



5 FEBRUARY 2024

Child sexual abuse online Regulation: moving the debate forward

Executive summary

DIGITALEUROPE fully supports the goal of creating a comprehensive legal framework to ensure better protection of children against sexual abuse and exploitation online.¹

Our members play an important role in the battle against this horrible crime and take this responsibility seriously. They have carried out extensive work to fight child sexual abuse and exploitation online, including developing technology vital to its prevention, detection, removal and reporting.

We welcome the European Parliament's position on the proposal, which has moved the debate forward. Many aspects of the Parliament's position represent a significant improvement that will help protect children online whilst reflecting technological realities and safeguarding fundamental rights. The Council should take inspiration from this and move swiftly to adopt a position.

To this end, the final Regulation should:

- ▶ Create the right conditions for industry to develop and deploy mitigation measures by providing appropriate derogations from the ePrivacy Directive (ePD) that are not contingent on receiving detection orders.² This will allow providers to continue to expand on their efforts to fight child sexual abuse on their services with sufficient legal certainty;
- ▶ Include the Parliament's text on infrastructure services, mirroring the e-Evidence Regulation,³ which better reflects the technical and contractual capabilities of infrastructure services;

¹ COM/2022/209 final.

² Directive 2002/58/EC, as modified by Directives 2006/24/EC and 2009/136/EC.

³ Regulation (EU) 2023/1543.

- ▶▶ Restrict detection orders to known child sexual abuse material (CSAM), with a commitment to reassess the scope at a later stage based on the robustness of technologies; and
- ▶▶ Include the Parliament’s text proposed protection for end-to-end encryption (E2EE) technology. Encryption plays an important role in providing private and secure communications that users, including children, demand and expect to keep them safe online

Table of contents

• Executive summary	1
• Table of contents	2
• Ensuring a continued legal basis for proactive efforts	3
Temporary solution.....	3
Finding a long-term solution	3
• Scope	4
Infrastructure services	4
App stores.....	5
• Detection orders	5
• Encrypted communications	6
• Risk assessments	6
• Age assurance	7
• Data preservation	8
• EU Centre	8
Interplay with the global framework	9

Ensuring a continued legal basis for proactive efforts

Temporary solution

We strongly support the European Commission's proposal to extend the temporary derogation to the ePD until August 2026.⁴ We urge policymakers to adopt this temporary extension as is proposed by the Commission.

Given the continued need for political debate, the long-term legal framework will unlikely be in place before the current derogation expires in August 2024, thus creating a dangerous legal vacuum.

This temporary solution will ensure providers of interpersonal communications services (ICS) have the continued ability to process data for the purpose of detecting and reporting CSAM in messaging services.

Recommendation: Act fast to adopt a minimum two-year extension to the temporary derogation that provides sufficient time for policymakers to reach a compromise. It is clear the new framework will not be in place before the current derogation expires, and this temporary solution will prevent a legal vacuum whilst the long-term framework is being negotiated.

Finding a long-term solution

One central element missing from the original Commission proposal, and still absent from the Parliament's position, is an appropriate derogation from the relevant ePD provisions to facilitate proactive efforts by ICS providers to combat child sexual abuse online, that are not conditional on receiving a detection order.

The Parliament has tried to address the issue by expanding the measures which can be taken to mitigate CSA within Art. 4. However, this stops short of allowing possible mitigation measures that ICS providers could develop and deploy by processing personal, traffic and other data, which is not currently allowed by the ePD. This is concerning because the innovative voluntary risk mitigation and detection measures carried out by ICS providers at present would halt when the temporary derogation expires, and ICSs will not be allowed to further develop comprehensive approaches to mitigating the risk of misuse of their services for child sexual abuse.

⁴ COM(2023)777 final.

DIGITALEUROPE members have invested, and continue to invest heavily, in developing state-of-the-art technology that has helped detect and report an increasing amount of CSAM worldwide, as well as a range of risk-mitigation and safety-by-design tools designed to help prevent child sexual abuse from happening in the first place. This has resulted in tens of millions of reports to authorities worldwide last year alone.⁵ This progress has been made thanks to the strength of the current system of voluntary industry-led measures.

The need to wait for the issuance of a detection order will discourage innovative, proactive efforts in ICS. Detection orders should be a measure of last resort for negligent companies who have not demonstrated sufficient risk mitigation efforts.

Recommendation: The final Regulation should provide appropriate derogations from the ePD to allow ICS providers to prevent, detect, remove and report instances of child sexual abuse that are not contingent on receiving detection orders.

A possible solution could be to include an additional authorisation process, whereby ICS providers would ask their competent authority for prior authorisation before they roll out new technologies within communication services that have not been subject to consultation as per the current Interim Regulation and that are not currently deployed by an ICS provider in the EU.⁶

Scope

Infrastructure services

The broad scope of ‘hosting service providers’ as defined in the Commission’s proposal would impose obligations on services deeper in the internet stack, such as cloud infrastructure service providers, failing to recognise that they are extremely limited in what they can (and should) do with the data controlled by their customers.

Infrastructure services like cloud infrastructure are the building blocks for IT, and offer services that include compute power and database storage. Technically and contractually, service providers often do not have visibility into, or control over, the specific items of content that their customers store and share on their services.

⁵ NCMEC, *CyberTipline 2022 Report*, available at <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>.

⁶ Regulation (EU) 2021/1232.

Cloud customers, who as data controllers are in closer proximity and control over data, are hence better suited to comply with detection and removal orders.

We welcome the Parliament's approach to infrastructure services, which borrows from the e-Evidence Regulation. This introduces a 'cascade approach' which focuses on parties closest to the content in the first instance, i.e. cloud customers. It will ensure that such obligations are met by the most appropriate actor and as swiftly as possible without the need for redirection, and gives guidance to law enforcement on which service provider to contact first to issue removal orders.

Recommendation: Support the Parliament's approach to infrastructure service providers, which mirrors the e-Evidence Regulation. This approach better reflects the technical and contractual capabilities of infrastructure services.

App stores

We remain concerned about the suitability of the proposed provisions for app store providers, which do not take into account the technical and contractual role of app store providers.

Most apps are created by third-party developers who retain control over the functioning of the application, not by the provider of the app store. In addition, app store providers are not privy to the inner workings of an app.

App developers are best placed to assess the risks posed by their service, establishing an appropriate age rating, and ensuring appropriate in-app age-gating measures are employed.

App store providers should take reasonable measures to prevent known child users from installing apps where the developer has indicated that an app is unsuitable for children or has a content rating in place.

Recommendation: Clarify those app store providers designated as 'gatekeepers' under the Digital Markets Act (DMA) shall take reasonable measures to prevent known child users from downloading or installing apps where the developer has indicated that the app is unsuitable for children or where the app has a content rating in place.⁷

Detection orders

⁷ Regulation (EU) 2022/1925.

We welcome the Parliament's proposal to focus the scope of detection orders, specifically known CSAM, removing grooming.

The technology for detecting grooming conversations is still nascent and should be excluded from the scope of detection orders. We support the Parliament's proposal to continue to assess the technologies and consider whether they may be robust enough to incorporate at a later stage.

Recommendation: Support the Parliament's proposal to limit detection orders to known CSAM.

Encrypted communications

We welcome the Parliament's clear stipulation that the legislation applies without prejudice to end-to-end encryption (E2EE) technology, and that end-to-end encrypted services are not in the scope of detection order provisions.

Encryption plays an important role in providing private and secure communications that users, including children, demand and expect to keep them safe online. Even well-intentioned efforts to provide a lawful intercept solution in E2EE can undermine critical security benefits by making all users of such services more vulnerable to malicious attacks.⁸ The legislation must not lead to a weakening of E2EE or other security measures, their decryption or restriction of their use.

Recommendation: Support the Parliament's proposed protection for E2EE technology, which was not sufficiently strong in the original Commission text. Encryption plays an important role in providing private and secure communications that users, including children, demand and expect to keep them safe online.

Risk assessments

We welcome the Commission's proposal, which requires providers to evaluate their services' specific risks and establish appropriate, tailored mitigation strategies.

We support the Parliament's proposal, which clarifies that services with a very low risk of exposure to CSAM should be exempted from this requirement.⁹ This

⁸ For more on the crucial role of encryption, see DIGITALEUROPE, *Encryption: finding the balance between privacy, security and lawful data access*, available at <https://www.digitaleurope.org/wp/wp-content/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf>.

⁹ Defined as services which have received two removal orders in the previous 12 months.

exemption should also apply to very large online platforms (VLOPs) as designated under the Digital Services Act if they have a low risk of CSAM.¹⁰ This ensures a more precise and fairer regulatory framework by emphasising exposure to CSAM rather than based on the platform's size.

The DSA already requires VLOPs and very large online search engines to identify, analyse, assess and mitigate systemic risks their services pose to the protection of children.

Recommendation: Support the Parliament's risk assessment exemption for services with a low risk of CSAM. Include VLOPs with low risk of CSAM in this exemption, following the risk-based approach rather than focusing on their size.

Age assurance

We acknowledge the ongoing discussions about the need to introduce proportionate age assurance techniques.

However, the technology for establishing the age of users with a high degree of confidence, especially at a granular level for users under the age of 18, remains imprecise and potentially privacy intrusive.

This is an emerging area with no identified best practice as yet, with privacy-protective techniques still being established. Certainty, or a high degree of accuracy, about age would require providers to collect a substantial amount of private data from all users and track the activities of all children to ensure their access is age appropriate.

If not designed carefully, requirements to verify users' age can exclude certain groups, including adults and the most vulnerable users, who may lack the required form of identification or may be unable or unwilling to share information.

Recommendation: To develop an effective, proportionate risk-based solution which is both technically feasible and manages the trade-offs between providing age-appropriate protection whilst balancing privacy and access to information and services, we urge policymakers to continue discussions in the framework of the

¹⁰ Regulation (EU) 2022/2065.

Better Internet for Kids (BIK+) strategy and the EU Code of Conduct on age-appropriate design.¹¹

Data preservation

The Commission and Parliament propose a maximum period of 12 months for the retention of content and other data processed in connection with obligations under the Regulation.

We support imposing a general retention period in line with the storage limitation principle under the General Data Protection Regulation (GDPR),¹² namely that all content and other data processed in connection with the measures taken to comply with the Regulation should be stored no longer than necessary for the applicable purpose. Given the sensitivity of CSAM, we propose that this content is preserved for no longer than strictly necessary and, in any event, no later than 24 months from the date of the detection.

As the Parliament suggests, providers should be able to retain certain data for the purpose of improving the effectiveness and accuracy of detection technologies over time.

Recommendation: Given the sensitivity of the material, we propose that this content processed in connection with the legislation is preserved for no longer than strictly necessary and, in any event, no later than 24 months from the date of the detection.

As the Parliament suggests, providers should be able to retain certain data for the purpose of improving the effectiveness and accuracy of detection technologies over time.

EU Centre

We support the Commission's proposal to strengthen the European infrastructure and capacity to fight against child sexual abuse and exploitation. The EU Centre on Child Sexual Abuse, if sufficiently resourced, can help strengthen the EU-level response against this crime, focus on prevention, support victims, ensure better

¹¹ For more info see *EU Code of conduct on age-appropriate design*, available at <https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design>

¹² Regulation (EU) 2016/679.

coordination between Member States and international authorities, and help develop and share best practices across relevant service providers.


Interplay with the global framework


The requirement to report detected CSAM to the EU Centre creates a conflict of laws for US-established companies, who are currently legally required to report to the National Center for Missing and Exploited Children (NCMEC) when they become aware of CSAM on their platforms. Their ability to disclose the contents of a report elsewhere is proscribed by US statute.

The current proposal does not acknowledge that the reporting obligations to the EU Centre may conflict with the existing reporting and distribution laws in the US and other jurisdictions. We encourage the EU and US to intensify their dialogue to ensure that any services would be allowed to disclose to the EU Centre without falling foul of US law. However, until a solution to such conflict is found, it should be possible to continue central reporting to NCMEC as such reporting is recognised and established.

Recommendation: Intensify negotiations with the US authorities to avoid a conflict of laws regarding the reporting and distribution of CSAM. In the meantime, continued reporting to NCMEC should be allowed.

FOR MORE INFORMATION, PLEASE CONTACT:

 **Hugh Kirk**
Senior Manager for Consumer, IP and Platform Policy
hugh.kirk@digitaleurope.org / +32 490 11 69 46

 **Alberto Di Felice**
Policy and Legal Counsel
alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 108 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, LSEG, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Energy, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Tesla, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Vantiva, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ

Belgium: AGORIA

Croatia: Croatian Chamber of Economy

Cyprus: CITEA

Czech Republic: AAVIT

Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv

Estonia: ITL

Finland: TIF

France: AFNUM, SECIMAVI, numeum

Germany: bitkom, ZVEI

Greece: SEPE

Hungary: IVSZ

Ireland: Technology Ireland

Italy: Anitec-Assinform

Lithuania: Infobalt

Luxembourg: APSI

Moldova: ATIC

Netherlands: NLdigital, FIAR

Norway: Abelia

Poland: KIGEIT, PIIT, ZIPSEE

Portugal: AGEFE

Romania: ANIS

Slovakia: ITAS

Slovenia: ICT Association of Slovenia at CCIS

Spain: Adigital, AMETIC

Sweden: TechSverige, Teknikföretagen

Switzerland: SWICO

Turkey: Digital Turkey Platform, ECID

Ukraine: IT Ukraine

United Kingdom: techUK