CONFEDERATION OF INDUSTRY
OF THE CZECH REPUBLIC

PRAGUE, SEPTEMBER 4, 2023

Spanish Presidency of the Council
European Commissioner for Home Affairs Ylva Johansson and DG HOME
MEPS

Joint letter from European industry players:

The Child Sexual Abuse Regulation must be balanced, technologically neutral and future-proof

Dear Madam/Sir,

The undersigned organizations and their members have been long committed to combating online child sexual abuse (CSA) and fully share the objectives of the European Commission to prevent and fight these crimes. Cooperation between regulators, tech companies, law enforcement agencies, governments and civil society is crucial in the process - and so is a sound legal framework that is effective, balanced, technologically neutral and future-proof.

We welcome the progress made in the European Parliament so far. We believe these improvements maintain the essence of the proposal while providing more feasible options for the industry to continue to innovate in this space while also further scaling their efforts.

While we applaud the Spanish Presidency's commitment to reaching a compromise, considering the complexities of the proposal, we warn against adopting a rushed general approach in the EU Council, without addressing the most critical aspects of the legislation. In this regard, we share concerns expressed by the European Data Protection Board and the European Data Protection Supervisor about the impact of the proposal on the fundamental rights, particularly to privacy and the protection of personal data, in addition to the lack of legal clarity related to detection and delisting orders.

To address our concerns, we propose the following five points that can contribute to creating a sound and proportionate legal framework, with the ultimate goal of benefitting society and keeping children safe:

1. Given the extremely high stakes, **it is critical to find the right balance between protecting children and privacy**. We believe it is possible to strike such a balance by carefully evaluating the feasibility of technological solutions, allowing innovation to continue in this space and by avoiding enshrining broad legal actions that would violate fundamental rights. Any technology should be developed and discussed continuously in close cooperation with industry. The required technical solutions should be implementable on a technical level without interfering with digital infrastructure and networks. The proposal should recognize the crucial role that encryption technologies, including end-to-end

PHONE (+420) 225 279 111 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADDRESS FREYOVA 948/11, 190 00 PRAGUE 9, CZECH REPUBLIC

encryption play in providing private and secure communications for users, including children. Strong encryption, including end-to-end encryption, protects users' sensitive data – including individuals, corporations, and governments. Requiring providers to engineer vulnerabilities into products and services would undermine the security and privacy of customers' data. In cases where encryption is used in the cloud, any request to break encryption could also undermine the information technology infrastructure and leave customers with sensitive data exposed.

2. **Without voluntary actions and an appropriate derogation from the relevant provisions of the e-Privacy Directive, some services will not be able to proactively search for illegal content**. Providers may need to stop detection of online child sexual abuse in certain services while they wait for a detection order, which could lead to a gap in online child safety. We propose providing a clear legal basis and long-term derogation from the ePrivacy Directive to allow providers of electronic communications services to continue to innovate and carry out voluntary detection efforts. We believe that the current e-Privacy Directive derogation is transparent, proportionate and reliable.

3. **Detection and delisting orders must be a measure of last resort**. They need to be flexible, with appropriate safeguards. The text should clarify that services should exhaust all risk mitigation measures before a detection or delisting orders can be issued. This is why voluntary efforts must be maintained. In addition, it is unclear how providers could meet this obligation without breaching the prohibition of general monitoring obligations since human review remains essential[1], and detecting these types of CSA cannot be fully automated through to enforcement decision making. Legal mandates should be only used as last resort measures where voluntary efforts and other risk mitigates are deemed insufficient and, then, only when such orders do not violate the prohibition on general monitoring.

4. **Narrow the scope of detection orders to appropriate service providers**: the legislation should focus on services that present high risk of abuse due to their nature. Software application stores, search engines, number-based interpersonal communication services and cloud infrastructure providers are examples with low risk due to the nature of the service. Similarly, interpersonal communication services and cloud infrastructure providers are not well placed to take action due to technical and contractual limitations We propose keeping only high-risk service providers that are able to act in scope, while the order should be directed first and foremost to the hosting service to which it was uploaded.

5. **The regulation should be aligned with other pieces of EU legislation** to prevent the fragmentation of the digital single market. The legislation should build upon the recently adopted Digital Services Act (DSA) and its risk assessments. Governments should avoid any action requiring companies to

[1] Tech Coalition, 2022. Research Paper: Considerations for Detection, Response, and Prevention of Online Grooming: https://paragonn-cdn.nyc3.cdn.digitaloceanspaces.com/technologycoalition.org/uploads/Research-Paper-Online-Grooming-Considerations-for-Detection-Response-and-Prevention-of-Online-Grooming.pdf

create security vulnerabilities in their products and services, while preserving its ban on general monitoring, and carefully map out the interplay between other pieces of legislation.

We are aware of the high stakes this legislation involves - fulfilling the goals of the legislation is crucial for all stakeholders, and above all, for children. We believe that our proposed solutions help find such a framework.

We remain committed to fighting child abuse online and helping co-legislators reach a strong long-term legislation to tackle child abuse online in the most effective, balanced, technologically neutral and future-proof way.

The Confederation of Industry of the Czech Republic, on behalf of the undersigned organizations.

adigital

ASIC Association des Services Internet Communautaires

CCIA Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

DIGITAL POLAND

DANISH ENTREPRENEURS

DI Confederation of Danish Industry

SP CONFEDERATION OF INDUSTRY OF THE CZECH REPUBLIC


iab
polska


infobalt
LITHUANIA


ITI


LEWIATAN


LIKTA
LATVIAN INFORMATION
AND COMMUNICATIONS TECHNOLOGY
ASSOCIATION


sapie