

Legal questionnaire completed by K&L Gates • December 2025

This document contains responses from the law firm listed above to a questionnaire distributed by NCMEC (questions are in **bold text**). Responses to the questionnaire may be limited to officially enacted legislation; it is possible that actual practice or enforcement of the law varies, and relevant court rulings or case law may also differ from legislative text. Responses have been reformatted and may have been slightly edited for clarity. Furthermore, responses may include commentary, paraphrasing, and unofficial translations of source material (e.g., national legislation) originally produced in other languages. Only official source documents in official languages should be relied upon as legally binding. This document serves to inform further research and does not constitute legal advice from NCMEC or the listed law firm.

Note Regarding Regulations and Directives:

Please note that this questionnaire includes references to two particular types of EU legislation – “Regulation” and “Directive”. In the EU legal context, **Regulations** have *direct effect* in the Member States, meaning they apply automatically in all Member States without the need for national implementation – i.e. they effectively become part of local law (subject to the relevant discretions given to the Member States (if any) as specified in the Regulation in question). By contrast, **Directives** must be **transposed into national law** by each Member State, which (depending on how the relevant Member State transposes it) involves enacting or amending national legislation to give effect to the requirements set out in the Directive.

As a result, while Directives set a common framework across the EU, the **practical application of their requirements can vary** depending on each Member State’s legal system and the degree of harmonisation mandated in the particular Directive. The core obligations remain consistent, but **national transposition may lead to differences** in e.g. interpretation, scope or the level of protection – for a “maximum harmonisation” Directive, the Member States are generally not permitted to transpose it in a way that goes beyond the requirements set out in the Directive; for a “minimum harmonisation” Directive, the Member States may at their discretion go beyond the requirements in the Directive (commonly known as “goldplating”).

1. What laws and regulations contain legal definitions of the following terms or corresponding terms in your local jurisdiction (links to existing U.S. legal definitions are included, where relevant, as background for comparison – please include definitions of any corresponding terms in your jurisdiction):

a. child or minor (18 U.S.C. 2256(1), <https://www.law.cornell.edu/uscode/text/18/2256>)

The European Union as a jurisdiction does not have one single or universal definition of “child” or “minor” used across all its instruments. However, multiple Directives contain specific definitions of these terms that apply to their respective scopes.

Definition of a “Child”

Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 3 of the Lanzarote Convention



defines a “child” as “*a person under the age of 18 years*”. Relevant EU legislation references and aligns with its provisions.

The definitions of “child” in EU legislation are found in Directives relating to employment laws and criminal laws. The criminal law Directives all define “child” as any person below the age of 18, however, the employment Directive defines “child” as any young person under 15 or still subject to compulsory full-time schooling.

Article 3(b) of [Directive 94/33/EC of 22 June 1994 on the protection of young people at work](#) defines a “child” as “*any young person of less than 15 years of age or who is still subject to compulsory full-time schooling under national law*”. This Directive creates a complete prohibition of work below 15, while regulated employment between 15-18 requires special protections. Consequently, a 16-year-old may be legally employed under this Directive (with appropriate protections) while simultaneously being protected as a “child” under the Lanzarote Convention.

Article 2(6) of [Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA \(“Anti-Trafficking Directive”\)](#) defines a “child” as “*any person below 18 years of age*”.

Article 2 of [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 \(“CSAD”\)](#) defines a “child” as “*any person below the age of 18 years*”.

Article 2 of [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 \(“Victims’ Right Directive” or “VRD”\)](#) defines “child” as “*any person below 18 years of age*”.

Article 3(1) of [Directive \(EU\) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings](#) defines a “child” as “*a person below the age of 18*”. This Directive also establishes that where a person's age remains in doubt, that person shall be presumed to be a child (introductory paragraph (13)).

Definition of a “Minor”

The definitions of “minor” in EU legislation are found in Regulations and Directives relating to immigration and asylum laws and define a “minor” as a person below the age of 18 years.

Article 2(k) of [Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted \(recast\)](#) defines a “minor” as “*a third-country national or stateless person below the age of 18 years*”.



Article 3(10) of [Regulation \(EU\) 2024/1347 of the European Parliament and of the Council of 14 May 2024 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection and for the content of the protection granted, amending Council Directive 2003/109/EC and repealing Directive 2011/95/EU of the European Parliament and of the Council](#) defines a “minor” as a *“a third-country national or stateless person below the age of 18 years”*.

Article 3(6) of [Regulation \(EU\) 2024/1348 of the European Parliament and of the Council of 14 May 2024 establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU](#) defines a “minor” as a *“a third-country national or stateless person below the age of 18 years”*.

Other relevant definitions

Additional EU Directives contain related age-based definitions that are relevant to the protection and legal status of young persons.

Article 3 of [Directive 94/33/EC of 22 June 1994 on the protection of young people at work](#) contains the following relevant definitions:

- In Article 3(a), “Young person” is defined as *“any person under 18 years of age”*.
- In Article 3(c), “Adolescent” is defined as *“any young person of at least 15 years of age but less than 18 years of age who is no longer subject to compulsory full-time schooling under national law”*.

Article 2(f) [Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification](#) defines an “unaccompanied minor” as a *“third country nationals or stateless persons below the age of eighteen, who arrive on the territory of the Member States unaccompanied by an adult responsible by law or custom, and for as long as they are not effectively taken into the care of such a person, or minors who are left unaccompanied after they entered the territory of the Member States.”* Article 4(1) refers to “minor children” as must being *“below the age of majority set by the law of the Member State concerned and must not be married”*.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“**Proposal**”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

Pursuant to Article 2 of the Proposal, a “child” is defined as “any natural person below the age of 18 years”, in line with existing EU law and international standards; the positions adopted by the European Parliament and the Council do not propose to change this definition.



Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by [Regulation \(EU\) 2024/1307](#) to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

b. child sexual exploitation (Missing Children’s Assistance Act of 2023, Section 2, (a)(1)(9), <https://www.congress.gov/118/bills/s2051/BILLS-118s2051es.pdf>)

Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 3 of the Lanzarote Convention states “sexual exploitation and sexual abuse of children” “*shall include the behaviour as referred to in Articles 18 to 23 of this Convention*”, which we set out below.

Article 18 – Sexual abuse

1. *Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:*
 - a) *engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities;*
 - b) *engaging in sexual activities with a child where:*
 - *use is made of coercion, force or threats; or*
 - *abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or*
 - *abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.*
2. *For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.*
3. *The provisions of paragraph 1.a are not intended to govern consensual sexual activities between minors*

Article 19 – Offences concerning child prostitution

1. *Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:*
 - a) *recruiting a child into prostitution or causing a child to participate in prostitution;*
 - b) *coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes;*
 - c) *having recourse to child prostitution.*
2. *For the purpose of the present article, the term “child prostitution” shall mean the fact of using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person.*

Article 20 – Offences concerning child pornography



1. *Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:*
 - a) *producing child pornography;*
 - b) *offering or making available child pornography;*
 - c) *distributing or transmitting child pornography;*
 - d) *procuring child pornography for oneself or for another person;*
 - e) *possessing child pornography;*
 - f) *knowingly obtaining access, through information and communication technologies, to child pornography.*
2. *For the purpose of the present article, the term “child pornography” shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.*
3. *Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:*
 - *consisting exclusively of simulated representations or realistic images of a non-existent child;*
 - *involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.*
4. *Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.*

Article 21 – Offences concerning the participation of a child in pornographic performances

1. *Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:*
 - a) *recruiting a child into participating in pornographic performances or causing a child to participate in such performances;*
 - b) *coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes;*
 - c) *knowingly attending pornographic performances involving the participation of children.*
2. *Each Party may reserve the right to limit the application of paragraph 1.c to cases where children have been recruited or coerced in conformity with paragraph 1.a or b.*

Article 22 – Corruption of children

Each Party shall take the necessary legislative or other measures to criminalise the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.

Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

While [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 (“CSAD”) does not contain a definition of “child sexual exploitation”, Article 4 lists several cases of “Offences concerning sexual exploitation” of a child, including:

- “2. *Causing or recruiting a child to participate in pornographic performances, or profiting from or otherwise exploiting a child for such purposes [...]*
3. *Coercing or forcing a child to participate in pornographic performances, or threatening a child for such purposes [...]*
4. *Knowingly attending pornographic performances involving the participation of a child [...]*
5. *Causing or recruiting a child to participate in child prostitution, or profiting from or otherwise exploiting a child for such purposes [...]*
6. *Coercing or forcing a child into child prostitution, or threatening a child for such purposes [...]*
7. *Engaging in sexual activities with a child, where recourse is made to child prostitution [...]*”

Article 2(d) of CSAD includes a related definition of “child prostitution”, which means “*the use of a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether that payment, promise or consideration is made to the child or to a third party*”.

While Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (“Anti-Trafficking Directive”) does not contain a definition of “child sexual exploitation”, Article 2(1) describes “Offences concerning trafficking in human beings”, which includes “*the recruitment, transportation, transfer, harbouring or reception of persons, including the exchange or transfer of control over those persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation*”. (Emphasis added.)

Article 2(3) of the Anti-Trafficking Directive defines “exploitation” to include “*the exploitation of the prostitution of others or other forms of sexual exploitation*”. Where the victim is a child (i.e., a person under 18 years), Articles 2(5) and 2(6) provide that it is sufficient to establish the offence of trafficking if any of the listed acts (e.g., recruitment, transportation, transfer, harbouring or reception) has occurred for the purpose of exploitation; there is no requirement to prove coercion, deception, abuse of vulnerability, or any other ‘means’ element.

c. **sexually explicit conduct (18 U.S.C. 2256(2), <https://www.law.cornell.edu/uscode/text/18/2256>)**

EU legislation does not have a definition of “sexually explicit conduct”.

Although the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the “Lanzarote Convention”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU



Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 20(2) of the Lanzarote Convention states “child pornography” “*shall mean any material that visually depicts a child engaged in real or simulated **sexually explicit conduct** or any depiction of a child’s sexual organs for primarily sexual purposes.*” (emphasis added), but does not define what “sexually explicit conduct” means.

“Sexually explicit conduct” is also mentioned within descriptions of prohibited content under the [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 \(“CSAD”\)](#), notably under the definition of “child pornography”. Article 2(c)(i) defines “child pornography” as “*any material that visually depicts a child engaged in real or simulated **sexually explicit conduct**”.* (Emphasis added.)

d. **child sexual abuse (18 U.S.C. 2243(a), <https://www.law.cornell.edu/uscode/text/18/2243>)**

Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 3 of the Lanzarote Convention states “sexual exploitation and sexual abuse of children” “*shall include the behaviour as referred to in Articles 18 to 23 of this Convention*”, which we set out below.

Article 18 – Sexual abuse

1. *Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:*
 - a) *engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities;*
 - b) *engaging in sexual activities with a child where:*
 - *use is made of coercion, force or threats; or*
 - *abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or*
 - *abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.*
2. *For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.*
3. *The provisions of paragraph 1.a are not intended to govern consensual sexual activities between minors*

Article 19 – Offences concerning child prostitution

1. *Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:*
 - a) *recruiting a child into prostitution or causing a child to participate in prostitution;*
 - b) *coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes;*
 - c) *having recourse to child prostitution.*



2. For the purpose of the present article, the term “child prostitution” shall mean the fact of using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person.

Article 20 – Offences concerning child pornography

1. Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:
 - a) producing child pornography;
 - b) offering or making available child pornography;
 - c) distributing or transmitting child pornography;
 - d) procuring child pornography for oneself or for another person;
 - e) possessing child pornography;
 - f) knowingly obtaining access, through information and communication technologies, to child pornography.
2. For the purpose of the present article, the term “child pornography” shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:
 - consisting exclusively of simulated representations or realistic images of a non-existent child;
 - involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.
4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

Article 21 – Offences concerning the participation of a child in pornographic performances

1. Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:
 - a) recruiting a child into participating in pornographic performances or causing a child to participate in such performances;
 - b) coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes;
 - c) knowingly attending pornographic performances involving the participation of children.
2. Each Party may reserve the right to limit the application of paragraph 1.c to cases where children have been recruited or coerced in conformity with paragraph 1.a or b.

Article 22 – Corruption of children

Each Party shall take the necessary legislative or other measures to criminalise the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.

Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for



the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

Article 3 of the [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 \(“CSAD”\)](#) provides several examples of “offences concerning sexual abuse”, including:

- “2. Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities, even without having to participate [...]*
- 3. Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual abuse, even without having to participate, [...]*
- 4. Engaging in sexual activities with a child who has not reached the age of sexual consent [...]*
- 5. Engaging in sexual activities with a child, where:*
 - (i) abuse is made of a recognised position of trust, authority or influence over the child [...]*
 - (ii) abuse is made of a particularly vulnerable situation of the child, in particular because of a mental or physical disability or a situation of dependence [...]*
 - (iii) use is made of coercion, force or threats [...]*
- 6. Coercing, forcing or threatening a child into sexual activities with a third party [...]*”

For the purposes of this section, Article 2(b) of CSAD, defines the “age of sexual consent” as *“the age below which, in accordance with national law, it is prohibited to engage in sexual activities with a child”*.

e. child pornography or child sexual abuse material (CSAM) (18 U.S.C. 2256(8), <https://www.law.cornell.edu/uscode/text/18/2256>)

Child pornography

Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 20(2) of the Lanzarote Convention states “child pornography” *“shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.”* Articles 20 and 21 sets out a number of offences concerning child pornography (see above).

Article 2(c) of the [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 \(“CSAD”\)](#) defines “child pornography” as:

- “(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;*
- (ii) any depiction of the sexual organs of a child for primarily sexual purposes;*
- (iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any*



- person appearing to be a child, for primarily sexual purposes; or*
(iv) *realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes’.*

Article 2(e) of CSAD defines “pornographic performance” as, “*a live exhibition aimed at an audience, including by means of information and communication technology, of:*

- (i) *a child engaged in real or simulated sexually explicit conduct; or*
(ii) *the sexual organs of a child for primarily sexual purposes.”*

Child sexual abuse material

EU legislation does not have a definition of the exact term “child sexual abuse material” or “CSAM”.

There is a term “online child sexual abuse material” under Article 2 of the [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 \(the “Interim Regulation”\)](#) which says “*online child sexual abuse material’ means: (a) child pornography as defined in Article 2, point (c), of Directive 2011/93/EU [i.e. CSAD]; (b) pornographic performance as defined in Article 2, point (e), of Directive 2011/93/EU’.* See above on the definition of child pornography under CSAD.

Pending Legislation – the proposed CSAM Regulation

Child Sexual Abuse Material

Article 2(l) of Proposal (COM(2022) 209) (procedure 2022/0155(COD)) (the “**Proposal**”) defines “child sexual abuse material” (CSAM) as material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU (“**CSAD**”). The proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The Proposal distinguishes between “known child sexual abuse material” and “new child sexual abuse material.”

Pursuant to Article 2(1)(m) of the Proposal, “known CSAM” is content that corresponds to a detection indicator generated from confirmed CSAM and included on an official indicator list. A detection indicator is a machine-readable fingerprint (e.g., cryptographic or perceptual hash, or comparable content signature) derived from a file that has already been verified as CSAM; it is one-way and cannot be used to reconstruct the underlying content. The EU Centre on Child Sexual Abuse (as envisaged to be established in the Proposal) would curate and distribute the indicator list/database to eligible providers and competent authorities. Providers may compare fingerprints of content they lawfully process to that list; a match is then subject to human verification prior to removal/disablement of the CSAM content and reporting in accordance with the Proposal or other applicable laws. “New CSAM” is content not yet represented on the indicator list but which is, in the first instance, identified by a



provider (e.g., via classifier tools, trusted-flagger reports or moderation) as reasonably suspected to meet the cross-referenced legal definition; once an authorised entity (e.g., the EU Centre or a competent authority) verifies that the content does meet that definition, an indicator is generated and added to the list so that subsequent occurrences are treated as known CSAM across services (Article 2(1)(n)).

Child Pornography

The Proposal does not define “child pornography” but cross-references to Article 2, points (c) and (e) of CSAD.

Neither the European Parliament nor the Council have proposed to change these definitions or this approach in their respective positions.

- f. **computer-generated images or videos of child pornography or CSAM (created by artificial intelligence or morphed) (18 U.S.C. 2256(8) & (9), <https://www.law.cornell.edu/uscode/text/18/2256>)**

EU legislation does not have definitions of:

- “computer-generated images of child pornography”;
- “computer-generated videos of child pornography”;
- “computer-generated images of CSAM”; or
- “computer-generated videos of CSAM”,

whether created by artificial intelligence or morphed.

Article 2(c) of the [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 \(“CSAD”\)](#) contains a definition of “child pornography” which includes (emphasis added):

*“(i) any material that visually depicts a child engaged in real **or simulated** sexually explicit conduct;*

[...]

*“(iii) any material that visually depicts any person appearing to be a child engaged in real **or simulated** sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or*

*“(iv) **realistic images** of a child engaged in sexually explicit conduct or **realistic images** of the sexual organs of a child, for primarily sexual purposes”.*

In other words, CSAD does not require the material to involve a real child or be an actual photograph.

[Regulation \(EU\) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations \(EC\) No 300/2008, \(EU\) No 167/2013, \(EU\) No 168/2013, \(EU\) 2018/858, \(EU\) 2018/1139 and \(EU\) 2019/2144 and Directives 2014/90/EU, \(EU\) 2016/797 and \(EU\) 2020/1828 \(Artificial Intelligence Act\)](#) also known as the “**EU Artificial Intelligence Act**” was adopted on 13 June 2024. It was published in the Official Journal of the European Union on 12 July 2024 and entered into force on 1 August 2024. The EU Artificial Intelligence Act introduces a risk-based framework, classifying AI systems as unacceptable, high risk, limited risk, or minimal



risk, with obligations that vary according to the potential impact on health, safety, or fundamental rights. The EU Artificial Intelligence Act introduces staggered application dates for its provisions:

- The first set of obligations, including prohibitions on certain AI practices, became applicable on 2 February 2025;
- Governance and general-purpose AI requirements apply from 2 August 2025;
- The majority of the Act's provisions become effective from 2 August 2026; and
- The remaining obligations concerning certain high-risk AI systems will apply from 2 August 2027.

While the EU Artificial Intelligence Act itself does not create new criminal offences relating to child pornography or CSAM, the prohibitions in Article 5(1)(b) include certain AI systems that exploit vulnerabilities due to age, particularly those designed to materially distort a person's behaviour in a manner that causes harm.

Under Article 9(8) of the EU Artificial Intelligence Act, when setting up and applying the required risk management system, providers of a high-risk AI system must assess whether, given its intended purpose, the system is likely to have an adverse impact on persons under 18 and, where relevant, other vulnerable groups, and take this into account in the risk management process.

- g. **enticement or grooming (encouraging, persuading, or coercing a child to engage in sexual activity or to create child pornography or CSAM) (18 U.S.C. 2422(b), <https://www.law.cornell.edu/uscode/text/18/2422>)**

EU legislation does not have definitions of “enticement” or “grooming”.

Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 23 of the Lanzarote Convention criminalises the “*intentional proposal, through information and communication technologies, of an adult to meet a child...*” for sexual purposes. This could capture “enticement” or “grooming”.

Article 6 of [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 \(“CSAD”\)](#) states that Member States shall take the necessary measures to ensure that the following intentional conduct is punishable (emphasis added):

“the proposal, by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent, for the purpose of committing any of the offences referred to in Article 3(4) [engaging in sexual activities with a child who has not reached the age of sexual consent] and Article 5(6) [production of child pornography], where that proposal was followed by material acts leading to such a meeting”.

In other words, the intentional proposal by an adult to meet a child for sexual purposes, followed by material acts leading to such a meeting, are punishable. This could capture



“enticement” or “grooming”.

Article 2 of [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 (the **Interim Regulation**) has a term “solicitation of children”, which is defined by reference to Article 6 of CSAD.

Pending Legislation – the proposed CSAM Regulation

Proposal (COM(2022) 209) (procedure 2022/0155(COD)) (“**Proposal**”) does not contain a separate definition for “enticement” or “grooming”, however, Article 2(o) defines “solicitation of children” by reference to the definition of “solicitation of children for sexual purposes as referred to in Article 6 of Directive 2011/93/EU (“**CSAD**”).

This approach, derived from existing EU criminal-law definitions, is retained in the positions of both the European Parliament and the Council; the final wording remains subject to trilogue agreement.

h. legal age of consent for sexual activity – are there laws and regulations, if so, what ages are specified?

There is no fixed legal age of consent for sexual activity within EU legislation.

Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. Article 18 of the Lanzarote Convention obliges parties to criminalise sexual activities with a child where there is coercion, abuse of authority, or a vulnerable situation, and requires States to set a minimum legal age for sexual activity, but allows each State to determine at what age this is set.

Article 2(b) of [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 \(“**CSAD**”\) defines the “age of sexual consent” as the “*the age below which, in accordance with national law, it is prohibited to engage in sexual activities with a child*”.](#)

Therefore, the legal age of consent for sexual activity is up to the local law of each Member State.

i. Sextortion (extorting money or sexual favors from a child by threatening to share sexually explicit, child pornography or CSAM images of the child) (Missing Children’s Assistance Act of 2023, Section 2, (a)(1)(8), <https://www.congress.gov/118/bills/s2051/BILLS-118s2051es.pdf>)

EU legislation does not have a definition of “sextortion”.



Although the [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse](#) (the “**Lanzarote Convention**”) is a Council of Europe treaty and not EU legislation per se, it is directly relevant to the EU legal framework as all EU Member States have ratified it, creating binding international obligations and the Lanzarote Convention acts as a minimum standard across Europe. There is no explicit use of the word “sextortion” but Articles 18 – 20, and 23 (see above) criminalise recruiting, coercing, or exploiting a child for prostitution and sexual abuse, including threats or blackmail involving images.

Articles 3(5)(iii) and (6) of [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](#) (“**CSAD**”) criminalises the act of engaging in sexual activities with a child where “*use is made of coercion, force or threats*” and activities encompassing “*coercing, forcing or threatening a child into sexual activities with a third party*”. Furthermore, Articles 4(3) and 6 criminalises the act of “*coercing or forcing a child to participate in pornographic performances, or threatening a child for such purposes*” and of “*coercing or forcing a child into child prostitution, or threatening a child for such purposes*”.

The abovementioned articles of the Lanzarote Convention and CSAD could capture the term “sextortion”.

Resources:

- [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), “**CSAD**”.
- [Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA](#), (OJ L 101 15.4.2011, p. 1), “**Anti-Trafficking Directive**”.
- [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](#), (OJ L 315, 14.11.2012, p. 57–73), “**Victims’ Right Directive**” – VRD.
- [Council Directive 94/33/EC of 22 June 1994 on the protection of young people at work](#) (OJ L 216, 20.8.1994, p. 12–20), “**Young Workers Directive**”.
- [Directive \(EU\) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings](#) (OJ L 132, 21.5.2016, p. 1–20).
- [Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification](#) (OJ L 251, 3.10.2003, p. 12–18).
- [Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted \(recast\)](#) (OJ L 337, 20.12.2011, p. 9–26).
- [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.

- [Regulation \(EU\) 2024/1347](#) of the European Parliament and of the Council of 14 May 2024 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection and for the content of the protection granted, amending Council Directive 2003/109/EC and repealing Directive 2011/95/EU of the European Parliament and of the Council (OJ L 6, 11.6.2024, p. 1).
- [Regulation \(EU\) 2024/1348](#) of the European Parliament and of the Council of 14 May 2024 establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU (OJ L 6, 11.6.2024, p. 104).
- [Regulation \(EU\) 2024/1689](#) of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L 211, 12.7.2024, p. 1), “**EU Artificial Intelligence Act**”.
- [Council of Europe Convention](#) on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, Lanzarote Convention) (signed 25 October 2007, entered into force 1 July 2010).

2. Please explain any legal or regulatory requirement or recommendation for Online Platforms to undertake any of the following activities on their systems to protect children online from sexual exploitation:

a. review, screen, moderate, or detect content to identify child pornography or CSAM content

Digital Services Act

[Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”), which regulates (amongst others) Online Platforms and has been applicable since February 2024, does not **mandate** proactive screening or detection (automated or otherwise) of child pornography/CSAM content. Article 8 states there is “*no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers*”. Please note, this does not prevent Online Platforms voluntarily implementing detection systems without losing liability protection (Article 7 of the DSA).

However, obligations imposed on Online Platforms (which vary depending on primarily the size of the platform) relating to transparency, risk assessment/mitigation, and removal of illegal content are understood to have the practical effect of imposing indirect obligations on Online Platforms, particularly Very Large Online Platforms (“**VLOPs**”) or Very Large Online Search Engines (“**VLOSEs**”), to have in place “content moderation” procedures. We summarise these obligations below:

- Pursuant to Articles 15, 24 and 42, all service providers subject to the DSA (including Online Platforms) must publish annual reports on their DSA activities. The required content of the annual report varies depending on the service provider’s categorisation



(e.g., if they are an intermediary, hosting provider, or Online Platform). As relevant: for all service providers, the content must include information on their “content moderation” activities including the use of automated tools; for VLOPs and VLOSEs, the reports must be published twice yearly and the content must also include information on content moderation resources, system risk assessments and corresponding mitigation measures.

- Pursuant to Article 14, all service providers subject to the DSA (including Online Platforms) must include in their terms and conditions, required information which includes information on their content moderation policy and procedure.
- Pursuant to Article 34, VLOPs and VLOSEs must assess four required categories of systemic risks – the first category being the risk of dissemination of illegal content, and when conducting risk assessment, they must consider how various factors including content moderation mechanisms influence any of the specified systemic risks, and risk assessments must consider “*the protection of...minors*”. Recital 80 specifically references “child sexual abuse material” as an example of “illegal content”, when explaining the first systemic risk category.
- Pursuant to Article 35, VLOPs and VLOSEs must take action to mitigate identified systemic risks, including: “*adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified*”; VLOPs “*shall put in place reasonable, proportionate and effective mitigation measures (...) with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: (...) taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate*”.
- Pursuant to Article 42, VLOPs and VLOSEs must also publish half-yearly transparency reports which must include, amongst others, information on the human resources dedicated to content moderation, the accuracy and error rates of automated moderation (if used).
- Pursuant to Article 16(1), under what is known as the notice-and-action mechanism, “*providers of hosting services [i.e., an Online Platform] shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means*”.
- Pursuant to Article 28(1), online platforms that are accessible to minors must “*put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service*”.

“Content moderation” is defined in Article 3(t) as “*the activities, whether automated or not, ... that are aimed, in particular, at detecting, identifying and addressing illegal content ..., including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient’s account*”.

“Illegal content” is defined broadly in Article 3(h) to mean “*any information ... not in compliance with Union law or the law of any Member State which is in compliance with Union*”.



law, irrespective of the precise subject matter or nature of that law'. Various recitals of the DSA references child pornography or CSAM when explaining the concept of "illegal content", for example, Recital 12 states that illustrative examples of "illegal content" include images depicting child sexual abuse; Recital 119 refers to removal of webpages containing or disseminating "child pornography". Please note, recitals are not binding legal provisions. Furthermore, [Directive 2011/93/EU \(Child Sexual Abuse Directive\)](#) requires all Member States to criminalise the production, distribution, possession, and access to child pornography. Such material therefore constitutes "illegal content" under the DSA.

In addition, on 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors ("[Guidelines](#)"). In Section 6.7 of the Guidelines, the European Commission considers that Online Platforms accessible to minors should put in place a number of specified measures including:

- Establish moderation policies and procedures that set out how content and behaviour that is harmful for the privacy, safety and security of minors is detected and how it will be moderated aiming at limiting minors' exposure to harmful content.
- Ensure that content moderation teams are well-trained and resourced and that moderation mechanisms are active and functioning at all times (24 hours a day, 7 days a week) to deliver effective moderation, including at least one employee who is on call to respond to urgent requests and emergencies at all times.

While the European Commission states expressly in the Guidelines that these do not impose a general obligation on service providers subject to the DSA to monitor content (paragraph 74), it sets out immediately below that statement a "Poor practice" example where a hypothetical social media platform does not have any "*robust content moderation mechanisms to detect and prevent the upload of harmful and explicit content, including child sexual abuse material*".

For completeness, under the DSA, Online Platforms are defined as "*a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation*" (Article 3(i) of the [DSA](#)).

VLOPs, defined by Article 33 of the DSA, means online platforms that have "*a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms*". Please see [here](#) for the latest list of designated VLOPs. As of July 2025, the list includes the following platforms: AliExpress, Amazon (Amazon Store), Apple (App Store), Aylo Freesites (Pornhub), Booking.com, Google (Google Search, Google Play, Google Shopping, Youtube), Infinite Services (Shein), MSFT (Linkedin, Bing), Meta (Facebook, Instagram), NKL Associates s.r.o. (XNXX), Pinterest Europe, Snapchat, Technius (Stripchat), TikTok, Twitter (X), Whaleco Technology (Temu), WebGroup (XVideos), Wikipedia, and Zalando).

The European Commission has opened formal DSA proceedings against Meta (Facebook/Instagram) and X regarding suspected breaches in areas that include risk



management, protection of minors, content moderation, and transparency obligations. See the European Commission's press releases on the investigations into [Facebook, Instagram](#) and [X](#).

Audiovisual Media Services Directive (AVMSD) for Video-Sharing Platforms

The revised [Audiovisual Media Services Directive \(Directive \(EU\) 2018/1808\)](#) ("AVMSD") specifically applies to Video-Sharing Platforms ("VSPs"). Article 28b(1)(c) requires VSPs to take "appropriate measures" to protect the general public from content which constitutes an activity which is a criminal offence under Union law, including offences concerning child pornography as set out in Article 5(4) of [Directive 2011/93/EU](#) ("CSAD"). These measures must be "appropriate in the light of the nature of the content, the category of persons to be protected and the rights and legitimate interests at stake" (Article 28b(3)).

The Interim Regulation

On 14 July 2021, the European Commission adopted [Regulation \(EU\) 2021/1232](#) (the "Interim Regulation") as a temporary derogation from certain provisions of the [E-Privacy Directive \(2002/58/EC\)](#) for the purpose of combating online child sexual abuse. The Interim Regulation creates an exception to the ePrivacy Directive ([Directive 2002/58/EC of 12 July 2002](#)), which would ordinarily prohibit providers of messaging or email services from scanning the content of private communications. The Interim Regulation permits, but does not mandate, certain providers (primarily number-independent interpersonal communications services, such as webmail and messaging apps) to derogate from data protection rules in the electronic communications sector to voluntarily use specific technologies for the processing of personal and other data to detect, remove, and report online CSAM. The Interim Regulation initially expired in August 2024. However, on 30 November 2023, the European Commission [adopted a limited time extension to the Interim Regulation](#) to extend the Interim Regulation to 3 April 2026. This was to prevent a gap in legal coverage and to enable the continuation of voluntary activities to detect and report child sexual abuse until a permanent solution, the [proposed CSAM Regulation](#), is enacted.

Under Article 3 of the Interim Regulation, providers may voluntarily:

- Detect known CSAM using technologies such as hash-matching or fingerprinting
- Detect new or previously unknown CSAM using classifier technologies and artificial intelligence tools
- Report detected material to competent authorities and specialized organizations
- Remove or disable access to detected illegal content

Any detection measures implemented must be:

- Strictly necessary for the specified purposes
- Proportionate to the risks addressed
- Limited to what is necessary for detection and reporting
- Subject to appropriate human oversight and verification
- Accompanied by transparent information to users about the processing

Article 3(1)(g)(vii) requires providers utilising the derogation to submit detailed annual reports to national supervisory authorities, including statistics on detection activities, false positive rates, and the effectiveness of implemented measures. Article 8(1) requires Member States to submit annual statistics to the Commission by August 3 each year, including, the total number of CSAM reports submitted to law enforcement by providers and organizations, the



number of children identified through detection actions, and the number of perpetrators convicted.

The Interim Regulation relies on definitions contained in the [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 \(“CSAD”\)](#) when determining what CSAM is.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“[Proposal](#)”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the Member States (Articles 7 to 15). The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Article 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the proposed Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This proposed Proposal has been included given its significance to the future of CSAM regulation in the EU.

- b. review, screen, moderate, or detect content to identify enticement, grooming, or sextortion of a child**

Digital Services Act



See item (a) above.

In addition, as specific to this item (b), within the Guidelines published by the European Commission on the DSA, the European Commission considers that Online Platforms and VLOPs should at a minimum identify and take into account *“the actual or potential impact on the privacy, safety and security of minors that the online platform may pose or give rise to, based on the (...) typology of online risks to children”* (Section 5, para. 18, b, [Guidelines](#)). Among these risks, the Annex to the Guidelines mentions *“contact risks”*, which refer to *“situations in which minors are victims of the interactions, as opposed to the actor: a. hateful encounters; b. harmful encounters (e.g. the encounter takes place with the intention to harm the minor); c. illegal encounters (e.g. can be prosecuted under criminal law); and d. other problematic encounters. Examples of contact risks include, but are not limited to, **online grooming, online sexual coercion and extortion**, sexual abuse via webcam, cyberbullying and trafficking in human beings for the purposes of sexual exploitation. These risks also extend to online fraud practices such as phishing, marketplace fraud, and identity theft”* (Annex, 5C typology of online risks to children, [Guidelines](#)).

Online Platforms are further encouraged to *“ensure that irrespective of the account settings chosen by minors, [they] can never be easily found or contacted by accounts they have not previously accepted as contacts”* (Section 6.3.2, para. 59, b, i, [Guidelines](#)).

The Guidelines further specify that *“age assurance tools can help providers to enforce access restrictions for users below a certain age, in order to protect minors from accessing age-inappropriate content online, such as gambling or pornography, or from being exposed to other risks such as **grooming**”* (Section 6.1.1, para. 25, [Guidelines](#)).

Audiovisual Media Services Directive (AVMSD) for Video-Sharing Platforms

The revised [Audiovisual Media Services Directive \(Directive \(EU\) 2018/1808\)](#) (“AVMSD”) specifically applies to Video-Sharing Platforms (“VSPs”). Article 28b(1)(c) requires VSPs to take “appropriate measures” to protect the general public from content which constitutes an activity which is a criminal offence under Union law, including offences concerning child pornography as set out in Article 5(4) of [Directive 2011/93/EU](#) (“CSAD”). These measures must be “appropriate in the light of the nature of the content, the category of persons to be protected and the rights and legitimate interests at stake” (Article 28b(3)). This could also include other criminal offences caught by CSAD, such as engaging in sexual activities with a child where *“use is made of coercion, force or threats”* and activities encompassing *“coercing, forcing or threatening a child into sexual activities with a third party”* (Articles 3(5)(iii) and (6)).

The Interim Regulation

On 14 July 2021, the European Commission adopted [Regulation \(EU\) 2021/1232](#) (the “Interim Regulation”) as a temporary derogation from certain provisions of the [E-Privacy Directive \(2002/58/EC\)](#) for the purpose of combating online child sexual abuse. The Interim Regulation creates an exception to the ePrivacy Directive ([Directive 2002/58/EC of 12 July 2002](#)), which would ordinarily prohibit providers of messaging or email services from scanning the content of private communications. The Interim Regulation permits, but does not mandate, certain providers (primarily number-independent interpersonal communications services, such as webmail and messaging apps) to derogate from data protection rules in the electronic communications sector to voluntarily use specific technologies for the processing of personal



and other data to detect, remove, and report online CSAM. The Interim Regulation initially expired in August 2024. However, on 30 November 2023, the European Commission [adopted a limited time extension to the Interim Regulation](#) to extend the Interim Regulation to 3 April 2026.

Under Article 3 of the Interim Regulation, providers may voluntarily:

- Detect solicitation of children through automated analysis of communications
- Report detected material to competent authorities and specialized organizations
- Remove or disable access to detected illegal content

Any detection measures implemented must be:

- Strictly necessary for the specified purposes
- Proportionate to the risks addressed
- Limited to what is necessary for detection and reporting
- Subject to appropriate human oversight and verification
- Accompanied by transparent information to users about the processing

Article 3(1)(g)(vii) requires providers utilising the derogation to submit detailed annual reports to national supervisory authorities, including statistics on detection activities, false positive rates, and the effectiveness of implemented measures. Article 8(1) requires Member States to submit annual statistics to the Commission by August 3 each year, including, the total number of CSAM reports submitted to law enforcement by providers and organizations, the number of children identified through detection actions, and the number of perpetrators convicted.

The Interim Regulation relies on definitions contained in the [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](#) (“CSAD”) when determining what the solicitation of children is.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“**Proposal**”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material and solicitation of children on their services (Article 7 to 15), under a regime overseen and enforced by co-ordinating authorities designated by the Member States. The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-



to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council's approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

The Proposal includes specific provisions for grooming detection, including court-ordered detection requirements with enhanced safeguards such as time limitations (maximum 1 year for grooming detection orders) and mandatory data protection impact assessments (Article 7). This position has not been changed in the Council's and European Parliament's positions.

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

- c. **report child pornography, CSAM, enticement, grooming, or sextortion that they become aware of or are notified about on their systems to a law enforcement or government agency or nongovernmental organization**

Digital Services Act

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (known as the Digital Services Act and hereinafter defined as the "DSA") does not explicitly create a universal, standalone reporting obligation to law enforcement for CSAM or grooming. However, it contains a set of interconnected obligations that together form a functional framework for detection, action, and escalation.

Pursuant to Article 16(1) of the DSA, Online Platforms are required put in place a "*mechanism allowing any individual or entity*" to notify them about illegal content, which includes "*the sharing of images depicting child sexual abuse*" (Recital 12 of the DSA) and potentially "enticement of a child", "grooming of a child", or "sextortion" (Articles 18 – 20, and 23 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the "**Lanzarote Convention**"), and Articles 3(5)(iii) and (6) of 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 ("CSAD")).

In particular, Online Platforms and VLOPs are required to promptly inform and provide all relevant information to the law enforcement or judicial authorities of the Member State or Member States concerned of the suspicion "*that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place*" (Article 18, 1, DSA). For the sake of completeness, "*the Member State concerned shall be the*



Member State in which the offence is suspected to have taken place, to be taking place or to be likely to take place, or the Member State where the suspected offender resides or is located, or the Member State where the victim of the suspected offence resides or is located' (Article 18, 3, [DSA](#)).

The DSA does not provide definitions of what constitutes a "*criminal offence involving a threat to life or safety of a person or persons has taken place, is taking place or is likely to take place*". However, Recital 56 of the DSA gives examples of this by referring to the offences specified in the CSAD and [Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims](#) (the "**Anti-Trafficking Directive**"). Please note, recitals are not binding legal provisions.

On 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors ("[Guidelines](#)"). The aforementioned requirements are underlined in the Guidelines, which provide that "*the Commission recalls the obligations laid down in [the DSA], including the obligations to put in place notice and action mechanisms in Article 16, to provide a statement of reasons in Article 17, to notify suspicions of criminal offence in Article 18'* (Section 7.1, 76, [Guidelines](#)). In addition, the Commission considers that providers of online platforms accessible to minors should put in place the following measures to ensure a high level of privacy, safety, and security of minors on their service for the purposes Article 28 of the DSA: (i) ensure the availability of an option that allows minors to provide their own reasons for a report or complaint; and (ii) ensure that reporting, feedback and complaints are confidential and anonymous by default, while providing the option for minors to remove anonymity. They should also regularly review the reports, feedback and complaints that they receive. They should use this information to identify and address any aspects of their platform that may compromise the privacy, safety and/or security of minors, refine their recommender systems and moderation practices, improve overall safety standards, and foster a more trustworthy and responsible online environment (Section 7.1, para. 77, c to e, [Guidelines](#)).

Audiovisual Media Services Directive (AVMSD) for Video-Sharing Platforms

The revised [Audiovisual Media Services Directive \(Directive \(EU\) 2018/1808\)](#) ("**AVMSD**") specifically applies to Video-Sharing Platforms ("**VSPs**"). Article 28b(1)(c) requires VSPs to take "appropriate measures" to protect the general public from content which constitutes an activity which is a criminal offence under Union law, including offences concerning child pornography as set out in Article 5(4) of [Directive 2011/93/EU](#) ("**CSAD**"). These measures must be "appropriate in the light of the nature of the content, the category of persons to be protected and the rights and legitimate interests at stake" (Article 28b(3)). This could require VSPs to create a reporting mechanism or process for CSAM to a law enforcement or government agency or nongovernmental organization but this is left to proportionality assessments by the platform and regulators.

The Interim Regulation

On 14 July 2021, the European Commission adopted [Regulation \(EU\) 2021/1232](#) (the "**Interim Regulation**") as a temporary derogation from certain provisions of the [E-Privacy Directive \(2002/58/EC\)](#) for the purpose of combating online child sexual abuse.

Article 3(1)(g)(vii) of the Interim Regulation requires annual reporting to supervisory



authorities and the Commission of the number of cases of online child sexual abuse identified, differentiating between online child sexual abuse material and solicitation of children (ss 4) and the names of the organisations acting in the public interest against child sexual abuse with which data has been shared pursuant to this Regulation (ss9).

Article 3(1)(j) of the Interim Regulation requires providers to report “*every case of a reasoned and verified suspicion of online child sexual abuse... without delay to competent national law enforcement authorities or to organisations acting in the public interest against child sexual abuse*”. Article 3(1)(g)(iii) of the Interim Regulation requires prior human confirmation before such report can be made.

Article 8 of the Interim Regulation requires Member States to submit annual statistics to the Commission

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD) (“[Proposal](#)”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the Member States (Articles 7 to 15). The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

Article 12 of the [Proposal](#) would require providers to report detected CSAM and grooming to the new EU Centre for Child Sexual Abuse without delay which would then forward reports to:

- Europol
- Competent law enforcement authorities in Member States likely to have jurisdiction
- Relevant national Coordinating Authorities

This position has not been changed in the Council's and European Parliament's positions.

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

- d. **remove or take down any child pornography, CSAM, enticement, grooming, or sextortion that they identify, become aware of, or are notified about**

Digital Services Act

Articles 5 and 6 of the [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”) establish a liability framework that creates an indirect obligation for content removal. Hosting service providers (including online platforms) maintain their liability exemption for the storage of illegal content only if such service provider “*acts expeditiously to remove or to disable access to illegal content*” once they are aware or have knowledge of that material. When Online Platforms remove illegal content, they must notify the user and provide a statement of reasons including the legal basis for action (Article 17 of the [DSA](#)). Article 9 of the DSA provides the direct legal mechanism for mandatory removal through judicial or administrative orders. Article 9(1) states that “*upon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities ... providers of intermediary services shall inform the authority issuing the order, or any other authority specified in the order, of any effect given to the order without undue delay, specifying if and when effect was given to the order.*”

In addition to removing or disabling access to illegal content, Online Platforms are required to suspend “*for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content*” (Article 23(1) of the [DSA](#)).

Online Platforms must take special measures to “*ensure a high level of privacy, safety, and security of minors, on their service*” (Article 28, [DSA](#)). VLOPs have special obligations to adopt measures “*to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate*” (Article 35)(1)(j) [DSA](#)).

On 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors (“[Guidelines](#)”). According to the Guidelines, platforms are required carry out risk assessments and take mitigation measures against the risks arising from illegal content that could be encountered by minors. This includes detecting and removing content uploaded by other users that is criminal in nature, such as child sexual exploitation material or grooming-related communications. Platforms must then determine whether their current detection and removal systems are adequate to mitigate these risks and, if not, introduce new tools or escalation procedures (Section 5, para. 18, b, [Guidelines](#)).



Audiovisual Media Services Directive (AVMSD) for Video-Sharing Platforms

The revised [Audiovisual Media Services Directive \(Directive \(EU\) 2018/1808\)](#) (“AVMSD”) specifically applies to Video-Sharing Platforms (“VSPs”). Article 28b(1)(c) requires VSPs to take “appropriate measures” to protect the general public from content which constitutes an activity which is a criminal offence under Union law, including offences concerning child pornography as set out in Article 5(4) of [Directive 2011/93/EU](#) (“CSAD”). These measures must be “appropriate in the light of the nature of the content, the category of persons to be protected and the rights and legitimate interests at stake” (Article 28b(3)). It requires “appropriate measures,” which *may include* removing or taking down CSAM, but this is left to proportionality assessments by the platform and regulators.

Interim Regulation

On 14 July 2021, the European Commission adopted [Regulation \(EU\) 2021/1232](#) (the “Interim Regulation”) as a temporary derogation from certain provisions of the [E-Privacy Directive \(2002/58/EC\)](#) for the purpose of combating online child sexual abuse. Article 3(1)(i) of the Interim Regulation. Article 1 and Article 3(1)(a)(i) of the Interim Regulation permits providers to use specific technologies for the processing of personal and other data to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services, notwithstanding e-Privacy restrictions.

CSAD

Article 25(1) of [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](#) (“CSAD”) establishes the primary EU legal framework for child pornography removal, but relates to obligations at a Member State level (not directly on Online Platforms). It states, “*Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory*”. Although not representing a binding legal provision, Recital 47 of CSAD notes that “*the removal of child pornography content at its source is often not possible when the original materials are not located within the Union*”. Article 25(2) permits (but does not mandate) Member States taking measures “*to block access to web pages containing or disseminating child pornography towards the Internet users within their territory.*”

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“[Proposal](#)”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the



Member States (Articles 7 to 15). The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council's approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

The Proposal would establish a framework for removal through judicial removal orders (Article 14), but does not create automatic removal obligations upon detection. This position has not been changed in the Council's and European Parliament's positions.

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

e. review content by human moderators to screen or moderate for child pornography or CSAM

There is no explicit requirement for Online Platforms to use human moderators specifically to detect or screen child pornography or CSAM.

Digital Services Act

Although not representing a binding legal provision, Recital 58 of [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”) specifies that “*providers of online platforms should be required to provide for internal complaint-handling systems, which meet certain conditions that aim to ensure that the systems are easily accessible and lead to swift, non-discriminatory, non-arbitrary and fair outcomes, and are **subject to human review where automated means are used***”. Article 14(1) further requires providers to include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. Article 42 of the DSA also requires VLOPs and VLOSEs to publish half-yearly transparency reports which must include, amongst others, information on the human resources dedicated to content moderation, the accuracy and error rates of automated moderation (if used).

Further, the DSA imposes obligations that require effective and operational systems, which *may* include human moderation as part of broader content moderation measures. Online



Platforms are required to put into place notice and action mechanisms (Article 16 of the [DSA](#)) and VLOPs are required to adopt reasonable, proportionate, and effective measures to mitigate systemic risks such as illegal content (Article 35 of the [DSA](#)).

On 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors ("[Guidelines](#)"). The Guidelines states that Online Platforms should "*ensure **human review is available in addition to automated content review** and any other relevant tools for reported accounts or content that the provider suspects may pose a risk of harm to minors' privacy, safety or security*" (Section 6.7, para. 72, d, [Guidelines](#)).

Audiovisual Media Services Directive (AVMSD) for Video-Sharing Platforms

The revised [Audiovisual Media Services Directive \(Directive \(EU\) 2018/1808\)](#) ("[AVMSD](#)") specifically applies to Video-Sharing Platforms ("[VSPs](#)"). Article 28b(1)(c) requires VSPs to take "appropriate measures" to protect the general public from content which constitutes an activity which is a criminal offence under Union law, including offences concerning child pornography as set out in Article 5(4) of [Directive 2011/93/EU](#) ("[CSAD](#)"). These measures must be "appropriate in the light of the nature of the content, the category of persons to be protected and the rights and legitimate interests at stake" (Article 28b(3)). The AVMSD does not mandate "human moderators." It requires "appropriate measures," which *may include* human review, but this is left to proportionality assessments by the platform and regulators.

General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)

Article 22 of the [General Data Protection Regulation \(GDPR, Regulation \(EU\) 2016/679\)](#) ("[GDPR](#)") on automated decision-making says "*data subjects shall have the right not to be subject to a decision based solely on automated processing...*" unless safeguards are in place, including the right to human intervention. This is not drafted with CSAM moderation in mind, but if moderation decisions affect users' rights (e.g., account suspension due to suspected CSAM), human review may be required.

EU Artificial Intelligence Act (2024)

While [Regulation \(EU\) 2024/1689](#) of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the "[EU Artificial Intelligence Act](#)") does not mandate AI use for CSAM detection, Online Platforms using AI or machine learning tools for detecting CSAM, grooming, sextortion etc. are users of AI systems under the Act. If an Online Platform uses AI tools for CSAM detection, those tools must comply with Chapter III, Section 2 (Articles 8–15) of the Act, including using appropriate human oversight to prevent or minimize risks (Article 14). The Act was published in the [Official Journal](#) on July 12, 2024, and entered into force on August 1, 2024. Most provisions will start applying in by 2 August 2026, with other parts having earlier or later deadlines for implementation. High-risk AI obligations, including Article 14, apply from 2 August 2026. The remaining obligations concerning certain high-risk AI systems will apply from 2 August 2027.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) ("[Proposal](#)"). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU



legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted

The Proposal does not impose a general duty for human moderators to review user content. Instead, when a provider is executing a detection order, it must ensure “*regular human oversight ... and, where necessary ... human intervention,*” particularly where potential errors or potential solicitation of children are detected (Article 10(4)(c)).

The European Parliament [adopted its position](#) in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented.

On 26 November 2025, the Council of the European Union [adopted its position](#), which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. Like the Commission proposal and the Parliament position, the Council text does not impose an explicit legal obligation on providers to conduct content review through human moderators, leaving the choice of compliance measures to providers subject to regulatory oversight. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by [Regulation \(EU\) 2024/1307](#) to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

- f. **remove child pornography, CSAM, enticement, grooming, or sextortion from their systems when notified of its presence by a victim, nongovernmental organization, law enforcement, or government agency**

Digital Services Act

Pursuant to the [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”), platforms must implement notice-and-action mechanisms and remove illegal content upon knowledge (i.e., notification). The DSA has been in force since October 2022 and applicable since February 2024. Very Large Online Platforms (“**VLOPs**”, defined by Article 33 of the DSA, face enhanced obligations to assess risks and implement targeted content moderation measures. Pursuant to Article 3(h) of the DSA, “illegal content” means “*any information, which, in itself or by its reference to an activity, including the sale of products or provision of services, is not in compliance with Union law or the law of a Member State*”.



Offences of child pornography/CSAM (Article 5(4)) and grooming/solicitation of children (Article 6) are criminalised under [Directive 2011/93/EU](#) on combating the sexual abuse and sexual exploitation of children. Such material therefore constitutes “illegal content” under the DSA.

Pursuant to Article 16(1) of the [DSA](#), “*providers of hosting services [i.e., an Online Platform] shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means*”. Therefore, the notification can be by a victim, nongovernmental organization, law enforcement, or government agency.

Articles 5 and 6 of the DSA establish a liability framework that creates an indirect obligation for content removal. Hosting service providers (including online platforms) maintain their liability exemption for the storage of illegal content only if such service provider “*acts expeditiously to remove or to disable access to illegal content*” once they are aware or have knowledge of that material. When Online Platforms remove illegal content, they must notify the user and provide a statement of reasons including the legal basis for action (Article 17 of the [DSA](#)).

Article 9 of the DSA provides the direct legal mechanism for mandatory removal through judicial or administrative orders. Article 9(1) states that “*upon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities ... providers of intermediary services shall inform the authority issuing the order, or any other authority specified in the order, of any effect given to the order without undue delay, specifying if and when effect was given to the order.*” This Article does not mention notification by a victim or nongovernmental organization.

In addition to removing or disabling access to illegal content, Online Platforms are required to suspend “*for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content*” (Article 23(1) of the [DSA](#)).

Audiovisual Media Services Directive (AVMSD) for Video-Sharing Platforms

The revised [Audiovisual Media Services Directive \(Directive \(EU\) 2018/1808\)](#) (“**AVMSD**”) specifically applies to Video-Sharing Platforms (“**VSPs**”). Article 28b(1)(c) requires VSPs to take “appropriate measures” to protect the general public from content which constitutes an activity which is a criminal offence under Union law, including offences concerning child pornography as set out in Article 5(4) of [Directive 2011/93/EU](#) (“**CSAD**”). These measures must be “appropriate in the light of the nature of the content, the category of persons to be protected and the rights and legitimate interests at stake” (Article 28b(3)). This provision can require platforms to maintain effective notice-and-action and removal systems, potentially including mechanisms for victims, NGOs, LE, or government bodies, but this is left to proportionality assessments by the platform and regulators.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to



prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD) (“[Proposal](#)”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the Member States (Articles 7 to 15). The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

Article 12(3) of the Proposal requires providers to “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,” thereby establishing a direct pathway for victims and the general public to report suspected CSAM or solicitation of children to platforms. The proposed Regulation would also establish a framework for removal through binding judicial or administrative removal orders (Article 14).

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

- g. use any specific technology to detect, remove, block, or take down any child pornography, CSAM, enticement, grooming, or sextortion, including:**
 - i. “Hashing technology” (<https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery/>). Many Online Platforms hash and tag images and videos of child pornography or CSAM and then use hashing technology to scan content on their systems to detect the distribution of child pornography or CSAM online so it can be removed.**

At present, there is no obligation under EU law for Online Platform to use any specific detection technology, including hashing, for the purpose of combating CSAM,



grooming or related offences. Historically, EU laws have taken a “technology neutral” approach, instead focusing on the outcome (keeping illegal material off the service and notifying authorities) rather than prescribing specific tools). However, EU law provides multiple legal avenues through which the use of specific technologies, such as hashing, is either permitted or encouraged.

Interim Regulation

On 14 July 2021, the European Commission adopted [Regulation \(EU\) 2021/1232](#) (the “Interim Regulation”) as a temporary derogation from certain provisions of the [E-Privacy Directive \(2002/58/EC\)](#) for the purpose of combating online child sexual abuse. The Interim Regulation creates an exception to the ePrivacy Directive ([Directive 2002/58/EC of 12 July 2002](#)), which would ordinarily prohibit providers of messaging or email services from scanning the content of private communications.

The Interim Regulation allows Online Platforms to voluntarily use specific technologies to detect, remove and report online child sexual abuse content. Recital 7 clarifies that *“the technology used (...) could be hashing technology for images and videos and classifiers and artificial intelligence for analysing text or traffic data. When using hashing technology, online child sexual abuse material is reported when a positive hit is returned, which means a match resulting from a comparison between an image or a video and a unique, non-reconvertible digital signature (‘hash’) from a database maintained by an organisation acting in the public interest against child sexual abuse that contains verified online child sexual abuse material”*.

Article 3(1)(h)(iii) of the [Interim Regulation](#) specifies in addition that *“where suspected online child sexual abuse has been identified (...) the content data [is] stored in a secured manner, solely for the purposes of creating a unique, non-reconvertible digital signature (‘hash’) of data reliably identified as online child sexual abuse material”*.

On 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors (“[Guidelines](#)”). The Guidelines adopted under Article 28 of the DSA indicate that *“the Commission considers that providers of online platforms accessible to minors should (...) put in place effective technologies, internal mechanisms and preventative measures to reduce the risk of content and behaviour that are harmful to minors’ privacy, safety or security from being recommended to minors, including by implementing effective technical solutions to tackle known harmful and illegal content, such as hash matching and URL detection”* (Section 6.7, para. 72, g, [Guidelines](#)).

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“**Proposal**”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt

positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the Member States (Articles 7 to 15). The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

The proposed Regulation would establish explicit technology requirements. Article 10 specifies detection technologies must meet specific criteria:

- Technologies must be “sufficiently reliable” with limited error rates
- Must be “the least intrusive in terms of privacy and data protection”
- Must be “in accordance with the state of the art in the industry”
- For known CSAM: Technologies “are typically based on hashing, a sort of digital fingerprint

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

ii. Artificial intelligence or machine learning tools to detect the presence of child pornography, CSAM, enticement, grooming, or sextortion.

At present, there is no obligation under EU law for Online Platform to use any specific detection technology, including hashing, for the purpose of combating CSAM, grooming or related offences. Historically, EU laws have taken a “technology neutral” approach, instead focusing on the outcome (keeping illegal material off the service and notifying authorities) rather than prescribing specific tools). However, EU law provides multiple legal avenues through which the use of specific technologies, such as artificial intelligence (“AI”) or machine learning tools to detect CSAM, grooming, enticement or sextortion, is either permitted or encouraged.



Digital Services Act

Article 34 of the [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”) requires Very Large Online Platforms (VLOPs) to conduct comprehensive risk assessments. These assessments must examine system risks from the design or functioning of their service, including “*algorithmic systems*” (Article 34(1)). Systemic risks also includes the dissemination of illegal content through their services (Article 34(1)(a)). Article 35 of the DSA mandates VLOPs to implement “*reasonable, proportionate and effective mitigation measures*”. While not specifying AI/ML tools, platforms could deploy these technologies to meet systematic risk mitigation obligations for child safety.

On 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors (“[Guidelines](#)”). The Guidelines adopted under Article 28 of the DSA, while not legally binding, indicate that “*Providers should also explore potential added benefits of emerging technical solutions such as AI classifiers to detect new or altered content and conduct*” (Section 6.7, para. 72, g, [Guidelines](#)). The Commission also considers that providers of online platforms accessible to minors should implement “*technical solutions to prevent the AI systems on their platform from allowing users to access, generate and disseminate content that is harmful for the privacy, safety and/or security of minors*” (Section 6.7, para. 72, h, [Guidelines](#)). This paragraph further says that “*Integrating into any AI systems safeguards that detect and prevent prompts that the provider has identified in their moderation policies as being harmful to minors’ privacy, safety and/or security. This may include, for example, the use of prompt classifiers, content moderation and other filters*” (Section 6.7, para. 72, h(i), [Guidelines](#)).

Interim Regulation

On 14 July 2021, the European Commission adopted [Regulation \(EU\) 2021/1232](#) (the “**Interim Regulation**”) as a temporary derogation from certain provisions of the [E-Privacy Directive \(2002/58/EC\)](#) for the purpose of combating online child sexual abuse. The Interim Regulation creates an exception to the ePrivacy Directive ([Directive 2002/58/EC of 12 July 2002](#)), which would ordinarily prohibit providers of messaging or email services from scanning the content of private communications.

The Interim Regulation allows Online Platforms to voluntarily use specific technologies to detect, remove and report online child sexual abuse content. Recital 7 of the Interim Regulation allows Online Platforms to voluntarily use specific technologies to detect and remove online child sexual abuse content, including AI (“*the technology used (...) could be hashing technology for images and videos and classifiers and **artificial intelligence** for analysing text or traffic data*”).

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“[Proposal](#)”). The Proposal is intended to provide a long-term legal



framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The initial draft of the Proposal would have required providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the Member States (Articles 7 to 15). The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11), making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures. The Council agreeing its position in relation to the Proposal enables trilogues with the European Parliament to begin.

The proposed Regulation would establish explicit technology requirements. Article 10 specifies detection technologies must meet specific criteria:

- Technologies must be “sufficiently reliable” with limited error rates
- Must be “the least intrusive in terms of privacy and data protection”
- Must be “in accordance with the state of the art in the industry”
- For new CSAM detection: “Technologies currently used...include classifiers and artificial intelligence (AI) that analyse images and videos”
- For grooming detection: Employ “machine learning classifiers” that “apply machine learning to help identify content that shares similar characteristics to known grooming conversations”

Given that interinstitutional negotiations are still pending, the final text remains uncertain. The Interim Regulation was extended by Regulation (EU) 2024/1307 to 3 April 2026 to prevent a legal gap while interinstitutional negotiations are pending. If the Proposal is not adopted before 3 April 2026, and the Interim Regulation is not extended again, the Interim Regulation will lapse, removing the legal basis for voluntary detection under EU law. This Proposal has been included given its significance to the future of CSAM regulation in the EU.

- h. if the applicable laws or regulations require some, but not all, Online Platforms to perform any of the above activities, describe how the differing requirements apply. For example, are differences based on the number of online users, types of services offered, etc.?**

[Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#)



(known as the Digital Services Act and hereinafter defined as the “DSA”) distinguishes between types of platforms.

Hosting Services (all platforms storing user content) must comply with Article 16 (notice and action mechanisms) requiring expeditious removal of CSAM when notified by any individual or entity (e.g., victims, NGOs, law enforcement, or government agencies). All hosting services must also comply with Article 18 (notification of suspicions of criminal offences) requiring prompt notification to law enforcement or judicial authorities of suspected a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place (which could include CSAM and other serious crimes).

Online Platforms (hosting services that publicly disseminate content) face enhanced CSAM obligations including Article 22 (trusted flaggers) which mandates priority processing of CSAM notifications certain trusted flaggers. Trusted flagger status may be granted to child protection organisations and NGOs with expertise in detecting illegal content.

Very Large Online Platforms (“VLOPs”), defined as having a number of average monthly active recipients of the service in the Union equal to or ~~higher~~ than 45 million under Article 33, face the most comprehensive CSAM-related obligations. Under Articles 34-35, VLOPs must conduct systematic risk assessments specifically examining “*the dissemination of illegal content through their services*” (which includes CSAM) and implement “*reasonable, proportionate and effective mitigation measures*” including deployment of detection technologies for child protection. These requirements to conduct risk assessments and adopt mitigating measures are stricter than for other Online Platforms.

The DSA provides proportionate relief for smaller companies for CSAM relevant obligations under the DSA. Micro Enterprises (fewer than 10 employees, €2 million turnover/balance sheet, as set out in the [EU Commission Recommendation 2003/361/EC](#)) remain subject to core CSAM removal requirements under Article 6 (hosting liability) and Article 16 (notice and takedown). However, they receive complete exemptions from Article 15 (general transparency reporting requirements for all intermediary services) and from all online platform obligations under Articles 20-24 (including Article 24 transparency reporting), except for Article 24(3) which requires disclosure of user numbers if requested by authorities to identify potential VLOPs.

Small Enterprises (fewer than 50 employees, €10 million turnover/balance sheet, as set out in the [EU Commission Recommendation 2003/361/EC](#)) must comply with all CSAM removal and reporting obligations under Articles 16 (notice and takedown), 18 (notification of suspicions of criminal offences), and 22 (which requires priority processing of notices from trusted flaggers in relation to illegal content in general). However, they receive complete exemptions from Article 15 (general transparency reporting requirements for all intermediary services) and from all online platform obligations under Articles 20-24 (including Article 24 transparency reporting), except for Article 24(3) which requires disclosure of user numbers if requested by authorities to identify potential VLOPs. When crossing the VLOP threshold under Article 33, they receive a 12-month transitional exemption from the enhanced risk assessment and mitigation requirements under Articles 34-35, but core CSAM removal obligations under Article 16 remain applicable.

Resources:

- [Directive 2002/58/EC](#) of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the “**ePrivacy Directive**”).



- [Council of Europe Convention](#) on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, Lanzarote Convention) (signed 25 October 2007, entered into force 1 July 2010).
- [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), “**CSAD**”.
- [Directive](#) 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, (OJ L 101 15.4.2011, p. 1), “**Anti-Trafficking Directive**”.
- [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, (OJ L 315, 14.11.2012, p. 57–73), “**Victims’ Right Directive**” – VRD.
- [Regulation \(EU\) 2016/679](#) 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 (“**General Data Protection Regulation**” or “**GDPR**”)
- [Directive \(EU\) 2018/1808](#) of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions concerning audiovisual media (Revised Audiovisual Media Services Directive, introducing rules for video-sharing platforms) (“**AVMSD**”)
- [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. 41–51), Temporary Derogation Regulation (“**Interim Regulation**”).
- Proposal for a Regulation (COM(2022) 209 final, 11 May 2022, procedure 2022/0155(COD)) laying down rules to prevent and combat child sexual abuse online (the “**Proposal**”).
- [Regulation \(EU\) 2022/2065](#) of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, (OJ L 277, 27.10.2022, p. 1–102), (the “**Digital Services Act**” or “**DSA**”).
- [Regulation \(EU\) 2024/1307](#) of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 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 277, 27.10.2022, p. 1–102) (extension to the Interim Regulation).
- [Regulation \(EU\) 2024/1689](#) of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain acts (the “**EU Artificial Intelligence Act**”)
- [Communication](#) to the Commission, Approval of Guidelines on measures to ensure a high level of privacy, safety and security for minors online, 14 July 2025, C (2025) 4764 final (adopted under Article 28 of the DSA).

3. Are Online Platforms legally required or recommended to implement any method to verify the age of a user before allowing access to an online platform?

Digital Services Act

While EU law does not impose universal age verification mandates on all platforms, it creates strong legal incentives through the [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”) framework.

Pursuant to the DSA, Online Platforms “*accessible (...) to minors*” must adopt “*appropriate and proportionate measures*” to ensure a high level of privacy, safety and security for minors (Article 28 of the DSA).

On 14 July 2025, the European Commission issued Guidelines under Article 28(4) of the DSA on the protection of minors (“[Guidelines](#)”). The Guidelines specify that “*the use of access restrictions supported by **age verification methods** [are] appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors [(Section 6.1.3.1, para. 37 of the [Guidelines](#))]. For this purpose, age assurance tools can help providers to enforce access restrictions for users below a certain age, in order to protect minors from accessing age-inappropriate content online, such as gambling or pornography, or from being exposed to other risks such as grooming*” (Section 6.1.1.1, para. 25 of the [Guidelines](#)). Three age verification methods are then described: (i) self-declaration; (ii) age estimation; and (iii) age verification (Section 6.1.1, para 29 of the Guidelines). For the purposes of this questionnaire, we will solely focus on the recommendations linked to age verification methods.

However, Article 28(3) states that platforms are “*not obliged to process additional personal data to determine whether the recipient of the service is a minor*”. Underpinning Article 28(3), the Guidelines further specify that “*age verification should be treated as a separate, distinct process that is not connected with other data collection activities exercised by online platforms. Age verification should not entitle providers of online platforms to store personal data beyond information about the user’s age group. (...) Methods that rely on verified and trusted government-issued IDs, without providing the platform with additional personal data, may constitute an effective age verification method, in so far as they are based on anonymised age tokens*” (Section 6.1.3.2, paras. 39 to 41 of the [Guidelines](#)). It is worth noting that any age verification implementation must comply with GDPR data minimization principles and process only the minimum personal data necessary to achieve the age verification purpose.

In addition, pursuant to Article 35 of the [DSA](#), VLOPs are required to put in place reasonable, proportionate and effective mitigation measures, including “*taking targeted measures to protect the rights of the child, including **age verification** and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate*”.

Therefore, for all Online Platforms, age verification methods are required when appropriate and proportionate to ensure a high level of privacy, safety and security for minors, as also recommended by the Guidelines. Further, VLOPs age verification and parental control tools are part of mandatory risk mitigation measures.

Age verification compliance under the DSA is supervised by National Digital Services Coordinators (appointed by each Member State pursuant to Article 49 of the DSA) for regular platforms and directly by the European Commission for VLOPs (Articles 56(2) and 56(3) of the DSA) in relation to certain Articles of the DSA. Non-compliance can result in fines up to 6% of global annual turnover. While the Guidelines are not legally binding but serve as the “significant and meaningful benchmark” that the Commission will use to assess compliance with the DSA.

Please note that on 14 July 2025 the Commission presented a “Age-Verification Blueprint/App” encouraging platforms (especially those with adult content or social media accessible to minors) to verify users are 18+ using reliable, privacy-respecting methods. The blueprint recommends methods that are accurate, reliable, robust, non-intrusive and non-discriminatory and that provide

age estimation for lower-risk services and full verification for higher-risk ones. This is not a legislative instrument, but a policy initiative. Please, see [here](#) for further details.

EU Artificial Intelligence Act (2024)

Not strictly relevant but worth noting, the [Regulation \(EU\) 2024/1689](#) of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the “**EU Artificial Intelligence Act**”) prohibits AI practices that manipulate vulnerable individuals (e.g., by age or disability), but does not require age verification tools, nor does it regulate access to age-restricted content via AI.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“[Proposal](#)”). The Proposal is intended to provide a long-term legal framework to tackle child sexual abuse at EU level and to replace the Interim Regulation, if adopted. Under the EU legislative process, the European Commission proposes laws, the Council of the European Union and European Parliament each adopt positions, and then they negotiate a compromise in “trilogues” before the Proposal can be formally adopted.

The Commission’s initial proposal envisaged binding obligations for providers of “relevant information society services” (ISS) to detect, report and remove child sexual abuse material on their services, under a regime overseen and enforced by co-ordinating authorities designated by the Member States (Articles 7 to 15). In relation to access by children, the Proposal does not establish a general obligation to verify the age of users prior to granting access to an online platform. Instead, it refers to age verification or age assessment only as a possible risk-mitigation measure, in particular where necessary to address risks of solicitation or grooming, without prescribing specific technical methods, age thresholds, or data-collection requirements.

The Proposal would establish mandatory age verification requirements for platforms (Article 4(3) and Article 6(1)(c)), in particular where they have identified “a risk of use of their services for the purpose of the solicitation of children”.

The European Parliament adopted its position in November 2023 (LIBE 14 Nov; plenary 22 Nov) and confirmed the opening of interinstitutional negotiations. In its position, the European Parliament narrowed the scope of detection obligations (Articles 7 to 11) and likewise did not introduce a mandatory age-verification requirement, emphasising proportionality, safeguards, and the avoidance of generalised monitoring, while allowing age-related measures to be considered where justified by identified risks.

On 26 November 2025, the Council of the European Union adopted its position, which does not include mandatory scanning obligations and instead introduces a risk-based approach. Under the Council’s approach, providers would be required to assess the risk that their services could be misused for the dissemination of child sexual abuse material or solicitation of children and implement proportionate mitigating measures; designated national authorities would review these assessments and may oblige providers to carry out additional measures (Article 4). The Council position similarly treats age verification as a discretionary, risk-based mitigation tool rather than a

universal access requirement, leaving its implementation, management and technical design to providers, subject to regulatory oversight by competent authorities (Article 6(1)).

Resources:

- [Regulation \(EU\) 2016/679](#) 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 (“**General Data Protection Regulation**” or “**GDPR**”).
- [Regulation \(EU\) 2022/2065](#) of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, (OJ L 277, 27.10.2022, p. 1–102), (the “**Digital Services Act**” or the “**DSA**”).
- [Communication](#) to the Commission, Approval of Guidelines on measures to ensure a high level of privacy, safety and security for minors online, 14 July 2025, C (2025) 4764 final (the “**Guidelines**”).
- [Regulation \(EU\) 2024/1689](#) of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain acts (the “**EU Artificial Intelligence Act**”).
- [Proposal for a Regulation \(COM\(2022\) 209](#) final, 11 May 2022, procedure 2022/0155(COD)) laying down rules to prevent and combat child sexual abuse online (the proposed “**Proposal**”).

4. Are Online Platforms legally required or recommended to implement any method to obtain parental consent before a child uses the services of such Online Platforms?

Online platforms in the EU are not universally required to obtain parental consent before children use their services but face specific obligations under different legal frameworks depending on the type of data processing, service offered, and age of the child.

General Data Protection Regulation

The most explicit obligation in this area is enshrined in Article 8 of the [General Data Protection Regulation \(GDPR, Regulation \(EU\) 2016/679\)](#) (“**GDPR**”), which governs the conditions for the lawful processing of children's personal data in relation to the offering of information society services (i.e. online services such as social media, games, apps, or streaming platforms). GDPR does not include a definition of what constitutes a “child” or “children” and does not cross-reference other EU legislation/instrument for the definition of “child” or “children.”

Under Article 8(1), if an Online Platform relies on consent as its lawful basis for processing a child's personal data, and that child is below the age of digital consent, consent must be given or authorised by the child's parent or legal guardian. In particular: *“the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child”* (Article 8, 1, GDPR).

The GDPR sets this age threshold at 16 years but permits Member States to lower it to a minimum of 13 years: *“Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years”* (Article 8, 2, GDPR). As a result, the applicable age threshold may vary across the EU.

The GDPR also requires Online Platforms to make “reasonable efforts” to verify that such consent is genuinely given or authorised by a person with parental responsibility, taking into consideration available technology (“*available technology*” is not defined in the GDPR). It is important to note that this requirement applies only when consent is the chosen legal basis for processing personal data. If

the platform relies on another legal ground (such as contractual necessity, legitimate interest or legal obligation) parental consent under Article 8 of the GDPR is not required by default.

The relevant National Data Protection Authority (provided by each Member State pursuant to Article 51(1) of the GDPR) enforce GDPR compliance, with fines up to €20 million or 4% of global annual turnover (Article 83(5) of the GDPR).

Digital Services Act

In addition, while [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\)](#) (known as the Digital Services Act and hereinafter defined as the “**DSA**”) itself does not mandate parental consent, the Guidelines issued by the European Commission under Article 28(4) of the DSA on the protection of minors (“[Guidelines](#)”) specify that parental consent may be necessary in certain circumstances, especially where the Online Platform poses heightened risks to children, or where parental authorisation is required under other laws such as the GDPR. In paragraph 56, the Guidelines explicitly state that platforms should “*ensure that consent from the child’s parent or guardian is sought where necessary under Union or Member State law*” (Section 6.2, Para. 56, g, [Guidelines](#)).

While the DSA does not mandate parental consent for platform access, Article 35(1)(j) requires Very Large Online Platforms (VLOPs) to implement 'parental control tools' as mandatory risk mitigation measures aimed at helping minors signal abuse or obtain support, as appropriate.

Compliance under the DSA is supervised by National Digital Services Coordinators (appointed by each Member State pursuant to Article 49 of the DSA) for regular platforms and directly by the European Commission for VLOPs (Articles 56(2) and 56(3) of the DSA) in relation to certain Articles of the DSA. Non-compliance can result in fines up to 6% of global annual turnover. While the Guidelines are not legally binding but serve as the “significant and meaningful benchmark” that the Commission will use to assess compliance with the DSA.

Resources:

- [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 (the “**General Data Protection Regulation**” or the “**GDPR**”), (OJ L 119, 4.5.2016, p. 1–88).
- [Regulation](#) (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, (OJ L 277, 27.10.2022, p. 1–102), (the “**Digital Services Act**” or the “**DSA**”).
- [Communication](#) to the Commission, Approval of Guidelines on measures to ensure a high level of privacy, safety and security for minors online, 14 July 2025, C (2025) 4764 final.

5. Are there legal remedies for children who have been victimized by online child sexual exploitation? This may include children who are victimized by the distribution of child pornography or CSAM imagery in which they are depicted, or children victimized by enticement, grooming or sextortion. If such legal remedies exist, do they include:

Yes, under EU law, children who are victims of online child sexual exploitation, including victims of child pornography (CSAM), grooming, enticement or sextortion, are entitled to a broad range of legal remedies, especially under criminal law as well as through data protection and digital services legislation.

The main EU-level legal instruments in this area include:

- Criminal Investigation and Prosecution
 - [Directive 2011/93/EU](#) (the “CSAD”), which, broadly, requires Member States to criminalise production, distribution, possession and access to CSAM (Article 5(4)) and to criminalise solicitation and grooming of children (Articles 6–7), ensuring such offences are subject to investigation and prosecution in national courts.
 - [Regulation \(EU\) 2022/2065](#) (the “DSA”), which, broadly, obliges providers of intermediary services to notify law enforcement where they suspect criminal offences involving a threat to life or safety (Article 18), which can encompass CSAM offences, enabling criminal investigations.
 - [Regulation \(EU\) 2021/1232](#) (the “Interim Regulation”), which, broadly, permits providers who voluntarily deploy CSAM detection under the derogation to report every verified suspicion of online child sexual abuse to law enforcement or organisations acting in the public interest (Article 3(1)(j)), thereby supporting investigations.
 - Content Takedown and Blocking Orders
 - The CSAD requires Member States to ensure prompt removal of web pages containing or disseminating CSAM hosted in their territory and to endeavour to secure removal abroad (Article 25(1)). It also permits blocking access to CSAM where removal is not feasible (Article 25(2)).
 - The DSA requires providers of hosting services to implement notice-and-action mechanisms (Article 16) and to act expeditiously to remove or disable access to illegal content such as CSAM once they are made aware of it (Articles 5–6). National authorities may also issue removal or blocking orders against specific items of illegal content (Article 9).
 - Civil Claims and Compensation
 - [Directive 2012/29/EU](#) (the “Victims’ Rights Directive” or the “VRD”), which, broadly, establishes rights for victims, including children, to information, support, and legal assistance, and requires Member States to ensure access to compensation in civil courts for harm suffered.
 - [Directive 2011/36/EU](#) (the “Anti-Trafficking Directive”) which, broadly, requires Member States to ensure that victims of trafficking, including child victims, have access to assistance and support before, during and after criminal proceedings, including appropriate protection and access to compensation. The Directive primarily addresses trafficking for sexual exploitation, but could apply to online CSAM cases if there's actual trafficking involved.
 - Data Protection Remedies
 - [Regulation \(EU\) 2016/679](#) (the “GDPR”), Article 17 of which enables children depicted in CSAM to invoke the right to erasure and object to distribution of their personal data, compelling platforms to delete CSAM and cease processing.
- a. The ability to stop the publication of the pornography or CSAM imagery by the Online Platform?**

EU law does not provide a pre-emptive “stop publication” mechanism for the pornography or online CSAM. Children’s legal remedies require platforms to remove, disable access, or block content already published.



Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD) ("[Proposal](#)"). Article 20 of the Proposal gives persons depicted in known CSAM a right to information (via their national Coordinating Authority, with the EU Centre providing the data), and Article 21 gives a right to assistance and support for removal/disablement - hosting providers must give reasonable assistance, and victims may request support from the EU Centre to secure removal/disablement of known CSAM. Removal and blocking themselves occur via authority orders (e.g., Article 14 removal orders; Article 17 blocking orders), not automatically upon a victim's request.

As mentioned above, the European Parliament narrowed the scope of detection obligations, making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. The Parliament position nonetheless retains and reinforces victim-centred remedies, including mechanisms enabling victims to request and obtain the removal or disabling of access to child sexual abuse material, and obligations on providers to comply with authority-issued removal and blocking orders.

The Council position explicitly recognises the rights of victims of online child sexual exploitation to seek the removal, blocking or delisting of child sexual abuse material and requires providers to cooperate with competent authorities and victim-support mechanisms to stop the continued publication or availability of such material.

b. An obligation on the part of the Online Platform to take active steps to remove the pornography or other imagery from their servers?

Victims (or their representatives) have the legal right to demand the cessation of publication of child sexual abuse material on Online Platforms based on several mechanisms.

Digital Services Act

Article 16 of the [DSA](#) specifies that "*providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content*". In general, when an Online Platform becomes aware of illegal content online, it must act expeditiously to remove or to disable access to the illegal content (Article 5 and 6, DSA). In particular, where an Online Platform receives such a notice via order issued by the relevant national judicial or administrative authorities, it must act without undue delay to disable access or remove content (Article 9, 1 of the DSA).

Victims also have the right to use internal complaint mechanisms (Article 20 of the DSA) and, if unsuccessful, to escalate the matter to certified out-of-court dispute resolution bodies (Article 21 of the DSA) and digital services coordinators or national courts. In particular, regarding the internal complaint mechanisms, "*providers of online platforms shall provide recipients of the service, including individuals or entities (...) with access to an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge, against the decision taken by the provider of the online platform*". In light of



this, individuals and users can lodge a complaint against the decision of the Online Platform to “*whether or not remove or disable access to or restrict visibility of the information*” (Article 20, 1 of the DSA).

General Data Protection Regulation

If the CSAM imagery qualifies as personal data (which it may, particularly if the child is identifiable), victims have a “right to erasure” or “right to be forgotten” pursuant to Article 17 [GDPR](#): individuals concerned are entitled to demand the immediate removal of their data from all platforms that control or process it where the “*personal data have been unlawfully processed*”.

CSAD

Article 25 of the CSAD requires that Member States to ensure that “*Member States shall take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory*” (Article 25, [CSAD](#)).

As CSAD is a Directive, a child victim cannot usually invoke these Directives directly against a platform. Instead, Member States must transpose the Directive into their national law (e.g. criminal codes, victim compensation schemes). The victim then asserts their rights under national law, not directly under the EU Directive.

Interim Regulation

Article 3(1)(j) of the [Interim Regulation](#) permits, and for voluntary participants requires, the immediate reporting of verified CSAM suspicions and removal or disabling of access to detected CSAM under the temporary derogation, supporting platforms’ active removal efforts.

Pending Legislation – the proposed CSAM Regulation

Together with its new European strategy for a Better Internet for Kids (BIK+), the European Commission adopted on 11 May 2022 a proposal for a Regulation laying down rules to prevent and combat child sexual abuse online (COM(2022) 209) (procedure 2022/0155(COD)) (“[Proposal](#)”). The Proposal establishes victim remedies and enforcement mechanisms that require online platforms, when subject to a removal or blocking order or when acting on a valid victim request supported by competent authorities, to take active steps to remove child sexual abuse material from their servers or otherwise disable access to it, rather than merely refraining from further dissemination (Article 14) and providers of internet access services must block access when served with a blocking order (Articles 16–18).

As mentioned above, the European Parliament narrowed the scope of detection obligations, making detection orders a last resort, prohibiting blanket scanning, and requiring that any orders be targeted and proportionate, and that end-to-end encryption not be weakened or circumvented. The Parliament position nonetheless retains binding removal and blocking obligations and continues to require providers to actively execute authority-issued removal measures in order to prevent the continued availability of child sexual abuse material on their services.

The Council position explicitly preserves the obligation for providers to cooperate with



competent authorities and to take active technical and organisational measures to remove, block access to or delist child sexual abuse material once its presence on the service has been identified.

c. An ability to get an injunction or other court order against the Online Platform to stop them from publishing the pornography or imagery?

Digital Services Act

The [DSA](#) specifies that “upon the receipt of an order to act against one or more specific items of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union law or national law in compliance with Union law, providers of intermediary services shall inform the authority issuing the order, or any other authority specified in the order, of any effect given to the order without undue delay, specifying if and when effect was given to the order” (Article 9 of the DSA). The specific procedure to get an injunction or court order against the Online Platform will depend on the Member State’s judicial system and internal procedural law.

General Data Protection Regulation

As outlined in Section 4 of this questionnaire, the GDPR empowers individuals, including minors, to demand erasure of personal data (Article 17 of the [GDPR](#)) and provides with a right to lodge a complaint either with a supervisory authority and to have effective judicial remedy against a controller or processor of personal data (including Online Platforms).

Article 77 of the [GDPR](#) gives individuals the right “to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation”. Article 79, [GDPR](#), empowers individuals with the “right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers”.

CSAD

In addition, Article 17 of the [CSAD](#) mandates Member States to “take the necessary measures to establish their jurisdiction over the offences referred to in Articles 3 to 7”, including (i) offences concerning sexual abuse; (ii) offences concerning sexual exploitation; (iii) offences concerning child pornography; (iv) solicitation of children for sexual purposes; and (v) incitement, aiding and abetting and attempt to commit any of these offences.

Finally, Article 25 of the [CSAD](#) mandates Member States to “take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory”.

The CSAD leaves it to Member States to decide which measures to adopt to ensure the



removal of web pages containing or disseminating child pornography.

- d. **A protective order or other court order that prohibits the person who posts the pornography or imagery from doing so in the future on the same or other Online Platform?**

Pursuant to Article 23(1) of the [DSA](#), Online Platforms are required to suspend “*for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content*”. This suspension applies to accounts, not individual content items.

Otherwise, under EU law, there is no regulatory framework specifically addressing individuals who posts pornography or imagery on Online Platforms.

- e. **the ability to seek financial damages or any sort of monetary recovery from an offender who has shared the child’s image or video, either in a civil or a criminal proceeding?**

Victims’ Right Directive

The [VRD](#) establishes minimum rules in terms of compensation for victims of crime, which would include child victims of sexual exploitation, CSAM or child pornography. In particular, Article 16 mandates Member States to “*ensure that, in the course of criminal proceedings, victims are entitled to obtain a decision on compensation by the offender, within a reasonable time, except where national law provides for such a decision to be made in other legal proceedings*” and to “*promote measures to encourage offenders to provide adequate compensation to victims*”. Courts must inform victims about compensation possibilities. For child victims, Article 24 of the VRD requires Member States to ensure child victims benefit from special protection measures during criminal proceedings, including measures to avoid secondary victimisation.

Recital 10 of [Directive 2004/80/EC](#) on compensation to crime victims acknowledges that “*crime victims will often not be able to obtain compensation from the offender, since the offender may lack the necessary means to satisfy a judgment on damages or because the offender cannot be identified or prosecuted*”. Recital 6 states that “*crime victims in the European Union should be entitled to fair and appropriate compensation for the injuries they have suffered, regardless of where in the European Community the crime was committed*.” Accordingly, the Directive “*sets up a system of cooperation to facilitate access to compensation to victims of crimes in cross-border situations* (Recital 7). Article 12(2) requires each Member State to establish a national scheme guaranteeing fair and appropriate compensation.

The VRD and Council Directive 2004/80/EC are complementary. The VRD covers offender compensation rights, and Council Directive 2004/80/EC covers state compensation schemes.

CSAD

Article 20 of the [CSAD](#) mandates Member States to “*ensure that child victims have, without delay, access to legal counselling and, in accordance with the role of victims in the relevant justice system, to legal representation, including for the purpose of **claiming compensation***. *Legal counselling and legal representation shall be free of charge where the victim does not have sufficient financial resources*”. It does not itself grant compensation rights, but ensures



procedural support to pursue damages under national law.

Digital Services Act

The [DSA](#) empowers victims of infringements of this Regulations to obtain compensation. In particular, Article 54 of the DSA indicates that *"recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation"*.

General Data Protection Regulation

The [GDPR](#) empowers victims of infringements of this Regulations to obtain compensation. Article 82 of the GDPR specifies that *"any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"*.

Anti-Trafficking Directive

Articles 12 and 15 of the [Anti-Trafficking Directive](#) requires Member States to ensure victims have access without delay to free legal counselling and to free legal representation, including for the purpose of claiming compensation, unless they have sufficient financial resources (Articles 12(2) and 15(2)). Article 17 requires Member States to ensure victims have access to existing schemes of compensation to victims of violent crimes of intent (Article 17). This can cover online CSAM cases that amount to trafficking.

- f. **the ability to seek any other forms of victim compensation/recovery/services provided for under the law and/or by a government-funded source?**

VRD

Children can notably rely on the rights provided by the [VRD](#). Member States are required to put in place measures ensuring that children may notably obtain confidential victim support service free of charge (Article 8) and specialised services for victims of sexual violence (Article 9). Victim support services should provide, as a minimum: (i) information, advice and support relevant to the rights of victims including on accessing national compensation schemes for criminal injuries, and on their role in criminal proceedings including preparation for attendance at the trial; (ii) information about or direct referral to any relevant specialist support services in place; (iii) emotional and, where available, psychological support; (iv) advice relating to financial and practical issues arising from the crime; (v) unless otherwise provided by other public or private services, advice relating to the risk and prevention of secondary and repeat victimisation, of intimidation and of retaliation (Article 9, 1, a to e, of the VRD).

In addition, *"child victims shall be presumed to have specific protection needs due to their vulnerability to secondary and repeat victimisation, to intimidation and to retaliation"* (Article 22 of the [VRD](#)) and may benefit from specific procedural safeguards (Article 23 and 24 of the [VRD](#)), including: (i) interviews with the child being carried out in premises designed or adapted for that purpose; (ii) interviews with the child being carried out by or through professionals trained for that purpose; (iii) all interviews with victims of sexual violence, gender-based violence or violence in close relationships, unless conducted by a prosecutor or a judge, being conducted by a person of the same sex as the victim, if the victim so wishes, provided that the course of the criminal proceedings will not be prejudiced.



Recital 10 of [Directive 2004/80/EC](#) on compensation to crime victims acknowledges that *“crime victims will often not be able to obtain compensation from the offender, since the offender may lack the necessary means to satisfy a judgment on damages or because the offender cannot be identified or prosecuted”*. Recital 6 states that *“crime victims in the European Union should be entitled to fair and appropriate compensation for the injuries they have suffered, regardless of where in the European Community the crime was committed.”* Accordingly, the Directive *“sets up a system of cooperation to facilitate access to compensation to victims of crimes in cross-border situations* (Recital 7). Article 12(2) requires each Member State to establish a national scheme guaranteeing fair and appropriate compensation.

The VRD and Council Directive 2004/80/EC are complementary. The VRD covers offender compensation rights, and Council Directive 2004/80/EC covers state compensation schemes.

CSAD

Pursuant to Article 18 of the [CSAD](#), *“Member States shall take the necessary measures to ensure that a child is provided with assistance and support as soon as the competent authorities have a reasonable-grounds indication for believing that a child might have been subject to any of the offences referred to in Articles 3 to 7”*, including (i) offences concerning sexual abuse; (ii) offences concerning sexual exploitation; (iii) offences concerning child pornography; (iv) solicitation of children for sexual purposes; and (v) incitement, aiding and abetting and attempt to commit any of these offences. In addition, assistance and support should be provided to children before, during and for an appropriate period of time after the conclusion of criminal proceedings of children that are victims of such offences (Article 19, [CSAD](#)).

Anti-Trafficking Directive

Articles 12 and 15 of the [Anti-Trafficking Directive](#) requires Member States to provide assistance, support and compensation to victims of trafficking, including child trafficking for sexual exploitation. This can cover online CSAM cases that amount to trafficking.

g. notification to a victim when an offender is arrested for distributing child pornography or CSAM in which the child is depicted?

Under current EU law, there is no standalone requirement to notify a victim the moment an offender is arrested for distributing CSAM.

The [VRD](#) is the only legal text at EU level specifically addressing this issue and ensures that child victims receive ongoing information about key stages of criminal proceedings, which covers procedural milestones rather than the arrest itself.

In particular, Article 6(5) specifies that *“Member States shall ensure that victims are offered the opportunity to be notified, without unnecessary delay, when the person remanded in custody, prosecuted or sentenced for criminal offences concerning them is released from or has escaped detention. Furthermore, Member States shall ensure that victims are informed of any relevant measures issued for their protection in case of release or escape of the offender”*. However, this relates to an offender being released or escaping from detention,



not the initial arrest itself. The closest obligation relating to the “arrest” of an offender is contained in Article 6(1)(b) and (2) - victims must be informed of the time and place of the trial and the nature of the charges against the offender.

Additionally:

- Pursuant to Article 5, victims must receive a written acknowledgement of their formal complaint, confirming that authorities have acted on their report and initiated an investigation.
- Pursuant to Article 6(1)(a), victims are entitled to be notified without unnecessary delay of any decision not to proceed with or to end an investigation or not to prosecute the offender.

Article 6(6) further indicates that “*victims shall, upon request, receive the information provided for in paragraph 5 at least in cases where there is a danger or an identified risk of harm to them, unless there is an identified risk of harm to the offender which would result from the notification*”.

Resources:

- [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), “**CSAD**”.
- [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, (OJ L 315, 14.11.2012, p. 57–73), “**Victims’ Right Directive**” – or “**VRD**”.
- [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 (the “**General Data Protection Regulation**” or “**GDPR**”), (OJ L 119, 4.5.2016, p. 1–88).
- [Regulation](#) (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, (OJ L 277, 27.10.2022, p. 1–102), (the “**Digital Services Act**” or “**DSA**”).
- [Directive 2004/80/EC](#) of 29 April 2004 relating to compensation to crime victims.

6. “**Safety by Design**” is defined as tools or processes that are built into an Online Platform to protect children by making it easier for the relevant Online Platform to detect or prevent the distribution of child pornography or CSAM.

a. Are Online Platforms legally required to incorporate “**Safety by Design**” into their systems?

There is no legal requirement for Online Platforms that explicitly mandate them to incorporate “**Safety by Design**” into their systems. However, a number of legal provisions require Online Platforms to adopt and implement technical, architectural, or system-level safeguards to protect minors, including against CSAM.

Firstly, the [DSA](#) mandates Online Platforms to “*put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service*” (Article 28 of the DSA). While not explicitly mentioning the incorporation of “**Safety by Design**” measures, this provision requires platforms to integrate protective measures into the



design of their systems. These measures may include, notably, adapting interface design, modifying recommender systems, changing default settings or improving moderation systems.

Secondly, from a personal data perspective, the [GDPR](#) clearly require Online Platforms and other systems of personal data processing to *"implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects"* (Article 25 of the GDPR).

Finally, the [Guidelines](#) adopted under Article 28 DSA specify that *"the Commission considers that any measure that a provider of an online platform accessible to minors puts in place to comply with Article 28(1) of Regulation (EU) 2022/2065 should adhere to the following general principles: (...) **Privacy-, safety- and security-by-design**: providers of online platforms accessible to minors should integrate high standards of privacy, safety and security in the design, development and operation of their services. By-design concepts aim to harness the influence of providers of online platforms, designers and policymakers to shape product and service development in ways that prioritise values that promote human well-being. They refer to embedding privacy, safety and security protections by default into the design, operation and management of organisations, as well as in products and services from the start"* (Section 4, para. 17, c, Guidelines). While these Guidelines are not legally binding, they serve as the Commission's benchmark for assessing Article 28 compliance.

In addition, the Guidelines specify that Online Platforms accessible to minors should *"ensure that privacy, safety and security by design principles are consistently applied to all account settings for minors"* (Section 6.3.1, para. 57, a, of the Guidelines).

i. If so, must these steps be taken before the launch of an Online Platform?

Article 25 of the [GDPR](#) says data protection by design and by default requires controllers to integrate appropriate technical and organisational measures *"at the time of the determination of the means for processing and at the time of the processing itself,"* ensuring protections (e.g. age-appropriate defaults, minimised data collection) are in place before the service goes live.

Under the [DSA](#), VLOPs must conduct systemic risk assessments 'before deploying functionalities that are likely to have a critical impact on systemic risks' (Article 34(1)) and put in place risk mitigation measures as part of the 'design, development and operation' of their services (Article 35(1)(j)), which requires integration of child-safety measures before launch or rollout of new functionalities.

Section 4, para 17(c) of the [Guidelines](#) adopted under Article 28 DSA says that platforms should *"integrate privacy, safety and security by design"* from the start of service development. Section 6.3.1, para 57(a) says platforms should *"apply those principles to all account settings for minors before deployment"*. While not legally binding, these Guidelines represent the Commission's benchmark for assessing compliance with Article 28.

- ii. **If so, if an Online Platform has already been in public use, when must they have incorporated “Safety by Design” measures?**

GDPR: Article 25 requires controllers to implement data protection by design and by default ‘at the time of the determination of the means for processing and at the time of the processing itself.’ This obligation applies continuously, meaning platforms must ensure compliance without undue delay if safeguards are not yet in place.

DSA: Article 28(1) requires Online Platforms accessible to minors to have ‘appropriate and proportionate measures’ in place at all times to ensure a high level of privacy, safety and security of minors. For Very Large Online Platforms (VLOPs), Articles 34–35 establish recurring obligations: systemic risk assessments must be carried out at least once a year and prior to deploying functionalities that could critically impact systemic risks (Article 34(1)), and mitigation measures must be integrated into the design, development and operation of the service (Article 35(1)(j)).

Guidelines: Section 5, para. 21 recommends that providers review measures ‘periodically, and at least on an annual basis or whenever they make significant changes to the platform’s design or become aware of other circumstances that affect the platform’s design and operation relevant for ensuring a high level of privacy, safety and security of minors.’ While not legally binding, these Guidelines represent the Commission’s benchmark for compliance with the DS.

- iii. **For each of 6(a)(i) or (ii) above, please describe the legal requirement or recommendation.**

Please see the description provided in the responses to 6(a)(i) and (ii) above.

- b. **Please include information about the parameters for monitoring, management, and enforcement of any legal or regulatory requirements for the Online Platform’s incorporation of “Safety by Design”?**

There are no EU legal instruments that establish a dedicated, standalone framework for monitoring or enforcement of ‘Safety by Design’ obligations. However, monitoring, management and enforcement occur through the broader supervisory regimes attached to existing instruments:

- GDPR: Article 25 obligations (‘data protection by design and by default’) are monitored and enforced by national supervisory authorities (Articles 51–59), with penalties for infringement under Articles 83–84.
- DSA: Article 28(1) obligations for Online Platforms accessible to minors are supervised by national Digital Services Coordinators (Article 49). For Very Large Online Platforms (VLOPs), systemic risk assessments must be carried out at least annually and before deploying functionalities that may critically impact systemic risks (Article 34(1)), and these must be independently audited (Article 42). The European Commission has direct enforcement powers over VLOPs (Article 51).



Resources:

- [Regulation](#) (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, (OJ L 277, 27.10.2022, p. 1–102), (Digital Services Act - DSA).
- [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 - GDPR), (OJ L 119, 4.5.2016, p. 1–88).
- [Communication](#) to the Commission, Approval of Guidelines on measures to ensure a high level of privacy, safety and security for minors online, 14 July 2025, C (2025) 4764 final.