ECLAG
Ending Child Sexual Abuse Online

Briefing note on the proposed Regulation combating child sexual abuse

December 2025

Every child has the right to be safe.

Europe is midst of an unprecedented Child Sexual Abuse Crisis. 1 in 5 children in Europe are subject to sexual violence and abuse. Reports of child sexual abuse have reached unprecedented levels – with more than 20 million global reports and over 63 million images and videos identified in 2024 alone. AI-generated abuse exploded by 400% in 2025, with 78% showing the most extreme forms of abuse. Sexual extortion and grooming reports surged 192% from 2023.

Behind these figures lie children who have to live with the lifelong trauma of their abuse, the horrendous violation of their rights, and the continued circulation of their abuse online. **Every child has the right to be protected from all forms of sexual abuse and the right to privacy.** With 62% of child sexual abuse webpages in 2024 traced to the EU, **the EU has a specific responsibility** to end this crisis and adopt ambitious legislation that ensures a safe digital environment for all children.

Our asks

ECLAG acknowledges the political realities that have shaped the Parliament's and Council's proposals. Progress is critical to ensure children are not left unprotected. ECLAG now urges EU negotiators to work toward an effective and comprehensive solution that:

- **Mandates child safety by design.** Platforms must be required to design their services with children's rights and needs at the forefront, assess the risk of child sexual abuse on their services and adopt risk mitigation measures.

- Establishes a **permanent legal basis for voluntary detection of all forms of abuse in all online spaces,** as part of risk mitigation measures. While not sufficient alone, proactive detection by online service providers has been instrumental in protecting children online over the past decades.

    - **Detection should cover all forms of child sexual abuse** (i.e. known child sexual abuse material (CSAM), unknown CSAM and grooming). Databases of known CSAM only exist because unknown CSAM can be detected, identified and added to existing databases. Detecting grooming is key in preventing the abuse before it occurs.

    - **Detection should not be limited to individual suspects.** Detecting the sharing of illegal material by suspects can already be authorised by an investigating judge. The scale of the issue requires technology to be used widely across platform's systems.

- **Mandates providers to report and expeditiously remove all CSAM notices** to the EU Centre for triage before law enforcement referral, with rapid removal protocols and strict penalties for non-compliance.

- Mandates providers at high risk of CSAM dissemination to **block upload of known CSAM** - material already confirmed as illegal by law enforcement. Upload prevention is a highly effective and widely-used tool across platforms. This prevents re-victimisation, reduces trauma, and eases the burden on platforms and authorities to repeatedly block the same known material.

- Allows **victims** and their representatives to request that platforms **detect, remove, and block CSAM depicting them**.

- Mandates providers at high risk of CSAM dissemination to **detect, report and expeditiously remove CSAM in publicly accessible content** to ensure online spaces meet safety standards.

- Implements **strong safeguards** to avoid any misuse of any detection technology and to ensure the fundamental rights of adult and child users are respected, including their right to privacy and protection.

- Is **technology neutral and future-proof** to ensure children are protected **in all online spaces,** and to enable the development and deployment of technical solutions in the rapidly evolving digital environment.

- Sets up a **strong EU Centre** which fits into the existing EU and global child safety ecosystem, and which includes a **Survivors' and Victims' Committee** which would provide policy recommendations to the EU Centre and contribute to subsequent related policy actions taken by the EU Commission.

The scale and urgency of the current Child Sexual Abuse Crisis demand an ambitious framework that **combines voluntary actions with enforceable obligations** to ensure action when providers fail to act. The suggested framework would represent a first step, laying a foundation to build a more comprehensive regulatory approach in the future. **Anything less would fall short of the responsibility we all share.**

In line with the UN Convention on the Rights of the Child, **EU representatives must protect children from child sexual abuse**, including in online environments. After three years of negotiations, it is urgent to adopt an effective and proportionate framework that prioritises the best interests of the child. **Together we can end the Child Sexual Abuse Crisis and protect children from further harm.**

Please find attached detailed overview of our proposed measures.

Annex - ECLAG proposed measures for the CSA Regulation, December 2025.

We ask for a **comprehensive, long-term and robust Regulation** that establishes:

1. Mandatory child safety by design

Mandatory risk assessment. The Regulation should require providers to carry out **child-rights impact assessments (CRIA)**. This will ensure that children's rights, including their right to be protected from violence, right to privacy and the best interests of the child, are fully accounted for.

Platforms should also assess the risk of their services being misused for disseminating CSAM or for committing child sexual abuse such as grooming. To assess the risk, ECLAG recommends a methodology that combines both an objective risk analysis (factors/environment-based) and, for existing platforms, an evidence-based risk analysis:

a. The risk factor/environment analysis should be based on multiple objective criteria, including:
   - The type of service,
   - Architecture and functionalities of the service (notably a safety-by-design architecture, user identification, age verification/assurance functionalities, end-to-end encrypted spaces),
   - Existing policies (taking into account the limited impact of policies in preventing risk).

b. This risk factor analysis must be based on:
   - Evidence of the service or evidence stemming from comparable services having been used in the past 12 months and to an appreciable extent for the dissemination of CSAM or the solicitation of children.

Mandatory mitigation measures. For providers that display a **significant risk** of being misused for the dissemination of CSAM or grooming after risk assessment and mitigation exercises, **the Coordinating Authorities should be empowered to mandate effective, targeted and proportionate measures, under the guidance of the EU Centre**. Such measures could include, but are not limited to:

- high-privacy by default for child accounts, including limiting the communication possibilities between adults and children,
- effective age verification,
- child-friendly, accessible and responsive reporting mechanisms,
- accessible blocking tools,
- sensitive content controls in private messaging (including keywords and nudity),
- automated content moderation tools with specialised CSAM identification capabilities,
- warnings and deterrence messages and/or blocking in upload and/or search of sensitive content
- Blocking upload of known CSAM (see below).

Mandatory transparency reports and audit. Following the model of the DSA risk assessment and mitigation reports, providers must **report** on the outcome of the risk assessment and on the child safety-by-design measures as well as any mitigation measures adopted in an annual report. They should also submit **an independent technical audit of child safety by design measures to the**

national Coordinating Authorities and the EU Centre, which should be able to collect relevant statistics about the use of such measures. The audits would cover, among others, the adequacy of the measures deployed (and for which user category), their effectiveness and the scope in terms of service and forms of abuse (known CSAM, unknown CSAM, child sexual abuse including grooming, and suspicious behaviours).

2. Permanent Legal Basis for Voluntary Detection

Voluntary detection already plays a critical role in tackling the millions of illegal child sexual abuse files circulating online. For more than a decade, more than 200 providers, from Google to Apple, have safely used trusted technologies like PhotoDNA to prevent their services from being used to share illegal child abuse material at scale. Without these tools, millions of abusive images would continue to circulate unchecked.

Voluntary detection of all forms of abuse. As long as technologies are vetted by the EU Centre, providers must be allowed **to detect all forms of child sexual abuse:** known child sexual abuse material (CSAM), unknown CSAM and grooming. Detecting new CSAM and grooming is crucial to stop ongoing abuse, protect children from imminent danger and enable police to arrest offenders:

- **Databases of known CSAM only exist because unknown CSAM can be detected**, identified and added to existing databases by trusted specialist organisations like the National Center for Missing and Exploited Children (NCMEC) and the Internet Watch Foundation (IWF). Without the continuous intake of newly identified material, these databases would quickly become outdated and lose their effectiveness. Moreover, it would be **unjustifiable to limit protection only to victims whose abuse has already been identified. All children who suffer sexual abuse deserve equal protection**, irrespective of whether the material depicting their abuse is currently known or unknown.

- **Detecting grooming is crucial to preventing abuse before it occurs**. Its exclusion would signal that children must wait until they have been abused and images and videos of their abuse have been circulated online before action can be taken. This is simply unacceptable. Excluding the detection of grooming within the voluntary schema would also **disincentivise technological innovation** in this area.

Voluntary detection drives innovation. Offenders constantly evolve their methods and providers need the flexibility to adapt and develop new detection tools to keep pace. Voluntary detection enables providers **to innovate responsibly and respond to emerging threats.** Under strong safeguards, they should be supported by the EU Centre to train and test their products on relevant data sets, in compliance with EU laws and standards for responsible innovation. In the absence of such support, European innovation in this domain risks being halted entirely, compromising child protection and the EU's capacity to maintain a leading role in the development of advanced safeguarding technologies.

Detection should not be limited to individual suspects. Targeted interception warrants to investigate the sharing of illegal materials by suspects can already be authorised by an investigating judge under strict conditions. **The scale of the issue requires technology to be used widely across platforms' systems**. Across the globe, thousands of people are constantly re-opening new accounts to target children and share millions of CSAM. Over the past years, 99% of the millions of images and videos reported were submitted by platforms using detection technology - a volume of identification that

public reporting could simply never achieve. In a month, Meta disabled more than 490,000 accounts for violating its child safety policies. Each month, Whatsapp detects and bans 300,000 accounts for suspected sharing of CSAM. And this is only the tip of the iceberg. To promptly remove this volume of unbearable content for human review, platforms need detection technologies.

3. Mandatory reporting and removal of CSAM (notice & takedown)

The Regulation should require online service providers to report and remove all notices of CSAM to the EU Centre, for a first triage, before referral to law enforcement. Mandatory reporting is crucial to identify perpetrators and rescue children. It also helps to build transparent European data - a key step toward understanding this complex and evolving crime. In a world of changing politics, the EU cannot depend on the US as the world's CSAM triage centre.

To ensure the efficiency of this obligation, the Regulation must :

- Impose substantial penalties for failure to report flagged CSAM.
- Empower the EU Centre with adequate competences and resources to triage CSAM, enforce the notice & takedown requirements and collect comprehensive statistics.

In line with the Digital Services Act, any notified instance of CSAM must be removed "expeditiously". The Regulation should mandate platforms to establish rapid response protocols for immediate action on CSAM reports and provide a maximum of 1 hour[1] for removal of CSAM. The faster material is removed, the sooner we stop its widespread dissemination, preventing further abuse and ending the trauma and privacy violation of children.

4. Mandatory blocking uploads of known CSAM

The Regulation should mandate providers that present a significant risk of being misused for the dissemination of CSAM to proactively block material that has already been confirmed by law enforcement authorities as illegal.

Upload prevention is a highly effective and widely used tool across a huge number of global platforms. Allowing known CSAM to reappear not only perpetuates the violation of victim's rights and deepens their trauma, but also creates unnecessary burdens for platforms and law enforcement, who must repeatedly detect, remove, and process the same illegal material.

5. Victim-initiated detection and removal requests

For a crime that knows no borders, the Regulation must deliver real justice for victims. Victims, survivors, and their legal representatives should be able to demand that National Coordinating Authorities and/or the EU Centre require platforms to c**ontinuously detect, remove, and block the upload of any CSA material depicting them**. They should also be able to submit content directly to the EU Centre, which can issue similar orders once the material is confirmed to meet the CSA definition. Such mechanisms must be **survivor-centered and trauma-informed**, grounded in the rights recognised under the Victims Rights Directive. This system is a**lready operating successfully in some countries**, triggered by cooperation between providers, law enforcement and hotlines (i.e.,

[1] Following the same approach of the time limit established for removal orders concerning terrorist content in EU Regulation 2021/784.

Report Remove, a service by the Internet Watch Foundation and the NSPCC in the UK which enables minors to confidentially report their own imagery to seek its removal).

At the same time, the Regulation must acknowledge that **non-EU victims** have their abuse spread and hosted by online service providers operating in the EU, in accordance with the Victims' Rights Directive 2012/29/EU which applies if the crime was committed in the European Union or if the proceeding takes place in the European Union, irrespective of the nationality or the residing status of the victim.

6. Mandatory detection in public space

The Regulation should mandate providers that display a significant risk of being misused for the dissemination of CSAM to **proactively detect illegal material on publicly accessible content**. This is critical to ensuring online public spaces meet the same safety standards expected offline.

Without such a mandate, platforms often prioritize growth and engagement over safety, leaving illegal material widely accessible. A legal obligation would also establish clear accountability standards, create consistency across the tech industry, reducing the uneven landscape in which some companies invest heavily in safety technologies while others do nothing. This consistency benefits both users and responsible companies by creating **a level playing field** where safety compliance is a shared baseline, not a competitive disadvantage. It would also spur innovation in privacy-preserving detection and moderation technologies and cross-platform collaboration frameworks.

7. A robust independent EU Centre

In the absence of mandatory detection, a strong and proactive EU Centre is crucial to ensuring the Regulation delivers meaningful child protection outcomes. While the Danish proposal preserves the Centre's key functions — coordination, triage, and support to national authorities — several enhancements are needed to make it effective and future-ready:

- **Legal authorization to detect CSAM in public spaces:** this will build in an additional layer of accountability for platforms.
- **Technical and risk guidance**: The Centre should develop detailed risk-assessment templates and technical guidance, including on good/bad practice mitigation measures, to ensure consistency across Member States and providers.
- **Technology evaluation and benchmarking**: The Centre should maintain a register of certified and benchmarked voluntary detection tools, assessing their accuracy, privacy compliance, and suitability for different service types. It could also provide recommendations on emerging technologies and privacy-preserving innovations to encourage safe uptake.
- **Transparency and reporting:** The Centre should publish periodic transparency reports summarising aggregated data on voluntary detection activities, reports processed, and response times. These reports would enable policymakers to monitor progress and identify systemic gaps in implementation.
- **Collaboration with existing ecosystem:** The EU Centre, as well as national Coordinating Authorities, should cooperate closely and integrate the work of the existing ecosystem, including all relevant helplines and hotlines (notably, but not limited to, CSAM, child safety, anti-trafficking, missing children, travel and tourism) as well as victims' support services, civil society organisations, and existing regulatory bodies.
- **Survivor, victim and expert engagement:** The Regulation should establish a Survivors' & Victims' Council and an expert advisory group to guide the Centre's work on prevention,

redress, and technology assessment. This would ensure that policy and operational choices remain grounded in both lived experience and technical evidence.

- **Innovation coordination**: The Centre should coordinate research and innovation projects on detection and prevention technologies and promote their interoperability across platforms.

By embedding transparency, accountability, and innovation into its mandate, the Centre would ensure baseline standards of protection while building the evidence and institutional capacity needed for a more comprehensive regulatory approach in the future. Without these enhancements, the voluntary model risks becoming a patchwork of good intentions with limited impact.

Additional resources

- ECLAG Myth Busting & Facts on the EU CSA Regulation
- Balancing The Right To Privacy With The Children's Right To Protection From Online Sexual Exploitation
- Briefing on technical solutions available to detect CSA in E2EE:
    - Balancing Cybersecurity, Privacy and Child Protection in detecting Child Sexual Abuse in End-to-End Encrypted Spaces
    - IWF - How Upload Prevention Protects Children Online
    - IWF - Preventing the upload of child sexual abuse imagery in end-to-end encrypted environments