Council of the European Union

Brussels, 15 September 2022
(OR. en)

12354/22

Interinstitutional File:
2022/0155(COD)

LIMITE

JAI 1165
ENFOPOL 456
CRIMORG 116
IXIM 217
DATAPROTECT 253
CYBER 294
COPEN 311
FREMP 180
TELECOM 366
COMPET 700
MI 656
CONSOM 217
DIGIT 161
CODEC 1290

NOTE

From:	Presidency
To:	Law Enforcement Working Party (Police)
No. prev. doc.:	9068/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Presidency compromise texts

Delegations will find in the Annex Presidency compromise texts on the above proposal. Changes to document 9068/22 are marked in **bold underline** and ~~strikethrough underline~~.

Compromise texts in Articles 1 to 24 are based on the discussions during the LEWP meetings of 5 and 20 July 2022 and delegations' written comments.

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

(Text with EEA relevance)

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

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

   It establishes, in particular:

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

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

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

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

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

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

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

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

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

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

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

(c) Directive 2010/13/EU;

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

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

4. This Regulation 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 ~~I~~ **II** 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[1];

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

(i) a hosting service;

(ii) an interpersonal communications service;

(iii) a software applications store;

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

(v) online search engines.

(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~~ **child** who uses a relevant information society service and who is a natural person below the age of 17 years

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

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

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

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

---

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

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

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

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

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

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

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

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

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

(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;

(x) 'online search engine' means online search engine as defined in Article 2(5) of Regulation (EU) 2019/1150 […on promoting fairness and transparency for business users of online intermediation services].

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:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 4

Risk mitigation

1. 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 to the manners in which the services covered by those provisions are offered and used.

Section 2
Detection obligations

Article 7

Issuance of detection orders

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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~~ **transmitted** in the language declared by the provider pursuant to Article 23(3).

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

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

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

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

3. Where the period of application of the detection order exceeds 12 months, or six months in the case of a detection order concerning the solicitation of children, the Coordinating Authority of establishment shall require the provider to report to it 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~~[3];

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

[3] Will be included in a recital.

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

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

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

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

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

3. The provider shall establish and operate an 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 **of upload, with associated date and time zone, and port number**;

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

   (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.~~

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

2. The provider shall execute the removal order as soon as possible and in any event within 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 **competent** ~~judicial or independent administrative~~ authority issuing the removal order and authentication of the removal order by that authority;

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

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

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

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

(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~~ **competent** authority issuing the removal order;

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

3a. **If the competent authority issuing the removal order is not designated as the Coordinating Authority of its Member State, it shall address a copy of the removal order to its Coordinating Authority without undue delay. The Coordinating Authority shall scrutinise the removal order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter or the EU law. If it notes such an infringement, it can recommend withdrawing the removal order to the competent authority. If the competent autority maintains the removal order, the Coordinating Authority can refer to a judicial authority.**

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

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

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

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

In such a case:

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

The competent ~~That judicial authority or independent administrative~~ authority may decide to extend the time period referred to in the second subparagraph, point (a), by a further time period of maximum six weeks, where and to the extent the non-disclosure continues to be necessary. In that case, **the competent** ~~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 **competent authority** ~~Coordinating Authority of establishment~~ shall have the power ~~to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State~~ to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing ~~known~~ child sexual abuse material.

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

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

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

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

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

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

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

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

4. The **competent authority** ~~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,~~ **to** the need to protect the rights of the victims and the existence and implementation by the provider of a policy to address the risk of such dissemination;

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

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

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

If the competent authority issuing the blocking order is not designated as the Coordinating Authority of its Member State, it shall address a copy of the blocking order to its Coordinating Authority without undue delay. The Coordinating Authority shall scrutinise the blocking order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter or the EU law. If it notes such an infringement, it can recommend withdrawing the blocking order to the competent authority. If the competent autority maintains the blocking order, the Coordinating Authority can refer to the judicial autority.

~~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 **competent authority** ~~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) **In case of known child sexual abuse material** 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 **competent** ~~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). **Where relevant, the blocking order shall also be communicated to the providers of online search engines under the jurisdiction of the competent authority.**

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

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

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

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

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

Section 5a
Delisting obligations

Article 18a

Delisting orders

1. The competent authority shall issue a delisting order addressed to the provider of online search engines, when the conditions indicated in paragraph 3 are met, under the jurisdiction of the Member State to take reasonable measures to delist a particular website indicating specific items of child sexual abuse material.

2. Before requesting the provider of online search engines to take such measures, the competent authority shall inform the provider of its intention specifying the main elements of the content of the delisting order and the reasons to delist a particular website. It shall afford the provider the opportunity to comment on that information, within a reasonable time period set by that authority.

3. The competent authority shall issue a delisting order, where it considers that the following conditions are met:

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

(b) the website indicates, in a sufficiently reliable manner, child sexual abuse material.

If the competent authority issuing the delisting order is not designated as the Coordinating Authority of its Member State, it shall address a copy of the delisting order to its Coordinating Authority without undue delay. The Coordinating Authority shall scrutinise the delisting in order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter or the EU law. If it notes such an infringement, it can recommend withdrawing the delisting order to the competent authority. If the competent autority maintains the delisting order, the Coordinating Authority can refer to a judicial autority.

Article 18b

Additional rules regarding delisting orders

1. The competent authority shall issue delisting orders referred to in Article 18a using the template set out in annex …. Delisting orders shall include:

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

(b) the specific service in respect of which the delisting order is issued;

(e) the start date of the delisting;

(f) a sufficiently detailed statement of reasons explaining the delisting order;

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

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

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

2. The competent authority that issues the delisting order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

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

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

5. If the provider cannot execute the delisting order because it contains manifest errors or does not contain sufficient information for its execution, the provider shall, without undue delay, request the necessary clarification 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 …….. where necessary to improve the templates in view of relevant technological developments or practical experiences gained.

Article 18c

Redress, information and reporting of delisting orders

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

2. When the delisting order becomes final, the competent authority 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 delisting order shall become final upon the expiry of the time period for appeal where no appeal has been lodged in accordance with national law or upon confirmation of the delisting order following an appeal.

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, blocking or reporting online child sexual abuse in accordance with those requirements.

Article 20

Victims' right to information

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

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

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

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

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

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

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

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

   (b) the date of the report;

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

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

Article 21

Victims' right of assistance and support for removal

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

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

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

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

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

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

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

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

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

Article 22

Preservation of information

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

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

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

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

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

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

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

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

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

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

Article 23

Points of contact

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

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.