly necessary. For the above reasons, access to the database of indicators should be given only to the parties and for the purposes specified in this Regulation, subject to the controls by the EU Centre, and be limited in time and in scope to what is strictly necessary for those purposes.

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

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

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

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

(69) In order to allow for the effective and efficient performance of its tasks, the EU Centre should closely cooperate with Coordinating Authorities, the Europol and relevant partner organisations, such as the US National Centre for Missing and Exploited Children or the International Association of Internet Hotlines ('INHOPE') network of hotlines for reporting child sexual abuse material, within the limits sets by this Regulation and other legal instruments regulating their respective activities. To facilitate such cooperation, the necessary arrangements should be made, including the designation of contact officers by Coordinating Authorities and the conclusion of

memoranda of understanding with Europol and, where appropriate, with one or more of the relevant partner organisations.

(70) 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 Authorities, providers of relevant information society services and law enforcement authorities of the Member States. The hotlines' expertise and experience is an invaluable source of information on the early identification of common threats and solutions, as well as on regional and national differences across the Union.

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

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

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

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

(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.

(78) Regulation (EU) 2021/1232 of the European Parliament and of the Council[45] 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. Regulation (EU) 2021/1232 should therefore be repealed.

(79) In order to achieve the objectives of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to amend the Annexes to this Regulation and to supplement it by laying down detailed rules concerning the setting up, content and access to the databases operated by the EU Centre, concerning the form, precise content and other details of the reports and the reporting process, concerning the determination and charging of the costs incurred by the EU Centre to support providers in the risk assessment, as well as concerning technical requirements for the information sharing systems supporting communications between Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services.

(80) It is important that the Commission carry out appropriate consultations during its preparatory work for delegated acts, including via open public consultation and at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law Making[46]. 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

[45] 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).

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

powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[47].

(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[48] and delivered their opinion on […].

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Regulation lays down uniform rules to address the misuse 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 misused for online child sexual abuse;

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

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

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

[47] 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).

[48] 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).

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

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

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

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

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

(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.

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

Article 2

Definitions

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

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

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

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

(d) 'software application store' means a service as defined in Article 2, point 12, of Regulation (EU) …/… [*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[49];

[49] 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).

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

(a) a hosting service;

(b) an interpersonal communications service;

(c) a software applications store;

(d) an internet access service.

(g) ‘to offer services in the Union’ means to offer services in the Union as defined in Article 2, point (d), of Regulation (EU) …/… [*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[50];

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

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

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

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

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

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

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

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

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

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

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

(v) ‘terms and conditions’ means terms and conditions as defined in Article 2, point (q), of Regulation (EU) …/… *[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.

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 identify, analyse and assess, for each such service that they offer, the risk of use of the service for the purpose of online child sexual abuse.

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

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

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

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

      – measures taken to enforce such prohibitions and restrictions;

      – functionalities enabling age verification;

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

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

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

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

      (1) the extent to which the service is used or is likely to be used by children;

      (2) 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;

      (3) 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.

4. 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.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 87 in order to supplement this Regulation with the necessary detailed rules on the determination and charging of those costs and the application of the exemption for micro, small and medium-sized enterprises.

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

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

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

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

7. 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.

8. 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. Providers of hosting services and providers of interpersonal communications services shall take reasonable mitigation measures, tailored to the risk identified pursuant to Article 3, to minimise that risk. Such measures shall include some or all of the following:

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

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

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

2. The mitigation measures shall be:

(a) effective in mitigating the identified risk;

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

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

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

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

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

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

Article 5

Risk reporting

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

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

(b) any mitigation measures taken pursuant to Article 4.

2. Within three months after receiving the report, the Coordinating Authority of establishment shall assess it and determine, on that basis and taking into account any

other relevant information available to it, whether the risk assessment has been carried out or updated and the mitigation measures have been taken in accordance with the requirements of Articles 3 and 4.

3. Where necessary for that assessment, that Coordinating Authority may require further information from the provider, within a reasonable time period set by that Coordinating Authority. That time period shall not be longer than two weeks. The time period referred to in the first subparagraph shall be suspended until that additional information is provided.

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

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

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

Article 6

Obligations for software application stores

1. Providers of software application stores shall:

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

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

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

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

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

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

Section 2
Detection obligations

Article 7

Issuance of detection orders

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. As regards the second subparagraph, point (d), where that Coordinating Authority substantially deviates from the opinion of the EU Centre, it shall inform the EU

Centre and the Commission thereof, specifying the points at which it deviated and the main reasons for the deviation.

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

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

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

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

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

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

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

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

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

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

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

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

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

The detection orders concerning the solicitation of children shall apply only to interpersonal communications where one of the users is a child user.

8. The Coordinating Authority of establishment when requesting the issuance of detection orders, and the competent judicial or independent administrative authority

when issuing the detection order, shall target and specify it in such a manner that the negative consequences referred to in paragraph 4, first subparagraph, point (b), remain limited to what is strictly necessary 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.

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

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

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

Article 8

Additional rules regarding detection orders

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 9

Redress, information, reporting and modification of detection orders

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

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

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

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

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

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

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

Article 10

Technologies and safeguards

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

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

3. The technologies shall be:

(a) effective in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;

(b) not be able to extract 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) 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) sufficiently reliable, in that they limit to the maximum extent possible the rate of errors regarding the detection.

4. The provider shall:

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

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

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

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

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

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

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

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

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

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

Article 11

Guidelines regarding detection obligations

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

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

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

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

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

Article 13

Specific requirements for reporting

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 4
Removal obligations

Article 14

Removal orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a removal order

requiring a provider of hosting services under the jurisdiction of the Member State that designated that Coordinating Authority to remove or disable access in all Member States of one or more specific items of material that, after a diligent assessment, the Coordinating Authority or the courts or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 15

Redress and provision of information

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

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

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

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

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

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

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

4. The Coordinating Authority of establishment may request, when requesting the judicial authority or independent administrative authority issuing the removal order,

and after having consulted with relevant public authorities, that the provider is not to disclose any information regarding the removal of or disabling of access to the child sexual abuse material, where and to the extent necessary to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

In such a case:

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

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

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

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

Section 5
Blocking obligations

Article 16

Blocking orders

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

   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.

2. 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(6) and Article 46, respectively;

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

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

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

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

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

(c) the uniform resource locators indicate, in a sufficiently reliable manner, child sexual abuse material;

(d) the reasons for issuing the blocking order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties, including the exercise of the users' freedom of expression and information and the provider's freedom to conduct a business.

When assessing whether the conditions of the first subparagraph have been met, account shall be taken of all relevant facts and circumstances of the case at hand, including any information obtained pursuant to paragraph 2 and the views of the provider submitted in accordance with paragraph 3.

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

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

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

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

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

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

That Coordinating Authority shall request to the competent judicial authority or independent administrative authority that issued the blocking order the modification or revocation of such order, where necessary in the light of the outcome of that assessment or to take account of justified requests or the reports referred to in Article 18(5) and (6), respectively. The provisions of this Section shall apply to such requests, *mutatis mutandis*.

Article 17

Additional rules regarding blocking orders

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 18

Redress, information and reporting of blocking orders

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

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

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

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

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

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

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

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

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

the blocking orders that occurred after the issuance thereof, in particular substantial changes preventing the provider from taking the required reasonable measures to execute the blocking order,

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

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

Section 6
Additional provisions

Article 19

Liability of providers

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

Article 20

Victims' right to information

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

2. 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 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.

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

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

   (b) the date of the report;

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

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

Article 21

Victims' right of assistance and support for removal

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

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

3. 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.

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

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

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

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

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

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

Article 22

Preservation of information

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

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

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

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

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

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

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

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

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

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

Article 23

Points of contact

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

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.

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

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

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

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

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

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

CHAPTER III

SUPERVISION, ENFORCEMENT AND COOPERATION

Section 1
Coordinating Authorities for child sexual abuse issues

Article 25

Coordinating Authorities for child sexual abuse issues and other competent authorities

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 26

Requirements for Coordinating Authorities

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

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

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

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

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

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

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

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

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

5. The management and other staff of the Coordinating Authorities shall, in accordance with Union or national law, be subject to a duty of professional secrecy both during

and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks. Member States shall ensure that the management and other staff are subject to rules guaranteeing that they can carry out their tasks in an objective, impartial and independent manner, in particular as regards their appointment, dismissal, remuneration and career prospects.

Section 2
Powers of Coordinating Authorities

Article 27

Investigatory powers

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

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

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

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

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

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

Article 28

Enforcement powers

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

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

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

   (c) the power to impose fines, or request a judicial authority in their Member State to do so, in accordance with Article 35 for infringements of this Regulation,

including non-compliance with any of the orders issued pursuant to Article 27 and to point (b) of this paragraph;

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

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

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

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

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

Article 29

Additional enforcement powers

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

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

(b) the infringement persists;

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

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

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

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

(ii) ensure that the provider takes those measures;

(iii) report on the measures taken;

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

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

(ii) the infringement persists and causes serious harm;

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

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

The invitation to submit written observations shall:

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

(b) identify the intended addressee or addressees thereof.

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

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

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

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

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

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

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

Article 30

Common provisions on investigatory and enforcement powers

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

operational capacity of the provider of relevant information society services concerned, where applicable.

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

Article 31

Searches to verify compliance

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

Article 32

Notification of known child sexual abuse material

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

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

Section 3

Other provisions on enforcement

Article 33

Jurisdiction

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

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

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

Article 34

Right of users of the service to lodge a complaint

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

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

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

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

Article 35

Penalties

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

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

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

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

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

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

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

   (b) whether the infringement was intentional or negligent;

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

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

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

(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 it to comply with this Regulation.

Section 4

Cooperation

Article 36

Identification and submission of online child sexual abuse

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

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

   (b) exact uniform resource locators indicating specific items of material that Coordinating Authorities or that competent judicial authorities or other independent administrative authorities of a Member State have identified, after a diligent assessment, as constituting child sexual abuse material, hosted by providers of hosting services not offering services in the Union, that cannot be removed due to those providers' refusal to remove or disable access thereto and to the lack of cooperation by the competent authorities of the third country having jurisdiction, for the EU Centre to compile the list of uniform resource locators in accordance with Article 44(3).

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

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

3. Member States shall ensure that, where their law enforcement authorities receive a report of the dissemination of new child sexual abuse material or of the solicitation of children forwarded to them by the EU Centre in accordance with Article 48(3), a diligent assessment is conducted in accordance with paragraph 1 and, if the material

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

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

Article 37

Cross-border cooperation among Coordinating Authorities

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

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

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

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

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

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

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

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

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

measures taken or envisaged in relation thereto to ensure compliance with this Regulation.

Article 38

Joint investigations

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

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

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

Article 39

General cooperation and information-sharing system

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

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

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

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

CHAPTER IV

EU CENTRE TO PREVENT AND COMBAT CHILD SEXUAL ABUSE

Section 1

Principles

Article 40

Establishment and scope of action of the EU Centre

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

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

Article 41

Legal status

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

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

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

Article 42

Seat

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

Section 2

Tasks

Article 43

Tasks of the EU Centre

The EU Centre shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) providing the opinions on intended blocking orders referred to in Article 16(3);

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) drawing up the annual reports referred to in Article 85.

Article 44

Databases of indicators

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

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

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

(c) indicators to detect the solicitation of children.

2. The databases of indicators shall solely contain:

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

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

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

3. The EU Centre shall generate the indicators referred to in paragraph 2, point (a), solely on the basis of the child sexual abuse material and the solicitation of children identified as such by the Coordinating Authorities or the courts or other independent authorities of the Member States, submitted to it by the Coordinating Authorities pursuant to Article 36(1), point (a).

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

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

Article 45

Database of reports

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

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

   (a) the report;

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

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

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

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

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

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

Article 46

Access, accuracy and security

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

2. The EU Centre shall give providers of hosting services, providers of interpersonal communications services and providers of internet access services access to the databases of indicators referred to in Article 44, where and to the extent necessary for them to execute the detection or blocking orders that they received in accordance

with Articles 7 or 16. It shall take measures to ensure that such access remains limited to what is strictly necessary for the period of application of the detection or blocking orders concerned and that such access does not in any way endanger the proper operation of those databases and the accuracy and security of the data contained therein.

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

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

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

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

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

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

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

Article 47

Delegated acts relating to the databases

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

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

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

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

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

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

Article 48

Reporting

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

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

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

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

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

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

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

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

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

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

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

Article 49

Searches and notification

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

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

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

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

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

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

Article 50

Technologies, information and expertise

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

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

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

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

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

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

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

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

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

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

Section 3

Processing of information

Article 51

Processing activities and data protection

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

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

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

   (b) cooperating with and responding to requests of Coordinating Authorities in connection to intended blocking orders as referred to in Article 16(3);

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

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

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

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

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

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

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

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

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

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

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

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

   (o) generating statistics in accordance with Article 83.

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

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

Section 4

Cooperation

Article 52

Contact officers

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

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

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

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

Article 53

Cooperation with Europol

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

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

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

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

Article 54

Cooperation with partner organisations

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

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

Section 5

Organisation

Article 55

Administrative and management structure

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

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

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

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

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

(e)

Part 1: Management Board

Article 56

Composition of the Management Board

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

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

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

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

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

order to ensure continuity of its work. All parties shall aim to achieve a balanced representation between men and women on the Management Board.

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

Article 57

Functions of the Management Board

1. The Management Board shall:

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

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

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

(d) adopt the assessment of performance of the Executive Board referred to in Article 61(4);

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

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

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

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

Article 58

Chairperson of the Management Board

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

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

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

Article 59

Meetings of the Management Board

1. The Chairperson shall convene the meetings of the Management Board.

2. The Executive Director shall take part in the deliberations, without the right to vote.

3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, or at the request of at least one-third of its members.

4. The Management Board may invite any person whose opinion may be of interest to attend its meetings as an observer.

5. The members of the Management Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.

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

Article 60

Voting rules of the Management Board

1. Unless provided otherwise in this Regulation, the Management Board shall take decisions by absolute majority of its members.

2. Each member shall have one vote. In the absence of a member, his/her alternate shall be entitled to exercise his/her right to vote.

3. The Executive Director shall not take part in the voting.

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

Part 2: Executive Board

Article 61

Composition and appointment of the Executive Board

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

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

2. The term of office of members of the Executive Board shall be four years. In the course of the 12 months preceding the end of the four-year term of office of the Chairperson and five members of the Executive Board, the Management Board or a smaller committee selected among Management Board members including a Commission representative shall carry out an assessment of performance of the Executive Board. The assessment shall take into account an evaluation of the Executive Board members' performance and the EU Centre's future tasks and challenges. Based on the assessment, the Management Board may extend their term of office once.

Article 62

Tasks of the Executive Board

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

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

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

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

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

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

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

(f) adopt its rules of procedure;

(g) exercise, with respect to the staff of the EU Centre, the powers conferred by the Staff Regulations on the Appointing Authority and by the Conditions of Employment of Other Servants on the EU Centre Empowered to Conclude a Contract of Employment[51] ("the appointing authority powers");

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

(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.

[51] 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)

(n) appoint a Data Protection Officer;

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

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

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

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

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

Article 63

Voting rules of the Executive Board

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

2. The representatives of the Commission shall have a right to vote whenever matters pertaining to Article 62(2), points (a) to (l) and (p) are discussed and decided upon. For the purposes of taking the decisions referred to in Article 62(2), points (f) and (g), the representatives of the Commission shall have one vote each. The decisions referred to in Article 62(2), points (b) to (e), (h) to (l) and (p), may only be taken if the representatives of the Commission casts a positive vote. For the purposes of taking the decisions referred to in Article 62(2), point (a), the consent of the representatives of the Commission shall only be required on the elements of the decision not related to the annual and multi-annual working programme of the EU Centre.

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

Part 3: Executive Director

Article 64

Responsibilities of the Executive Director

1. The Executive Director shall manage the EU Centre. The Executive Director shall be accountable to the Management Board.

2. The Executive Director shall report to the European Parliament on the performance of his/her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his/her duties.

3. The Executive Director shall be the legal representative of the EU Centre.

4. The Executive Director shall be responsible for the implementation of the tasks assigned to the EU Centre by this Regulation. In particular, the Executive Director shall be responsible for:

   (a) the day-to-day administration of the EU Centre;

   (b) preparing decisions to be adopted by the Management Board;

   (c) implementing decisions adopted by the Management Board;

   (d) preparing the Single Programming Document and submitting it to the Executive Board after consulting the Commission;

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

   (f) preparing the Consolidated Annual Activity Report (CAAR) on the EU Centre's activities and presenting it to the Executive Board for assessment and adoption;

   (g) preparing an action plan following-up conclusions of internal or external audit reports and evaluations, as well as investigations by the European Anti-Fraud Office (OLAF) and by the European Public Prosecutor's Office (EPPO) and reporting on progress twice a year to the Commission and regularly to the Management Board and the Executive Board;

   (h) protecting the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of OLAF and EPPO by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative, including financial penalties;

   (i) preparing an anti-fraud strategy, an efficiency gains and synergies strategy, a strategy for cooperation with third countries and/or international organisations and a strategy for the organisational management and internal control systems for the EU Centre and presenting them to the Executive Board for approval;

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

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

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

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

   (n) drawing up a draft statement of estimates of the EU Centre's revenue and expenditure as part of the EU Centre's Single Programming Document

pursuant to Article 67 and implementing the budget of the EU Centre pursuant to Article 68;

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

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

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

Article 65

Executive Director

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

2. The Executive Director shall be appointed by the 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 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 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 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 Management Board acting on a proposal from the Commission.

8. The 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.

Subsection 5: Technology Committee

Article 66

Establishment and tasks of the Technology Committee

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

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

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

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

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

6. The Technology Committee shall

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

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

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

Section 6

Establishment and Structure of the Budget

Subsection 1

Single Programming Document

Article 67

Budget establishment and implementation

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

2. The Executive Board shall, on the basis of the draft statement of estimates, adopt a provisional draft estimate of the EU Centre's revenue and expenditure for the following financial year and shall send it to the Commission by 31 January each year.

3. The Executive Board shall send the final draft estimate of the EU Centre's revenue and expenditure, which shall include a draft establishment plan, to the European Parliament, the Council and the Commission by 31 March each year.

4. The Commission shall send the statement of estimates to the European Parliament and the Council, together with the draft general budget of the Union.

5. On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates that it considers necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall place before the European Parliament and the Council in accordance with Articles 313 and 314 of the Treaty on the Functioning of the European Union.

6. The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to the EU Centre.

7. The European Parliament and the Council shall adopt the EU Centre's establishment plan.

8. The EU Centre's budget shall be adopted by the Executive Board. It shall become final following the final adoption of the general budget of the Union. Where necessary, it shall be adjusted accordingly.

9. The Executive Director shall implement the EU Centre's budget.

10. Each year the Executive Director shall send to the European Parliament and the Council all information relevant to the findings of any evaluation procedures.

Article 68

Financial rules

The financial rules applicable to the EU Centre shall be adopted by the Executive Board after consultation with the Commission. They shall not depart from Delegated Regulation (EU) 2019/715[52] unless such a departure is specifically required for the operation of the EU Centre and the Commission has given its prior consent.

1.

Subsection 2

Presentation, implementation and control of the budget

Article 69

Budget

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

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

3. The EU Centre may benefit from Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in

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

Article 68 and with the provisions of the relevant instruments supporting the policies of the Union.

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

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

Article 70

Presentation of accounts and discharge

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

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

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

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

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

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

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

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

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

Section 7

Staff

Article 71

General provisions

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

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

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

Article 72

Seconded national experts and other staff

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

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

Article 73

Privileges and immunities

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

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

Article 74

Obligation of professional secrecy

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

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

3. For the purpose of carrying out the tasks conferred on it by this Regulation, the EU Centre shall be authorised, within the limits and under the conditions set out in the

acts referred to in Article 1(2), to exchange information with national or Union authorities and bodies in the cases where these acts allow financial supervisors to disclose information to those entities or where Member States may provide for such disclosure under the relevant Union law.

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

5. The EU Centre shall apply Commission Decision (EU, Euratom) 2015/444[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[54] and (EU, Euratom) 2015/444. The security rules of the EU Centre shall cover, inter alia, provisions for the exchange, processing and storage of such information. The Executive Board shall adopt the EU Centre's security rules following approval by the Commission.

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

Section 8

General provisions

Article 76

Language arrangements

The provisions laid down in Regulation No 1[55] 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[56] shall apply to documents held by the EU Centre. The Management Board shall, within six months of the date of its first meeting, adopt the detailed rules for applying that Regulation.

2. The processing of personal data by the EU Centre shall be subject to Regulation (EU) 2018/1725. The Management Board shall, within six months of the date of its first meeting, establish measures for the application of that Regulation by the EU

53 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).

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

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

56 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.

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[57] shall apply.

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

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

4. OLAF may carry out investigations, including on-the-spot checks and inspections with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by the EU Centre, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96[58].

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.

---

57 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).

58 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).

2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the EU Centre.

3. In the case of non-contractual liability, the EU Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its departments or by its staff in the performance of their duties.

4. The Court of Justice of the European Union shall have jurisdiction in disputes over compensation for damages referred to in paragraph 3.

5. The personal liability of its staff towards the Centre shall be governed by the provisions laid down in the Staff Regulations or Conditions of Employment applicable to them.

Article 80

Administrative inquiries

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

Article 81

Headquarters Agreement and operating conditions

1. The necessary arrangements concerning the accommodation to be provided for the EU Centre in the Member State where the seat of the EU Centre is located and the facilities to be made available by that Member State, together with the specific rules applicable in that Member State to the Executive Director, members of the Executive Board, EU Centre staff and members of their families shall be laid down in a Headquarters Agreement between the EU Centre and the Member State where the seat of the EU Centre is located, concluded after obtaining the approval of the Executive Board and no later than *[2 years after the entry into force of this Regulation]*.

2. The Member State where the seat of the EU Centre is located shall provide the best possible conditions to ensure the smooth and efficient functioning of the EU Centre, including multilingual, European-oriented schooling and appropriate transport connections.

Article 82

Start of the EU Centre's activities

1. The Commission shall be responsible for the establishment and initial operation of the EU Centre until the Executive Director has taken up his or her duties following his or her appointment by the Executive Board in accordance with Article 65(2). For that purpose:

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

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

   (c) the Commission may offer assistance to the EU Centre, in particular by seconding Commission officials to carry out the activities of the EU Centre

under the responsibility of the interim Executive Director or the Executive Director;

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

CHAPTER V

DATA COLLECTION AND TRANSPARENCY REPORTING

Article 83

Data collection

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

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

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

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

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

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

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

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

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

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

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

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

      – where the report led to the launch of a criminal investigation or contributed to an ongoing investigation, the state of play or outcome of

the investigation, including whether the case was closed at pre-trial stage, whether the case led to the imposition of penalties, whether victims were identified and rescued and if so their numbers differentiating by gender and age, and whether any suspects were arrested and any perpetrators were convicted and if so their numbers;

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

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

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

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

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

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

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

(g) the number of blocking orders issued in accordance with Article 16, broken down by provider, and the number of instances in which the provider invoked Article 17(3);

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

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

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

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

(d) the online child sexual abuse to which the reports relate, including the number of items of potential known and new child sexual abuse material and instances of potential solicitation of children, the Member State the competent authority of which the EU Centre forwarded the reports to in accordance with Article 48(3), and type of relevant information society service that the reporting provider offers;

(e) the number of reports that the EU Centre considered 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.

4. The providers of hosting services, providers of interpersonal communications services and providers of internet access services, the Coordinating Authorities and the EU Centre shall ensure that the data referred to in paragraphs 1, 2 and 3, respectively, is stored no longer than is necessary for the transparency reporting referred to in Article 84. The data stored shall not contain any personal data.

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

Article 84

Transparency reporting

1. Each provider of relevant information society services shall draw up an annual report on its activities under this Regulation. That report shall compile the information referred to in Article 84(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 84(2). It shall, by 31 March of every year subsequent to the year to which the report relates, make the report available to the public and communicate it to the Commission and the EU Centre.

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

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

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

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 87 in order to supplement this Regulation with the necessary templates and detailed rules concerning the form, precise content and other details of the reports and the reporting process pursuant to paragraphs 1, 2 and 3.

CHAPTER VI

FINAL PROVISIONS

Article 85

Evaluation

1. By [*five years after the entry into force of this Regulation*], and every five years thereafter, the Commission shall evaluate this Regulation and submit a report on its application to the European Parliament and the Council.

2. By [*five years after the entry into force of this Regulation*], and every five years thereafter, the Commission shall ensure that an evaluation in accordance with Commission guidelines of the EU Centre's performance in relation to its objectives, mandate, tasks and governance and location is carried out. The evaluation shall, in particular, address the possible need to modify the tasks of the EU Centre, and the financial implications of any such modification.

3. On the occasion of every second evaluation referred to in paragraph 2, the results achieved by the EU Centre shall be assessed, having regard to its objectives and tasks, including an assessment of whether the continuation of the EU Centre is still justified with regard to those objectives and tasks.

4. The Commission shall report to the European Parliament and the Council the findings of the evaluation referred to in paragraph 3. The findings of the evaluation shall be made public.

5. For the purpose of carrying out the evaluations referred to in paragraphs 1, 2 and 3, the Coordinating Authorities and Member States and the EU Centre shall provide information to the Commission at its request.

6. In carrying out the evaluations referred to in paragraphs 1, 2 and 3, the Commission shall take into account the relevant evidence at its disposal.

7. Where appropriate, the reports referred to in paragraphs 1 and 4 shall be accompanied by legislative proposals.

Article 86

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 3, 8, 13, 14, 17, 47 and 85 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, 8, 13, 14, 17, 47 and 85 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day after the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 3, 8, 13, 14, 17, 47 and 85 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 87

Committee procedure

1. For the purposes of the adoption of the implementing acts referred to in Article 39(4), the Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

Article 88

Repeal

Regulation (EU) 2021/1232 is repealed from [*date of application of this Regulation*].

Article 89

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 6 months after its entry into force.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

1.2. Policy area(s) concerned

Policy area: Security

Activity: EU strategy for a more effective fight against child sexual abuse [59]

1.3. The proposal relates to

☒ **a new action**

☐ **a new action following a pilot project/preparatory action**[60]

☐ **the extension of an existing action**

☐ **a merger of one or more actions towards another/a new action**

1.4. Objective(s)

General objective(s)

The general objective is to improve the functioning of the internal market by introducing harmonised EU rules aimed at better identifying, protecting of and supporting victims of Child Sexual Abuse (CSA), ensuring effective prevention and facilitating investigations, notably through a clarification of the role and responsibilities of online service providers when it comes to CSA.

This objective directly contributes to achieving the most relevant SDGs for this initiative, 5.2., eliminate all forms of violence against women and girls, and 16.2., end abuse, exploitation, trafficking and all forms of violence against children, and partially addresses SDG 17 with respect to the collection of data on children with disabilities seeking information and assistance from the EU Centre.

Specific objective(s)

Specific objective No

1. ensure the effective detection, reporting and removal of online child sexual abuse,

2. improve legal certainty, transparency and accountability, and ensure that protection of fundamental rights,

3. reduce the proliferation and effects of child sexual abuse through better coordination.

[59] EU strategy for a more effective fight against child sexual abuse, COM(2020)607 of 24/7/20

[60] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

Expected result(s) and impact

Providers of information society services are expected to benefit from the legal certainty of harmonised EU rules on the detection, reporting and removal of online child sexual abuse, and from higher levels of trust where their services demonstrate greater accountability through the adoption of safer-by-design methods, and through improved and standardised transparency reporting.

All internet users and especially child users are expected to benefit from a more structured approach to preventing, detecting, reporting and removing online child sexual abuse across the Union, facilitated by the EU Centre, and from higher levels of trust in online services that adopt safer-by-design methods.

National authorities are expected to benefit from the EU Centre facilitation of the detection, reporting and removal process, and in particular contributing to ensure that the reports on online child sexual abuse received by national law enforcement agencies are relevant and contain sufficient information for law enforcement to act. National authorities will also benefit from the facilitation of the exchange of expertise provided by the EU Centre in terms of sharing best practices and lessons learned across the EU and globally on prevention and assistance to victims.

Indicators of performance

A dedicated monitoring framework, including a number of indicators per the specific objectives, is described in the Impact Assessment Report accompanying the proposal.

In addition, detailed objectives and expected results including performance indicators will be established by the EU Centre's annual work programme, while the multi-annual work programme will set out overall strategic objectives, expected results and performance indicators.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The proposal is based on Article 114 TFEU, focused on the establishment and functioning of the internal market.

The choice of legal basis reflects the main objectives and scope of the initiative given that the Internet is by nature cross-border. Article 114 is the appropriate legal basis to address differences between provisions of Member States' laws which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market, and to prevent the emergence of future obstacles to trade resulting from differences in the way national laws have developed.

This initiative aims to ensure common rules creating the best conditions for maintaining a safe online environment with responsible and accountable behaviour of service providers. At the same time, the intervention provides for the appropriate supervision of relevant service providers and cooperation between authorities at EU level, with the involvement and support of the EU Centre where appropriate. As such, the initiative should increase legal certainty, trust, innovation and growth in the single market for digital services.

A five year timeline from the date of the legislation coming into force is envisaged for the proposed EU Centre to achieve full operational capacity. Commission resources would also be deployed to support the setting up of the Centre during this lead-in period.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this

point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Reasons for action at European level

A satisfactory improvement as regards the rules applicable to relevant online service providers active on the internal market aimed at stepping up the fight against CSA cannot be sufficiently achieved by Member States acting alone or in an uncoordinated way. In particular, a single Member State cannot effectively prevent or stop the circulation online of a CSA image or video, or the online grooming of a child, without the ability to cooperate and coordinate with the private entities who provide services in several (if not all) Member States.

In the absence of EU action, Member States would have to keep adopting individual national laws to respond to current and emerging challenges with the likely consequence of fragmentation and diverging laws likely to negatively affect the internal market, particularly with regard to online service providers active in more than one Member State.

Expected added value for the Union

The expected added value for the Union of the initiative includes the following:

- Reduce fragmentation and compliance/operational costs, improving the functioning of the internal market. The EU Centre will contribute notably by facilitating the implementation of the obligations on service providers to detect, report and remove CSA online, and the action of law enforcement to follow up on those reports.

- Facilitate and support Member States' action on prevention and assistance to victims to increase efficiency and effectiveness. The EU Centre will contribute notably by facilitating the exchange of best practices and serving as a knowledge hub for Member States.

- Reduce dependence on and facilitate cooperation with third countries. The EU Centre will contribute notably by exchanging best practices with third countries, and facilitate Member States' access to expertise and lessons learned from actions to fight against CSA around the globe.

1.5.3. Lessons learned from similar experiences in the past

This proposal is informed by two items of sectoral legislation addressing the area of child sexual abuse. The first is Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and more recently Regulation 2021/1232/EU 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.

The 2011 Directive, which then represented an important step forward, must be fully transposed by Member States as a matter of urgency. The Commission will continue to use its enforcement powers under the Treaties through infringement procedures to ensure swift implementation. In parallel to this, and as indicated in the EU Strategy for a more effective fight against child sexual abuse, the Commission has initiated a study to prepare the evaluation of the 2011 Directive and its possible future revision.

The aim of Regulation 2021/1232/EU (the "Interim Regulation") was to enable certain online communications services to continue the use technologies to detect and report child sexual abuse online and remove child sexual abuse material on their services. It has a limited duration and narrow scope limited to voluntary activities of certain online services during an interim period of maximum 3 years, which will expire in August 2024.

The current proposal builds on the 2011 Directive, in particular for the definition of child sexual abuse offences, and on the Interim Regulation, in particular on its safeguards for the detection of online child sexual abuse.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The 2020 *EU Strategy for a more effective fight against CSA* set out eight initiatives as highlighting the importance of a holistic response to this crime area. Legislation is one such element. Accordingly, this proposal sets out to develop and implement an appropriate legal framework, enhance the law enforcement response, and stimulate coordinated multi-stakeholder action on prevention, investigation and assistance to victims.

This proposal is reflected under the heading of 'Promoting our European way of life' in the Commission Work Programme 2021.

This proposal will build on the necessity of the proposed Digital Services Act to ensure the best conditions for innovative cross-border digital services to develop in the EU across national territories, and at the same time maintain a safe online environment for all EU citizens.

This proposal's aim to create a specific EU framework to combat and prevent online CSA, with elements similar to that of the Terrorist Content Online Regulation, and building on the Digital Services Act provisions to create a harmonised baseline to address all illegal content by targeting child sexual abuse online and grooming in particular.

The EU Centre, a fundamental component to support the implementation of the obligations on service providers to detect, report and remove online child sexual abuse, is expected to generate important efficiency gains for Member States by facilitating their cooperation and in mutualising resources for technical assistance at EU level.

1.5.5. Assessment of the different available financing options, including scope for redeployment

Central to an assessment of the different financing options was the need that the proposed EU Centre must be independent in order to serve as a facilitator of the work of providers of information society services in detecting, reporting, and removing online child sexual abuse, and of the work of law enforcement in following up on those reports from service providers.

Other options for the EU Centre were addressed in the accompanying Impact Assessment where, for example, in terms of incorporating the EU Centre into the EU Centre for Fundamental Rights (FRA) Agency, it was found, inter alia, that this would result in *a significant imbalance in FRA's mandate: as it would double in size, half of it dedicated to CSA and the other half to its current tasks*, and that this would result in further complications associated with rewiring the FRA's governance and underlying legislation.

Accordingly, in order to further support the Centre's independence it is proposed that the Centre be financially independent and be funded by the EU.

The Centre should also be independent from national public entities of the Member State that would host it in order to avoid the risk of prioritising and favouring efforts in this particular Member State. This is without prejudice to the opportunity to draw on the expertise of Member States and EU Justice and Home Affairs agencies to assist with building a critical mass of expertise within the proposed EU Centre.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ Financial impact from YYYY to YYYY

☒ **unlimited duration**

– Implementation with a 5-year start-up period from 2025 onwards,

followed by full-scale operation.

1.7. Management mode(s) planned[61]

☐ **Direct management** by the Commission through

☐ executive agencies

☐ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

☐ international organisations and their agencies (to be specified);

☐the EIB and the European Investment Fund;

☒ bodies referred to in Articles 70 and 71;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

Comments

The level of EU contribution to the CSA Centre has been identified based on the Impact Assessment carried out.

[61] Details of management modes and references to Financial Regulation found on the BudgWeb site

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The implementation and functioning of the Regulation will be reviewed and evaluated periodically through reporting.

To monitor the implementation of the regulation, the EU Centre (along with service providers and Coordinating Authorities) shall collect and analyse data relevant for measuring the effectiveness of the detection, reporting and removal obligations. Coordinating Authorities and hosting or interpersonal communication service providers will contribute to data collection and reporting on aspects falling into their realm of responsibility. The data collected by the EU Centre should be made available to the Coordinating Authorities and to the Commission to enable assessment of implementation.

The EU Centre shall publish annual transparency reports. These reports, to be made public and communicated to the Commission, should compile and analyse the information contained in the annual reports from relevant information service providers and Coordinating Authorities, complemented with other relevant sources, and include information on the activities of the Centre.

Drawing on the statistics and information gathered from the structured processes and transparency mechanisms provided for under this Regulation, the Commission should carry out an evaluation of this Regulation within five years of the date of its entry into force, and then every 5 years thereafter. The Commission will report on the findings of the evaluation to the European Parliament and the Council.

All Union agencies work under a strict monitoring system involving an internal control coordinator, the Internal Audit Service of the Commission, the Management Board, the Commission, the Court of Auditors and the Budgetary Authority. This system is reflected and laid down in Chapter 4 of the proposed regulation setting up the EU Centre to Prevent and Combat Child Sexual Abuse.

In accordance with the Joint Statement on the EU decentralised agencies, the annual work programme of the Centre shall comprise detailed objectives and expected results including performance indicators. The Centre will accompany its activities included in its working programme by key performance indicators. The activities of the Centre will be then measured against these indicators in the Annual Activity Report.

The annual work programme shall be coherent with the multi-annual work programme and both shall be included in an annual single programming document which shall be submitted to European Parliament, the Council and the Commission.

The Management Board of the EU Centre will be responsible for general orientation of the EU Centre's activities. An Executive Board will be responsible efficient and effective administrative, budgetary and operational management of the EU Centre, , and would adopt a budget estimate for the Centre before relaying same to the Commission.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Given that the majority of funding under this proposal relates to setting up a new EU Centre the EU budget financing will be implemented via indirect management.

An appropriate internal control strategy will be instituted to ensure that this budget is implemented in an effective and efficient manner.

Regarding ex-post controls, the EU Centre, as a decentralised agency, is subject to:

- internal audit by the Internal Audit Service of the Commission;

- annual reports by the European Court of Auditors, giving a statement of assurance as to the reliability of the annual accounts and the legality and regularity of the underlying transactions;

- annual discharge granted by the European Parliament;

- possible investigations conducted by OLAF to ensure, in particular, that the resources allocated to agencies are put to proper use.

As a Justice and Home Affairs Agency partner to DG HOME the EU Centre will be subject to DG HOME's Control Strategy on decentralised agencies to ensure reliable reporting in the framework of its Annual Activity Report. While decentralised agencies have full responsibility for the implementation of their budget, DG HOME is responsible for regular payment of annual contributions established by the Budgetary Authority.

The activities of the EU Centre will also be subject to the supervision of the Ombudsman in accordance with Article 228 of the Treaty.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

As the Centre will be a new EU Centre there is a risk that the recruitment process may not be on schedule, and will impact the Centre's operational capacity. Here support of the parent DG is crucial with respect to the roles of Authorising Officer and the exercise of powers conferred by the Staff Regulations on the appointing authority (AIPN)[62] until the Centre achieves full administrative autonomy.

Frequent meetings and regular contacts will be required between the parent DG and the Centre throughout the 5-year start-up phase to ensure that the Centre is autonomous and operational as scheduled.

A risk to the effective implementation of this proposal takes account of the Regulatory aim to improve and enhance detection, reporting and removal of online CSA across the Union, and where the wider application of the Regulation would be a significant increase in the volume and quality of reporting. Whereas the impact assessment has provided estimates on the number of reports expected, the actual amount of reports that the Centre will receive, and therefore the Centre's workload, may vary from the estimates.

The EU Centre will be required to implement an Internal Control Framework in line with the European Commission's Internal Control Framework. Information on the EU Centre's internal controls will be included in the Centre's annual reports.

An Internal Audit capability will be established to take account of risks specific to the operation of the EU Centre, and bring a systematic and disciplined approach to evaluate the effectiveness of risk management, control, and governance processes, and by issuing recommendations for their improvement.

DG HOME runs an annual risk management exercise to identify and assess potential high risks related to agencies' operations. Risks considered as critical are reported annually in DG HOME management plan and are accompanied by an action plan stating the mitigating action.

[62] C(2013) 3288 final of the 4th of June 4/6/2013

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

The ratio of "control costs/value of the related funds managed" is reported on by the Commission. DG HOME's 2020 Annual Activity Report reports 0.16% for this ratio in relation to Indirect Management Entrusted Entities and Decentralised Agencies.

2.3. Measures to prevent fraud and irregularities

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation.

Concerning the proposed EU Centre, DG HOME has developed and regularly updates an in-house anti-fraud strategy by reference to that provided by OLAF.

The proposed EU Centre, established as a decentralised agency would fall within scope of this strategy.

DG HOME, in its 2020 Annual Activity Report, concluded that the fraud prevention and detection processes provided reasonable assurance on the achievement of the internal control objectives.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
5	12 10 04 EU Centre to prevent and counter child sexual abuse “CSA”	Non-diff.	~~YES~~/NO	~~YES~~/NO	~~YES~~/NO	YES/NO

3.2. Estimated impact on expenditure *

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	5	Security and Defence

CSA			2022	2023	2024	2025[63]	2026	2027	**TOTAL MFF 2021-2027**	2028	2029	2030
Title 1:	Commitments	(1)				11,122	10,964	16,497	**38,583**	22,269	26,694	28,477
	Payments	(2)				11,122	10,964	16,497	**38,583**	22,269	26,694	28,477
Title 2:	Commitments	(1a)										
	Payments	(2a)										
Title 3:	Commitments	(3a)										
	Payments	(3b)										
TOTAL appropriations for CSA	Commitments	=1+1a +3a				11,122	10,964	16,497	**38,583**	22,269	26,694	28,477
	Payments	=2+2a+3 b				11,122	10,964	16,497	**38,583**	22,269	26,694	28,477

* **Note** : All calculations have been made on a Brussels-based assumption, as the seat of the EU Centre is not yet determined. The start-up period for the establishment of the EU Centre has been assessed to five years commencing in **2025**, with a full operational capacity by **end 2029**, with a total Centre expenditure figure of **€ 28,477 m** in year 2030 where the first full-year staff costing of full staff complement falls due. The overall budget of the Centre increases by 2% every year to cover inflation.

Heading of multiannual financial	**7**	'Administrative expenditure'

[63] Year 1 includes €5 million initial set-up costs for infrastructure (i.e. a database of indicators and building)

framework		

EUR million (to three decimal places)

		2022	2023	2024	2025	2026	2027	TOTAL
DG: HOME								
○ Human Resources		0,201	0,780	1,174	1,197	1,221	1,245	5,818
○ Other administrative expenditure		-	0,660	0,660	0,330	-	-	1,650
TOTAL DG HOME	Appropriations	0,201	1,440	1,834	1,527	1,221	1,245	7,468

		2022	2023	2024	2025	2026	2027	TOTAL
DG: HOME								
• Human Resources		0,201	0,780	1,174	1,197	1,221	1,245	5,818
• Other administrative expenditure		-	0,660	0,660	0,330	-	-	1,650
TOTAL DG HOME	Appropriations	0,201	1,440	1,834	1,527	1,221	1,245	7,468

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	0,201	1,440	1,834	1,527	1,221	1,245	7,468

EUR million (to three decimal places)

		2022	2023	2024	2025	2026	2027	TOTAL
TOTAL appropriations under HEADINGS 1 to 7 of the multiannual financial framework	Commitments	0,201	1,440	1,834	12,649	12,185	17,742	**46,051**
	Payments	0,201	1,440	1,834	12,649	12,185	17,742	**46,051**

3.2.2. Estimated impact on CSA body's appropriations

☐ The proposal/initiative does not require the use of operational appropriations

☒ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million

Indicate objectives & outputs			Year 2025		Year 2026		Year 2027		Total MFF 2021-27		Year 2028		Year 2029		Year 2030	
⇩	Type	Avg. cost	No.	Cost	No.	Cost	No.	Cost	No.	Cost	No.	Cost	No.	Cost	No.	Cost
SPECIFIC OBJECTIVE NO 1																
Effective detection, reporting and removal of online child sexual abuse																
- Output	Services and supports to public authorities and service providers			1,919		3,741		5,835		**11,494**		8,017		9,700		10,448
- Output	Communication and facilitation activities			0,411		0,802		1,250		**2,463**		1,718		2,079		2,239
- Output	Research, audit and investigative activities			0,411		0,802		1,250		**2,463**		1,718		2,079		2,239
Subtotal for specific objective N°1				**2,741**		**5,344**		**8,335**		**16,420**		**11,453**		**13,857**		**14,926**
SPECIFIC OBJECTIVE NO 2																
Improved legal certainty, ensuring the protection of fundamental rights, transparency and accountability																
- Output	Services and supports to assist implementation of the Regulation			0,582		1,136		1,771		**3,489**		2,434		2,944		3,172
- Output	Communication and facilitation activities			0,103		0,200		0,313		**0,616**		0,429		0,520		0,560
Subtotal for specific objective N°2				**0,685**		**1,336**		**2,084**		**4,105**		**2,863**		**3,464**		**3,732**
SPECIFIC OBJECTIVE NO 3																
Reduction in the proliferation and effects of child sexual abuse through increased coordination of efforts																
- Output	Services and supports to public authorities, providers and experts			6,887		2,999		4,255		**14,141**		5,567		6,561		6,873
- Output	Communication and facilitation activities			0,404		0,643		0,912		**1,959**		1,193		1,406		1,473
- Output	Research and evaluation– Victim assistance and Prevention			0,404		0,643		0,912		**1,959**		1,193		1,406		1,473
Subtotal for specific objective N°3				**7,696**		**4,284**		**6,078**		**18,058**		**7,953**		**9,373**		**9,819**
TOTAL				**11,122**		**10,964**		**16,497**		**38,583**		**22,269**		**26,694**		**28,477**

3.2.3. Estimated impact on CSA body's human resources

Summary

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☑ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	2025	2026	2027	Total MFF 2021-27	2028	2029	2030
Temporary agents (AD Grades)	1,166	3,229	5,547	**9,942**	7,956	9,919	11,037
Temporary agents (AST grades)	0,500	1,445	2,687	**4,631**	3,978	4,779	5,151
Contract staff	0,226	0,690	1,173	**2,089**	1,675	2,197	2,490
Seconded National Experts							
TOTAL	**1,892**	**5,363**	**9,407**	**16,662**	**13,610**	**16,895**	**18,677**

Staff requirements (FTE):

	2025	2026	2027	Total MFF 2021-27	2028	2029	2030
Temporary agents (AD Grades)	14	24	40	**60**	50	60	60
Temporary agents (AST grades)	6	11	20	**20**	25	28	28
Contract staff	5	10	15	**15**	20	25	25
Seconded National Experts							
TOTAL	**25**	**45**	**75**	**75**	**95**	**113**	**113**

For new recruitment, a calculation of 50% of the staff costs for the year 2022 and 50% of the additional staff costs for the following years has been applied.

3.2.4. Estimated requirements of human resources for the parent DG HOME

☐ The proposal/initiative does not require the use of human resources.

☑ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

		2022	2023	2024	2025	2026	2027
• **Establishment plan posts (officials and temporary staff)**							
20 01 02 01 and 20 01 02 02 (Headquarters and Commission's Representation Offices)		2	5	5	5	5	5
20 01 02 03 (Delegations)							
01 01 01 01 (Indirect research)							
10 01 05 01 (Direct research)							
○ **External staff (in Full Time Equivalent unit: FTE)**[64]							
20 02 01 (AC, END, INT from the 'global envelope')		1	4	4	4	4	4
20 02 03 (AC, AL, END, INT and JPD in the Delegations)							
Budget line(s) (specify) [65]	- at Headquarters[66]						
	- in Delegations						
01 01 01 02 (AC, END, INT – Indirect research)							
10 01 05 02 (AC, END, INT – Direct research)							
Other budget lines (specify)							
TOTAL		3	9	9	9	9	9

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

64 AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations.

65 Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

66 Mainly for the EU Cohesion Policy Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Maritime Fisheries and Aquaculture Fund (EMFAF).

Description of tasks to be carried out:

Officials and temporary staff	Commission staff drawn from DG HOME will work on 1) preparing the ground for the setting up of the Centre as involves the development of work programme and activity reporting, 2) preparing guidance on operational processes relating to the risk, detection, reporting and removal obligations under the legislation, 3) continuing to advance Centre related activities in the prevention and victim assistance areas, 4) providing administrative support for the setting-up of the Centre5) provide secretariat to the Centre's Management Board as established
External staff	External staff as incrementally recruited into the EU Centre as established will assume certain responsibilities from Commission staff, and operationalise the Centre's systems and processes as related to the detection, reporting and removal processes. Centre staff will also begin to assist with building networks of expertise across the span of its responsibilities. Details of the tasks of the EU Centre are included in Chapter 4, Section 2 of the above proposed Regulation.

Description of the calculation of cost for FTE units included in section 4 of the below Annex.

3.2.5. Compatibility with the current multiannual financial framework

☐ The proposal/initiative is compatible the current multiannual financial framework.

☒ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

The proposal includes additional financial and human resources for CSA Centre. The budgetary impact of the additional financial resources for CSA will be offset through a compensatory reduction from programmed spending under Heading 5.

☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[67].

3.2.6. Third-party contributions

☒ The proposal/initiative does not provide for co-financing by third parties.

The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[67] See Articles 12 and 13 of Council Regulation (EU, Euratom) No 2093/2020 of 17 December 2020 laying down the multiannual financial framework for the years 2021 to 2027.

3.3. Estimated impact on revenue

☒ The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

– ☐ on own resources

– ☐ on other revenue

– ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[68]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

[…]

Specify the method for calculating the impact on revenue.

[…]

[68] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

1. ANNEX TO THE LEGISLATIVE FINANCIAL STATEMENT

Name of the proposal/initiative:

Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

1. NUMBER and COST of HUMAN RESOURCES CONSIDERED NECESSARY
2. COST of OTHER ADMINISTRATIVE EXPENDITURE
3. TOTAL ADMINISTRATIVE COSTS
4. METHODS of CALCULATION USED for ESTIMATING COSTS

4.1. Human resources

4.2. Other administrative expenditure

This annex must accompany the legislative financial statement when the inter-services consultation is launched.

The data tables are used as a source for the tables contained in the legislative financial statement. They are strictly for internal use within the Commission.

1. Cost of human resources considered necessary

☐ The proposal/initiative does not require the use of human resources

☑ The proposal/initiative requires the use of human resources, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework		2022		2023		2024		2025		2026		2027				TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
O Establishment plan posts (officials and temporary staff)																	
20 01 02 01 - Headquarters and Representation offices	AD	2	0,157	5	0,560	5	0,817	5	0,833	5	0,850	5	0,867			5	4.084
	AST																
20 01 02 03 - Union Delegations	AD																
	AST																
O External staff [69]																	
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	0	0,000	3	0,130	3	0,265	3	0,271	3	0,276	3	0,282			3	1,224
	END	1	0,044	1	0,090	1	0,092	1	0,093	1	0,095	1	0,097			1	0,511
	INT																
20 02 03 – External personnel - Union Delegations	AC																
	AL																
	END																
	INT																
	JPD																
Other HR related budget lines (*specify*)																	
Subtotal HR – HEADING 7		3	0,201	9	0,780	9	1,174	9	1,197	9	1,221	9	1,245			9	5,818

[69] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT= agency staff; JPD= Junior Professionals in Delegations.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Outside HEADING 7 of the multiannual financial framework		2022		2023		2024		2025		2026		2027				TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
O Establishment plan posts (officials and temporary staff)																	
01 01 01 01 Indirect Research[70] 01 01 01 11 Direct Research Other (please specify)	AD																
	AST																
O External staff [71]																	
External staff from operational appropriations (former 'BA' lines).	- at Headquarters AC																
	- at Headquarters END																
	- at Headquarters INT																
	- in Union delegations AC																
	- in Union delegations AL																
	- in Union delegations END																
	- in Union delegations INT																
	- in Union delegations JPD																
01 01 01 02 Indirect Research 01 01 01 12 Direct research Other (please specify)[72]	AC																
	END																
	INT																
Other budget lines HR related (*specify*)																	
Subtotal HR – Outside HEADING 7																	
Total HR (all MFF Headings)		3	0,201	9	0,780	9	1,174	9	1,197	9	1,221	9	1,245			9	5,818

70 Please choose the relevant budget line, or specify another if necessary; in case more budget lines are concerned, staff should be differentiated by each budget line concerned

71 AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT= agency staff; JPD= Junior Professionals in Delegations.

72 Please choose the relevant budget line, or specify another if necessary; in case more budget lines are concerned, staff should be differentiated by each budget line concerned

Outside HEADING 7 of the multiannual financial framework		2022		2023		2024		2025		2026		2027				TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)																	
01 01 01 01 Indirect Research[73] 01 01 01 11 Direct Research Other (please specify)	AD																
	AST																
• External staff [74]																	
External staff from operational appropriations (former 'BA' lines).	- at Headquarters AC																
	- at Headquarters END																
	- at Headquarters INT																
	- in Union delegations AC																
	- in Union delegations AL																
	- in Union delegations END																
	- in Union delegations INT																
	- in Union delegations JPD																
01 01 01 02 Indirect Research 01 01 01 12 Direct research Other (please specify)[75]	AC																
	END																
	INT																
Other budget lines HR related (*specify*)																	
Subtotal HR – Outside HEADING 7																	
Total HR (all MFF Headings)		3	0,201	9	0,780	9	1,174	9	1,197	9	1,221	9	1,245			9	5,818

[73] Please choose the relevant budget line, or specify another if necessary; in case more budget lines are concerned, staff should be differentiated by each budget line concerned

[74] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT= agency staff; JPD= Junior Professionals in Delegations.

[75] Please choose the relevant budget line, or specify another if necessary; in case more budget lines are concerned, staff should be differentiated by each budget line concerned

2. Cost of other administrative expenditure

☐ The proposal/initiative does not require the use of administrative appropriations
☑ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework	2022	2023	2024	2025	2026	2027	Total
At headquarters or within EU territory:							
20 02 06 01 - Mission and representation expenses	0,000	0,200	0,200	0,100	0,000	0,000	0,500
20 02 06 02 - Conference and meeting costs	0,000	0,460	0,460	0,230	0,000	0,000	1,150
20 02 06 03 - Committees[76]							
20 02 06 04 Studies and consultations							
20 04 – IT expenditure (corporate)[77]							
Other budget lines non-HR related (*specify where necessary*)							
In Union delegations							
20 02 07 01 - Missions, conferences and representation expenses							
20 02 07 02 - Further training of staff							
20 03 05 – Infrastructure and logistics							
Other budget lines non-HR related (*specify where necessary*)							
Subtotal Other - HEADING 7 of the multiannual financial framework	0,000	0,660	0,660	0,330	0,000	0,000	1,650

[76] Specify the type of committee and the group to which it belongs.

[77] The opinion of DG DIGIT – IT Investments Team is required (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020, page 7)

EUR million (to three decimal places)

Outside HEADING 7 of the multiannual financial framework	2022	2023	2024	2025	2026	2027	Total
Expenditure on technical and administrative assistance (not including external staff) from operational appropriations (former 'BA' lines):							
- at Headquarters							
- in Union delegations							
Other management expenditure for research							
Policy IT expenditure on operational programmes[78]							
Corporate IT expenditure on operational programmes[79]							
Other budget lines non-HR related (*specify where necessary*)							
Sub-total Other – Outside HEADING 7 of the multiannual financial framework							
Total Other admin expenditure (all MFF Headings)	0,000	0,660	0,660	0,330	0,000	0,000	1,650

[78] The opinion of DG DIGIT – IT Investments Team is required (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020, page 7)

[79] This item includes local administrative systems and contributions to the co-financing of corporate IT systems (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020)

3. Total administrative costs (all Headings MFF)

EUR million (to three decimal places)

Summary	2022	2023	2024	2025	2026	2027	Total
Heading 7 - Human Resources	0,201	0,780	1,174	1,197	1,221	1,245	5,818
Heading 7 – Other administrative expenditure		0,660	0,660	0,330			1,650
Sub-total Heading 7							
Outside Heading 7 – Human Resources							
Outside Heading 7 – Other administrative expenditure							
Sub-total Other Headings							
TOTAL HEADING 7 and Outside HEADING 7	0,201	1,440	1,834	1,527	1,221	1,245	7,468

The administrative appropriations required will be met by the appropriations which are already assigned to management of the action and/or which have been redeployed, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of existing budgetary constraints.

4. Methods of calculation used to estimate costs

4.1 Human resources

This part sets out the method of calculation used to estimate the human resources considered necessary (workload assumptions, including specific jobs (Sysper 2 work profiles), staff categories and the corresponding average costs)

HEADING 7 of the multiannual financial framework
NB: The average costs for each category of staff at Headquarters are available on BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Officials and temporary staff The costs for the officials in the parent DG HOME have been calculated on the basis of the following average cost: EUR 157,000 per year (reference: Circular note of DG BUDGET to RUF, Ares(2021)7378761 of 30/11/2021), by applying an inflation increase of 2% per year from 2023. The LFS proposes to use additional human resources in the parent DG (DG HOME), that is to say an additional 9 FTEs on top of those already working in the Security in the Digital Age policy area on the wider EU CSA Strategy and in administrative support. The human resources are split as follows (in FTE): * 5 AD
• External staff The costs for the Seconded National Expert and Contractual Agents in the partner DG have been calculated on the basis of the following average cost: EUR 88,000 and EUR 85,000 per year, (reference: Circular note of DG BUDGET to RUF, Ares(2021)7378761 of 30/11/2021), by applying an inflation increase of 2% per year from 2023. The human resources are split as follows (in FTE): * 1 SNE and 3 AC

Outside HEADING 7 of the multiannual financial framework
○ Only posts financed from the research budget
○ External staff

Outside HEADING 7 of the multiannual financial framework
• Only posts financed from the research budget
• External staff

4.2 Other administrative expenditure

Give details of the method of calculation used for each budget line and in particular the underlying assumptions (e.g. number of meetings per year, average costs, etc.)

HEADING 7 of the multiannual financial framework
These costs will cover: operational activities (e.g. tech. meetings with stakeholders); support to expert networks (coord. activities, meetings); translation and interpretation; publishing and research dissemination; communication (incl. campaigns).

Outside HEADING 7 of the multiannual financial framework