EU Affairs Team

FERMA MONTHLY REPORT: DECEMBER 2025

Digital Committee

Welcome to this month's EU regulatory Update.

1) Cyprus Council Presidency Priorities

Following the adoption of the Cyprus Presidency's programme for the first half of 2026, an initial overview of its digital and cybersecurity priorities has been prepared by the EU affairs team at FERMA to support internal policy discussions. The programme builds on the Trio Presidency agenda and focuses on consolidating recent legislative achievements while ensuring their effective and coherent implementation across Member States.

The Presidency places strong emphasis on **cyber resilience and operational security**, with particular attention to the implementation phase of major legislative acts. This includes supporting Member States and EU bodies in the early application of **NIS2**, **DORA**, and the **Cyber Resilience Act**, as well as facilitating coordination on supervisory practices and enforcement approaches. Cyprus also signals interest in advancing preparatory work for the future review of the **Cybersecurity Act**, notably in relation to EU cybersecurity certification schemes and ENISA's evolving role.

The Presidency will also oversee further implementation and coordination on horizontal digital legislation, including the **Digital Services Act** and **Digital Markets Act**, while contributing to the gradual rollout of the **AI Act**. Across these files, Cyprus underlines the importance of proportionality, legal certainty, and administrative simplification, while acknowledging that more substantive legislative reforms are likely to be addressed in subsequent policy cycles.

2) FERMA amendments to the digital omnibus

Following the publication of the European Commission's **Digital and AI Omnibus Package on 19 November 2025** and based on the input provided by its digital committee, FERMA is

finalising the drafting of targeted amendments reflecting the perspective of risk managers and their role in strengthening the cyber and digital resilience of EU companies. These proposals build on FERMA's long-standing support for the EU digital agenda while responding to persistent challenges linked to regulatory fragmentation and complexity.

FERMA welcomes the Omnibus as a **positive signal for businesses** and an opportunity to improve consistency across key legislative frameworks through the **implementation of a single-entry point (SEP)** and enhanced proportionality for SMEs, including the **AI Act, GDPR, NIS2 and DORA**. At the same time, FERMA underlines that **simplification should go beyond reducing administrative burden** and instead support a more strategic and holistic approach to risk management while **enhancing proportionality, especially for SMEs**.

Overall, FERMA's amendments seek to reinforce a **risk-based, proportionate and coherent regulatory framework** that enables companies to manage digital, cyber and AI risks effectively, while supporting the EU's broader resilience and competitiveness objectives.

Next steps

- Members are still welcome to **provide feedback to FERMA as soon as possible** based on the Commission's proposal.
- FERMA will circulate its amendments to members for their approval once they are finalised.
- The next advocacy steps will be discussed during **FERMA's Digital Committee** meeting taking place on **Friday 23 January from 11:00 to 12:00** (Brussels time).

3) Digital fitness Check

Following the European Commission's launch of a **Call for Evidence on the Digital Fitness framework**, FERMA has begun assessing how this initiative may shape the future coherence and effectiveness of EU digital legislation. The exercise aims to gather stakeholder input on whether existing digital rules are fit for purpose, proportionate, and aligned with the EU's competitiveness and resilience objectives.

The Commission's initiative seeks to evaluate how digital legislation operates in practice, with a particular focus on **regulatory complexity, overlaps between legal instruments, and the cumulative burden on companies**. It also explores whether current frameworks sufficiently support innovation, cybersecurity, and risk management in an increasingly digitalised economy.

From a risk management perspective, the Call for Evidence is a timely opportunity to highlight challenges linked to **fragmented reporting obligations, inconsistent**

definitions, and parallel governance requirements across digital, data, cybersecurity and AI legislation. FERMA sees particular relevance in the assessment of how multiple frameworks interact in practice and whether they allow companies to adopt integrated, enterprise-wide risk management approaches rather than siloed compliance models.

The Commission also invites views on **proportionality, especially for mid-sized companies**, and on how enforcement and supervision function across Member States. These elements are of direct interest to FERMA members, given the operational realities faced by organisations navigating complex and evolving digital risk landscapes.

Next steps

- FERMA will use its comprehensive Digital Omnibus position paper in order to respond. Nonetheless, FERMA encourages its members to contribute to this Call for Evidence should they wish to stress additional points.
- **The deadline for submitting contributions is Friday 11 February COB.**

4) TELE Council meeting – feedback from Member States on Digital Omnibus

On 5 December, EU ministers responsible for telecommunications and digital policy met in the framework of the **Telecommunications Council (TELE)** to exchange views on **simplification and digitalisation**, with a focus on **reducing regulatory burdens for businesses** while strengthening the EU's digital competitiveness.

Executive Vice-President Virkkunen presented the Commission's approach, structured around three pillars: a **Digital Omnibus** to fine-tune core digital legislation, a **Data Union strategy** to expand access to high-quality data for AI, and a **European Business Wallet** enabling fully digital business-to-government interactions. She underlined that the **Digital Omnibus represents only a first step**, to be followed by a broader **Digital Fitness Check** assessing cumulative impacts, overlaps and inconsistencies across the digital rulebook. EVP Virkkunen called for **rapid and visible progress**, urging Member States to deliver concrete results by **June 2026** and to make the Omnibus a "high-speed" boost for businesses and citizens.

Member States broadly welcomed the **Digital Omnibus as an initial move to cut bureaucracy and support innovation**. Many delegations stressed the need for **cross-cutting and evidence-based simplification across the entire digital acquis**, supported by the upcoming Digital Fitness Check. Several countries highlighted the importance of **realistic implementation timelines, timely guidance and standards, and consistent interpretation across Member States**, while cautioning that **simplification should not lead to deregulation or the weakening of core safeguards**.

Discussions also highlighted **persistent overlaps between digital legislation**, notably between the **AI Act and the GDPR, Data Act, Cyber Resilience Act and NIS2**. A number of delegations warned that these frictions risk **duplicated risk assessments and reporting obligations**, particularly for **SMEs and mid-sized companies**. Calls were made for **clearer definitions and thresholds for high-risk AI systems**, proportionate obligations, and more pragmatic transition periods.

Cybersecurity featured prominently in the exchanges, with many ministers pointing to **overlapping cyber incident-reporting requirements** across EU legislation. Several Member States advocated for **greater harmonisation**, including **common templates** and, where appropriate, **centralised reporting mechanisms**, while stressing that any single entry point must fully respect **national security competences** and meet the highest security standards.

Finally, ministers underlined the role of **digital tools in reducing compliance burdens**. Many supported **interoperable, digital-by-design solutions**, including automated compliance processes, AI-based regulatory tools, standardised documentation and interoperable platforms. The future **European Business Wallet** was highlighted as a key enabler, provided it remains compatible with national systems.

Overall, the TELE Council confirmed strong political support for a **more coherent, proportionate and digitally enabled EU regulatory framework**, closely aligned with **FERMA's priorities** on simplification, harmonised reporting and risk-based implementation of digital legislation.

5) Cybersecurity act review: what to expect

The European Parliament Research Service has published a briefing examining what to expect from the **upcoming review of the EU Cybersecurity Act**. The assessment comes at a time when cyber risks continue to increase and when companies are facing a growing number of overlapping cybersecurity and digital obligations at EU level.

The briefing recalls that the **Cybersecurity Act**, in force since 2019, gave ENISA a permanent mandate and created the EU cybersecurity certification framework for ICT products, services and processes. While the Act has helped strengthen the EU's cybersecurity architecture, the landscape has since evolved significantly, with the adoption of **NIS2 and the Cyber Resilience Act**, adding new layers of requirements and responsibilities.

Stakeholder feedback gathered as part of the review points to broad support for **reinforcing and clarifying ENISA's role**, particularly in light of its expanding tasks under newer legislation. Many stakeholders also see the review as an opportunity to improve

coordination between EU and national authorities and to reduce complexity across the cybersecurity framework.

Differences of view remain on some key issues. These include whether cybersecurity certification should remain **voluntary or become mandatory** in certain critical sectors, as well as whether schemes should include non-technical requirements related to sovereignty.

Overall, the EPRS briefing presents the Cybersecurity Act review as an opportunity to **simplify and better align EU cybersecurity rules** and reduce fragmentation, making the framework work more effectively in practice. These objectives closely mirror FERMA's long-standing calls for coherence, proportionality and a risk-based approach across EU digital and cybersecurity legislation.

Next steps

- The Commission's legislative proposal is expected around mid-January.
- Once issued, FERMA will inform members to gather their feedback and decide on potential further advocacy steps.

6) Bruegel: Analysis of EU digital services competitiveness

Following the publication of the Commission's **Digital Omnibus in November 2025**, Bruegel has published an analysis assessing whether the initiative is sufficient to improve the **competitiveness of EU digital services**. Bruegel is a Brussels-based think tank specialised in EU economic policy, with a strong focus on digital regulation, competition, and the functioning of the single market.

The analysis recognises the **Digital Omnibus as a positive step** towards reducing regulatory fragmentation and easing compliance across major digital files, including the AI Act, GDPR, Data Act and related cybersecurity and reporting obligations. Measures such as streamlined reporting requirements and adjusted implementation timelines are seen as helpful in lowering administrative burdens and improving regulatory predictability for companies operating across the EU.

However, Bruegel argues that **simplification alone will not be sufficient** to make EU digital services genuinely competitive. In particular, the article points to unresolved structural issues around **data access and data use**, especially in situations where data is jointly generated by multiple actors. The absence of clear, enforceable rules in these areas continues to create legal uncertainty and limits the development of competitive data-driven services.

EU Affairs Team

The analysis also warns that **regulatory simplification may disproportionately benefit large incumbent firms**. In highly concentrated markets such as cloud computing and digital infrastructure, reducing compliance costs without addressing switching barriers, interoperability, and market access risks reinforcing existing market power rather than supporting new entrants and innovation.