

EuroISPA Position Paper on the Digital Omnibus on Data and Cyber

INTRODUCTION

EuroISPA welcomes the European Commission's efforts to simplify the EU digital regulatory framework through the Digital Omnibus Package. A forward-looking and ambitious simplification agenda is essential to strengthen Europe's competitiveness, enhance legal certainty, and ensure that the EU digital acquis is fit for the next decade.

The main focus of this paper is the first Digital Omnibus Package covering data and cybersecurity. While we acknowledge and support several constructive steps taken by the Commission, we believe that further simplification is both possible and necessary. In particular, simplification should not only address individual provisions within legislative instruments but also tackle overlaps, inconsistencies, and fragmentation across the broader digital acquis.

Below, we outline EuroISPA's key recommendations.

GDPR & ePrivacy

EuroISPA is concerned that the current approach creates a fragmented regime between personal and non-personal data and does not resolve the long-standing split between the GDPR and ePrivacy Directive.

As outlined in previous positions, EuroISPA thinks that the EU should repeal the ePrivacy Directive, which is outdated and creates regulatory challenges. The proposals in the Digital Omnibus are a step in the right direction, but not enough; the principle of confidentiality of communications should be preserved and integrated into a harmonised legal framework that encompasses all communication providers, technologies, and usages (e.g. the Digital Networks Act).

1) Article 88a: narrow exemptions

The proposed exemptions to consent requirements in new Article 88a are too narrow to meaningfully address cookie fatigue. They risk creating a dual regime and failing to reduce complexity in practice. Exemptions should explicitly cover low-risk, non-profiling activities, including contextual advertising and its essential safety features, as well as fraud prevention and software updates. Expanding these exemptions would materially reduce unnecessary consent prompts while incentivizing privacy-by-design models.

2) Article 88b: browser-level consent

The proposed browser-level consent mechanism in new Article 88b is overly complex and risks creating “consent confusion” rather than solving user fatigue. It may also undermine the economic viability of ad-supported content models, including privacy-preserving contextual advertising. EuroISPA recommends deleting Article 88b.

More broadly, the rapid evolution of the proposal compared to earlier drafts raises concerns regarding legal certainty and stakeholder consultation.

3) Support for the Digital Omnibus proposals on pseudonymisation

Current anonymisation/pseudonymisation standards are set so high by Data Protection authorities that, in practice, full compliance is often unattainable. Easing these requirements would enable greater use of data, fostering the development of AI-based services and supporting innovation and more digitalised business models in the EU.

EuroISPA therefore supports the changes proposed in the Digital Omnibus that reflect the SRB caselaw and welcomes the introduction of the new definition of scientific research to be integrated under GDPR Article 4 (new paragraph (38)), which clarifies that GDPR provisions on academic research also apply to projects involving commercial participation, in line with Recital 159 of the GDPR.

EuroISPA also supports the objective of providing greater clarity regarding Data Protection Impact Assessments (DPIAs) and ensuring greater consistency across the EU on when they are required.

Cybersecurity

EuroISPA supports the creation of a Single Entry Point (SEP) for incident reporting managed by ENISA, as proposed in Article 6 of the Digital Omnibus amending article 23 of the NIS2 Directive. This is a promising step toward simplification. However, a single portal alone will not deliver regulatory relief unless accompanied by deeper harmonisation and sufficient regulatory clarity.

1) A Unified EU reporting framework

The Single Entry Point Platform must be built upon harmonised definitions, timelines, thresholds, and templates across NIS2, DORA, the Cyber Resilience Act (CRA), the AI Act, and GDPR. Without alignment, the portal risks merely consolidating fragmentation.

We recommend:

- A single EU-wide reporting template for cybersecurity and data breach notifications.
- Standardised definitions to provide legal and operational clarity on when cyber reporting obligations are triggered, what constitutes a reportable incident, and to prevent overlapping or duplicate notifications across regulatory frameworks.

EuroISPA

Rue de la Loi 38, 1000 Brussels

secretariat@euroispa.org

EU Transparency Register: 54437813115-56

- Harmonised reporting timelines, ideally centred around a consistent 72-hour deadline and aligned trigger points.
- Significantly raised thresholds to prevent overreporting and focus on incidents with systemic or economic impact.

2) Conformity assessments and auditing

Beyond reporting, the EU should align conformity assessment approaches across frameworks such as NIS2, DORA, and the CRA. Establishing a more centralised system with mutual recognition between Member States would help eliminate duplicate audits and ease administrative requirements. Reducing overlapping assessment obligations would lower compliance costs for businesses while still supporting strong cybersecurity protection throughout the European Union and delivering better outcomes for end-users.

3) Governance and resources

ENISA must be adequately resourced to fulfil its mandate and to develop and maintain the Single Entry Point Platform. The development and deployment of the SEP platform should be supported by clear regulatory direction and ongoing, transparent consultation with Member States, industry stakeholders, and private sector partners, ensuring effective implementation, practical usability, and broad operational acceptance.

CONCLUSION

EuroISPA supports the Commission's simplification agenda and welcomes several constructive elements in the Digital Omnibus Package. However, simplification must go beyond procedural adjustments and address structural fragmentation, overlapping obligations, and inconsistent enforcement.

A truly competitive and innovation-friendly Digital Single Market requires harmonised rules, coherent enforcement, proportionate risk-based obligations, and practical compliance mechanisms. We stand ready to engage constructively with EU policymakers to ensure that the Digital Omnibus delivers meaningful and lasting simplification for Europe's digital ecosystem.

EuroISPA

Rue de la Loi 38, 1000 Brussels

secretariat@euroispa.org

EU Transparency Register: 54437813115-56