

Second DSA Report on Systemic Risks

Anna Pingen

News

On 1 July 2026, the European Board for Digital Services, in cooperation with the European Commission, published its [second report](#) under Art. 35(2) of the Digital Services Act (DSA) on the most prominent and recurrent systemic risks as well as mitigation measures. The reporting period covered by the second report was from 17 February 2025 to 16 February 2026.

The report concerns the DSA risk-management framework for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). Under Arts. 34 and 35 DSA, these providers must assess systemic risks arising from the design, functioning, and use of their services, including their algorithmic systems, and put in place reasonable, proportionate, and effective mitigation measures. The report is based on a broad range of sources.

The systemic risks identified in the report are grouped into several categories, including:

- Risks linked to illegal content, such as illegal products and services, child sexual abuse material, terrorist content, illegal hate speech, and intellectual property infringements;
- Negative effects on fundamental rights, including freedom of expression and information, non-discrimination, children's rights, consumer protection, privacy and data protection;
- Risks to civic discourse, electoral processes and public security;
- Risks linked to gender-based violence, public health, the protection of minors, and physical and mental well-being.

A particular focus is placed on the protection of minors who are concerned with the most prominent and recurrent systemic risks identified: grooming, exposure to harmful or age-inappropriate content, unsafe account settings, addictive or compulsive design features, cyberbullying, and the dissemination of AI-generated or manipulated sexual content.

The report further discusses how artificial intelligence affects several risk categories: sexual abuse material, illegal hate speech, disinformation, gender-based violence, public security, and health misinformation. At the same time, it also refers to mitigation measures involving automated tools, hash-matching, detection systems, content provenance standards, AI-generated content labels, watermarks, and AI red-teaming.

As regards mitigation, the report does not identify any measures as “best practices” or “good practices”. Instead, it maps mitigation approaches currently reported or observed across different types of services: terms and conditions and their enforcement, content moderation and risk detection, safety-by-design meas-

AUTHOR

Anna Pingen 

Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

Preprint eucrim 2026, Vol. 21(2)

ISSN: 1862-6947

<https://eucrim.eu>



ures, user empowerment tools, awareness measures, and out-of-court dispute settlement. Additional measures cover social media platforms, online marketplaces, pornographic platforms, and online search engines.

The report highlights the importance of stakeholder engagement and data access. It reiterates that effective risk assessment and mitigation should involve users, affected groups, civil society organisations, independent experts, and researchers. It further notes that reliable data access and third-party scrutiny are important for identifying systemic risks and assessing whether mitigation measures are effective or not.

In its outlook, the report underlines that the DSA risk-management framework is still in the early stages of implementation. Future reports are expected to benefit from enforcement practice, stakeholder expertise, monitoring under DSA codes of conduct, and research outputs resulting from the Art. 40 DSA data-access mechanism.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the [Union Anti-Fraud Programme \(UAFB\)](#), managed by the [European Anti-Fraud Office \(OLAF\)](#).



**Co-funded by
the European Union**