Employers entrusted to deliver
Sustainability Growth Innovation

Position Paper

Response to the Call for Evidence - Digital Omnibus

14 October 2025

SGI EUROPE GENERAL SECRETARIAT Rue des Deux Eglises, 26 bt 5, BE – 1000 Brussels
T: + 32 (0) 2 219 27 98 | F: + 32 (0) 2 218 12 13 | E: SGIeurope@SGIeurope.org | www.SGIeurope.org
Registered stakeholder
ID Nr 59513031434-92

SGI europe

Employers entrusted to deliver
Sustainability Growth Innovation

Position

Introduction

SGI Europe, representing enterprises and employers providing services of general interest across Europe, welcomes the European Commission's initiative to simplify and improve the coherence of the EU's digital rulebook through the **Digital Omnibus**.

Providers of SGIs – including municipal utilities, broadcasters, digital infrastructure operators and local authorities – are strongly committed to digital transformation that supports competitiveness, sustainability, and citizens' trust.

However, the growing volume and complexity of the **EU digital acquis** – including the Data Governance Act (Reg. 2022/868), NIS2 Directive (Dir. 2022/2555), Cyber Resilience Act (Reg. 2024/1787), AI Act (Reg. 2024/1689), GDPR (Reg. 2016/679) and eIDAS 2.0 (Reg. 2024/1183) – has created challenges for compliance, particularly for smaller public and municipal actors.

SGI Europe supports a simplification agenda that reduces administrative burden, strengthens legal clarity, and ensures proportionality **without weakening the core objectives of the digital rulebook**: protection of fundamental rights, cybersecurity, innovation, and public trust.

Coherence and clarity across the digital acquis

The coexistence of multiple EU acts with overlapping definitions and reporting requirements has led to uncertainty and duplication.

SGI Europe recommends the Digital Omnibus should:

- **Clarify terminology and scope** across the Data Governance Act (DGA), Data Act (DA) and Open Data Directive (ODD). Key terms such as "data holder", "reuse", and "bodies governed by public law" should be harmonised to avoid divergent interpretations.
- **Ensure coherence between DGA Chapter III and Data Act Chapter VIII**, to clarify when each applies and whether obligations are cumulative.
- **Align references to "critical infrastructure"** across the different pieces of legislation, to prevent inconsistent implementation at national level.
- **Provide clear, consolidated guidance** on the relationship between data, AI, cybersecurity, and privacy legislation, possibly through a Commission Communication or staff working document accompanying the Omnibus.

Such clarifications will promote consistent enforcement, reduce unnecessary compliance costs, and increase confidence among public and private operators.

Simplified and harmonised reporting obligations

Public and municipal operators often face multiple, parallel reporting duties under different frameworks, such as the GDPR (Article 33), NIS2 Directive (Articles 23–30), and Cyber Resilience Act (Articles 14–16).

SGI Europe supports efforts to:

- **Develop a Single Reporting Platform (SRP)** at national or EU level to streamline incident and data breach notifications, provided that it demonstrably reduces burden and ensures data security.
- **Harmonise timelines and thresholds** for reporting incidents, taking into account weekends and public holidays in the 72-hour GDPR notification rule.
- **Promote interoperability between NIS2 and eIDAS 2.0 reporting frameworks**, as both apply similar duty-of-care and risk management obligations to public authorities.
- **Longer deadlines of 18-24 months after entering into force for all provisions** which require the local authorities to implement of supporting programmes and more mature IT processes should be given.

Simplified reporting should not reduce the quality of oversight but should ensure that each report serves a clear regulatory purpose.

Proportionality and practical support for local and public operators

To ensure that simplification has a tangible impact on the ground, SGI Europe calls for:

- **Clear, practical guidance and model templates** from supervisory authorities to support smaller entities in fulfilling compliance obligations, especially under the Data Act, AI Act and NIS2 Directive.
- **Encouragement of voluntary codes of conduct and certification mechanisms** under the GDPR (Articles 40–42) and AI Act (Article 69) to provide standardised, low-burden compliance pathways.
- **Sufficient transition periods** for new or amended obligations, avoiding changes while legislation is still being implemented nationally (as seen with NIS2).
- With the implementation of the NIS2 Directive, the number of entities required to report incidents is expected to rise sharply. It is already difficult for local authorities to keep an overview of the various reporting channels. A proposal would be to **establish a 'one-stop shop' approach, where security incidents can be reported via a single portal.**
- **Centrally provided digital tools, templates and process support** would be an important contribution to ensuring that local authorities are not overburdened while still guaranteeing a high level of protection.

Such measures will ensure simplification leads to legal certainty, not further complexity.

Data governance and protection of sensitive information

SGI providers frequently handle data essential for the operation of **critical infrastructures** and for the protection of public security.

SGI Europe therefore recommends:

- Maintaining existing **security exemptions**, notably Article 13(1) of the INSPIRE Directive (2007/2/EC), to prevent disclosure of sensitive infrastructure data.

- Preserving **sectoral exemptions** under Article 3(2)(b) of the DGA and Article 1(2)(i) of the ODD, which safeguard public service broadcasters' editorial independence and intellectual property.
- Clarifying that simplification measures will **not alter national security provisions** or the protection of critical infrastructure data.
- **Longer deadlines of 18-24 months** after entering into force for all provisions which require the local authorities **to implement of supporting programmes and more mature IT processes** should be given.

Simplification should improve clarity on when and how data sharing applies; not extend obligations in ways that could undermine public interest or security.

The goal of **simplifying data sharing** is to **enhance clarity** regarding its application, **not to broaden obligations** in a manner that could compromise public interest or security.

For this reason, **retaining this exception in the INSPIRE Directive is paramount** for the continuous security of critical infrastructure. Maintaining this safeguard **mitigates the escalating risk of manipulation and hybrid attacks**, particularly as the volume of technical and geographical data grows. The danger lies in the aggregation of data: even disparate datasets, when compiled, can form a comprehensive picture, thus **exposing sensitive infrastructure to attack**. These intentional assaults and manipulations not only pose a security threat but also cause **substantial financial losses** for businesses, diverting funds that are crucial for necessary transformation investments. The existing exemption is considered **necessary, proportional, and consistent** with both the **NIS2 Directive (2022/2555/EU)** and the **Critical Entities Resilience (CER) Directive (2022/2557/EU)**.

Artificial Intelligence Act implementation

SGI Europe supports the full and timely implementation of the AI Act (Reg. 2024/1689) and sees no need to reopen or delay its provisions. However, early guidance and alignment with related rules are essential.

We recommend that the Digital Omnibus should:

- **Clarify the relationship between Articles 25–28 of the AI Act** (provider/deployer responsibilities) and existing product safety legislation.
- Promote a **harmonised assessment model** combining the Fundamental Rights Impact Assessment (Article 27 AI Act) and the Data Protection Impact Assessment (Article 35 GDPR) to avoid duplication.
- Support the development of **certification schemes** under Article 43 AI Act, particularly for public sector procurement of trustworthy AI systems.
- **Clarify under which conditions AI components in critical infrastructures** (e.g. pressure sensors in water supply systems, autonomous control robots in power plants, intelligent cameras with image recognition) **are considered "safety components"** within the meaning of Article 3(14) of the AI Act. In this context, it should also be specified what is meant by the phrase "part of a product or AI system" in the legal definition of "safety component".
- Regarding Recital 55, **describe in more detail what is meant by 'exclusively for cybersecurity purposes'** as it is not always possible to make a clear distinction between cybersecurity and physical security, with cyberattacks often having direct physical (security) consequences.

The successful use of artificial intelligence in Europe requires a **coordinated and secure exchange of data, which, through clear guidelines, scalable data formats and common standards** among all stakeholders, enables a robust and innovative AI ecosystem.

ePrivacy and user consent

SGI Europe recognises the practical challenges of ePrivacy compliance and the issue of "consent fatigue" among users. Simplification should aim to **harmonise interpretations** across Member States while maintaining user trust.

We support:

- Aligning the ePrivacy Directive (2002/58/EC, Article 5(3)) with the GDPR's risk-based approach by exempting low-risk, non-intrusive cookies (e.g. audience measurement, functional cookies) when sufficient safeguards are in place.
- **Streamlining consent management** through technical solutions that remain compliant with the GDPR (Article 7), while avoiding mandatory centralisation that could disrupt user–service relationships or introduce gatekeeping risks.
- Developing **European guidance** on simplified and harmonised consent practices, in line with EDPB Guidelines 2/2023.

European Digital Identity and eIDAS 2.0

The forthcoming eIDAS 2.0 Regulation (Reg. 2024/1183) introduces substantial changes, including the European Digital Identity Wallet and the planned EU Business Wallet. SGI Europe welcomes this as a step toward greater interoperability but notes that implementation could create unnecessary administrative complexity.

SGI Europe recommends:

- **Clarifying Articles 5f(1) and 45b(2)** to ensure obligations on public sector bodies are proportionate and clearly limited to cross-border services.
- Ensuring that **delegated acts under eIDAS 2.0** are coordinated and prepared more transparently, encompassing meaningful consultation with stakeholders, including local and regional authorities.
- Promoting interoperability between the **identity wallet and the business wallet** and exploring reuse of European components from the Once-Only Technical System.

Ensuring equal treatment of public and municipal enterprises

SGI Europe reiterates that simplification measures should also apply to **municipal and public enterprises** meeting the same size criteria as SMEs or mid-caps.

We encourage the Commission to:

- Review Article 3(4) of Annex I to the General Block Exemption Regulation (Reg. 651/2014) to allow participation of public entities meeting SME thresholds; and
- Ensure that simplification measures in the Digital Omnibus apply equally to **public mid-caps and mixed-ownership operators**, thereby fostering fair competition and innovation.

SGI europe

Employers entrusted to deliver
Sustainability Growth Innovation

Position

Securing a competitive and privacy-conscious Digital Single Market

The future of Europe's digital economy hinges on a sustainably competitive and innovative connectivity ecosystem. Yet, European telecom operators, the essential providers of digital infrastructure, are confronted with an a significantly outdated, fragmented and disproportionate regulatory framework that stifles investment and creates an unsustainable competitive disadvantage against Big Tech platforms. **SGI Europe urgently calls on the European Union to implement a bold simplification agenda that ensures fair competition between all market players** and is committed to measures for the long-term health of the sector, primarily to safeguard consistent data privacy and consumer protection for all European citizens.

Ensuring a level playing field with "Big Tech" companies

The core principle guiding regulatory reform must be **functional equivalence**. When services – such as voice, messaging, and email – are substitutable in practice, users must benefit from **consistent protection, regardless of the provider**. Currently, the disparity is stark: telecom operators face sector-specific regulation across numerous policy areas, while functionally **equivalent services offered by Big Tech are subject to significantly fewer obligations**. This regulatory imbalance is not merely an administrative burden for telecoms; it is a fundamental gap in consumer safeguards.

This asymmetry **undermines end-user data privacy and locks consumers into dominant platforms**. Telecom operators are burdened by dual and often conflicting data breach notification rules under both GDPR (Regulation (EU) 2016/679) and the legacy ePrivacy Directive (2002/58/EC). Meanwhile, Big Tech escapes the vital obligations of provider switching and number portability, creating functional lock-in for services like messaging and cloud storage.
A **more balanced, future-oriented approach** requires reevaluating whether existing sector-specific obligations remain necessary, simplifying the landscape by relying on robust horizontal rules, and closing critical regulatory gaps where they exist.

SGI Europe recommends:

- **Harmonise Data Privacy & streamline ePrivacy: streamline the ePrivacy Directive (2002/58/EC)** to eliminate the costly dual regulatory burden with **GDPR (Regulation (EU) 2016/679) and ensure the consistency between the two**. The core **Principle of confidentiality of communications** must be consolidated into a modern, horizontal framework to ensure consistent privacy protection across all functionally equivalent services, including those offered by Big Tech.

Conclusion

SGI Europe supports the European Commission's intention to simplify the EU's digital framework in a **coherent, proportionate, and evidence-based** manner.

We emphasise the following priorities:

- Maintain the integrity of core regulations such as the GDPR, AI Act, and Cybersecurity Act.
- Improve coherence and consistency across the digital acquis.
- Simplify reporting and reduce overlaps between supervisory authorities.
- Ensure proportionate obligations and guidance for smaller and public entities.
- Safeguard data security, privacy, and SGIs' values throughout simplification.

The Digital Omnibus should deliver genuine simplification without reopening fundamental compromises or reducing the protection of citizens and public interest.