Open letter to EU Member States on the proposed CSA Regulation

Dear Ministers and Ambassadors of EU Member States,

We, the undersigned European enterprises, as well as the European DIGITAL SME Alliance - which represents more than 45.000 digital SMEs across Europe, write to you with deep concern regarding the proposed Regulation on Child Sexual Abuse (CSA). Protecting children and ensuring that everyone is safe on our services and on the internet in general is at the core of our mission as privacy-focused companies. We see privacy as a fundamental right, one that underpins trust, security and freedom online for adults and children alike. However, we are convinced that the current approach followed by the Danish Presidency would not only make the internet less safe for everyone but also undermine one of the EU's most important strategic goals: progressing towards higher levels of **digital sovereignty**.

Digital sovereignty is Europe's strategic future

In an increasingly unstable world, Europe needs to be able to develop and control its own secure digital infrastructure, services, and technologies in line with European values. The only way to mitigate these risks is to empower innovative European technology providers.

Digital sovereignty matters for two key reasons:

- **Economic independence**: Europe's digital future depends on the competitiveness of its own businesses. But forcing European services to undermine their security standards by scanning all messages, even encrypted ones, using client-side scanning would undermine users' safety online and go against Europe's high data protection standards. Therefore, European users - individuals and businesses alike - and global customers will lose trust in our services and turn to foreign providers. This will make Europe even more dependent on American and Chinese tech giants that currently do not respect our rules, undermining the bloc's ability to compete.
- **National security**: Encryption is essential for national security. Mandating what would essentially amount to backdoors or other scanning technologies inevitably creates vulnerabilities that can and will be exploited by hostile state actors and criminals. For this exact reason, governments exempted themselves from the proposed CSA scanning obligations. Nevertheless, a lot of sensitive information from businesses, politicians and citizens will be at risk, should the CSA Regulation move forward. It will weaken Europe's ability to protect its critical infrastructure, its companies, and its people.

The CSA Regulation will undermine trust in European businesses

Trust is Europe's competitive advantage. Thanks to the GDPR and Europe's strong data protection framework, European companies have built services that users worldwide rely on for data protection, security and integrity. This reputation is hard-earned and gives European-based services a unique selling point Big Tech monopolies will never be able to match. This is one of

the few, if not the only competitive advantage Europe has over the US and China in the tech sector, but the CSA Regulation risks reversing this success.
This legal text would undermine European ethical and privacy-first services by forcing them to weaken the very security guarantees that differentiate European businesses internationally. This is particularly problematic in a context where the US administration explicitly forbids its companies to weaken encryption, even if mandated to do so by EU law[1].
Ultimately, the CSA Regulation will be a blessing for US and Chinese companies, as it will make Europe kill its only competitive advantage and open even wider the doors to Big Tech.

Contradictions weaken Europe's digital ambitions
The EU has committed itself to strengthening cybersecurity through measures such as NIS2, the Cyber Resilience Act, and the Cybersecurity Act[2]. These policies recognize encryption as essential to Europe's digital independence. The CSA Regulation should not undermine these achievements by effectively mandating systemic vulnerabilities.
It is incoherent for Europe to invest in cybersecurity with one hand, while legislating against it with the other.

European SMEs will be hit the hardest
Small and medium-sized enterprises (SMEs) would be hit hardest if obliged to implement client-side scanning. Unlike large technology corporations, SMEs often do not have the financial and technical resources to develop and maintain intrusive surveillance mechanisms, meaning compliance would impose prohibitive costs or force market exit. Moreover, many SMEs build their unique market position on offering the highest levels of data protection and privacy; which particularly in Europe is a decisive factor for many to choose their products over the counterparts of Big Tech. Mandating client-side scanning would undermine this core value proposition of many European companies.
This will suffocate European innovation and cement the dominance of foreign providers. Instead of building a vibrant, independent digital ecosystem, Europe risks legislating its own companies out of the market.

For these reasons, we call on you to:
- Reject measures that would force the implementation of client-side scanning, backdoors, or mass surveillance of private communications, such as we currently see in the Danish proposal for a Council position on the CSA Regulation.
- Protect encryption to strengthen European cybersecurity and digital sovereignty.
- Preserve the trust that European businesses have built internationally.
- Ensure that EU regulation strengthens, rather than undermines, the competitiveness of European SMEs.
- Pursue child protection measures that are effective, proportionate, and compatible with Europe's strategic goal of digital sovereignty.

[1] https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-chairman-ferguson-warns-companies-against-censoring-or-weakening-data-security-americans-behest
[2] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

Digital sovereignty cannot be achieved if Europe undermines the security and integrity of its own businesses by mandating client-side scanning or other similar tools or methodologies designed to scan encrypted environments, which technologists have once again confirmed cannot be done without weakening or undermining encryption. To lead in the global digital economy, the EU must protect privacy, trust, and encryption.

Signatories:

Blacknight (Ireland)

Commown (France)

CryptPad (France)

Ecosia (Germany)

Element (Germany)

E-Foundation (France)

European DIGITAL SME Alliance (Europe)

Fabiano Law Firm (Italy)

FlokiNET (Iceland)

FFDN (France)

Gentils Nuages (France)

Hashbang (France)

Heinlein Group (Germany)

LeBureau.coop (France)

Logilab (France)

mailbox (Germany)

Mailfence (Belgium)

Mailo (France)

moji (France)

Murena (France)

Nextcloud (Germany)

Nord Security (Lithuania)

Octopuce (France)

Olvid (France)

OpenCloud (Germany)

OpenTalk (Germany)

Phoenix R&D (Germany)

Proton (Switzerland)

Skylabs (Ireland)

Sorware Ay (Finland)

Soverin (Netherlands)

Startmail (Netherlands)

Surfshark (Netherlands)

TeleCoop (France)

The Good Cloud (Netherlands)

Tuta Mail (Germany)

Unicorns Lithuania (Lithuania)

Volla Systeme GmbH (Germany)

WEtell (Germany)

Wire (Switzerland)

XWiki SAS (France)

zeitkapsl (Austria)