Nemko Digital

The Digital Omnibus:

Simplifying Europe’s Digital Rulebook

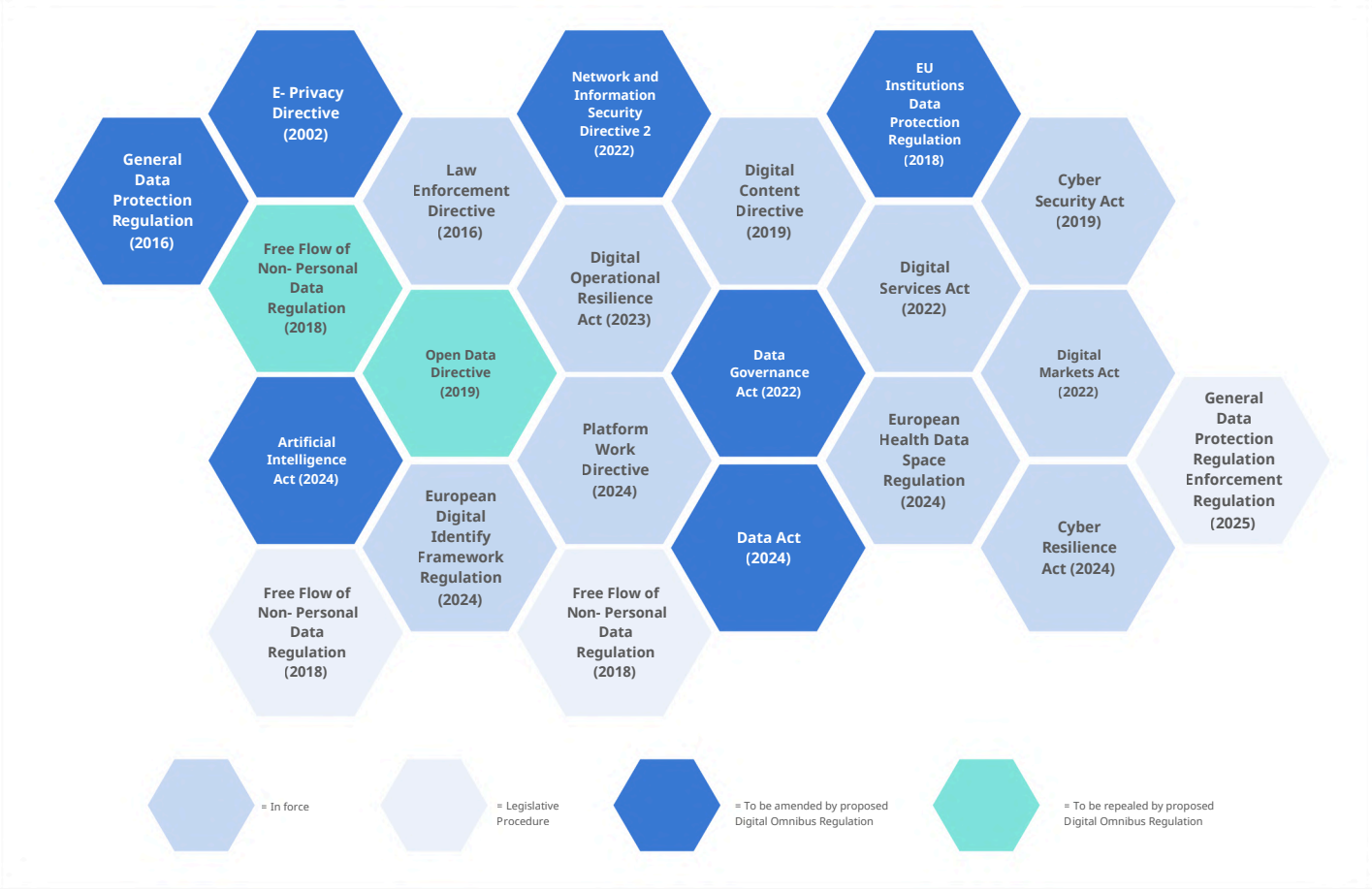
The Digital Omnibus is a legislative proposal by the European Commission aimed at simplifying and streamlining the European Union's increasingly complex digital regulatory framework. Rather than introducing new regulatory regimes, it focuses on improving how existing rules function in practice—reducing administrative burdens, increasing legal clarity, and strengthening Europe's competitiveness.

It represents a notable shift in EU policymaking: from expanding digital regulation to making it work more effectively.

A Shift Toward Simpler, More Coherent Regulation

Over the past decade, the EU has built a dense and ambitious body of digital legislation. This framework has established high standards for privacy, cybersecurity, and fairness in digital markets. However, it has also led to fragmentation, overlapping obligations, and rising compliance costs.

The Digital Omnibus is a response to these challenges. Its purpose is not to weaken the regulatory framework, but to ensure that it is coherent, efficient, and easier to navigate, especially for businesses operating across multiple regulatory domains.



Data Act

At the centre of the reform sits the Data Act, which is repositioned as the primary framework for Europe's data economy.

Over recent years, multiple instruments—such as the Free Flow of Non-Personal Data Regulation, the Open Data Directive, and the Data Governance Act—have developed in parallel. While each addressed specific policy goals, their coexistence has led to fragmentation and duplication.

The Digital Omnibus resolves this by consolidating key elements of these frameworks into the Data Act, effectively turning it into a central hub. This reduces the need for businesses and public authorities to navigate multiple regimes and aligns definitions, processes, and obligations across the data landscape.

The reform does not fundamentally change the substance of the rules. Instead, it transforms them into a single, more navigable system, enabling data sharing, reuse, and innovation with greater legal certainty.

GDPR

The General Data Protection Regulation (GDPR) remains a cornerstone of the EU digital framework. The Digital Omnibus does not reopen its core principles, but introduces targeted adjustments to improve its practical application.

These changes address areas where implementation has proven complex or burdensome. Clarifications around the definition of personal data, the treatment of pseudonymised data, and the conditions for scientific research aim to provide greater legal certainty. At the same time, obligations for low-risk processing are streamlined, allowing organisations to focus resources where risks are highest.

In this sense, the GDPR is not weakened, but recalibrated toward usability, ensuring that its protective goals can be achieved more efficiently in practice.



ePrivacy Directive → GDPR

The longstanding coexistence of the ePrivacy Directive and the GDPR has created one of the most visible frictions in the digital ecosystem—most notably in the form of repetitive and often ineffective cookie consent banners.

The Digital Omnibus addresses this by shifting key rules on access to terminal equipment and consent into the GDPR framework. This move simplifies the legal landscape by replacing a dual regime with a more unified and consistent approach to privacy.

At the same time, the proposal introduces the possibility of machine-readable consent signals, allowing user preferences to be expressed through browser settings or similar tools. This reflects a broader transition from formalistic compliance toward scalable and user-centric mechanisms.

NIS2, DORA, and GDPR incident reporting

Fragmentation within the EU digital framework is not limited to legislation—it also manifests in how obligations are operationalised.

Currently, organisations may be required to report the same cybersecurity incident under multiple frameworks, including NIS2, DORA, and GDPR. The Digital Omnibus introduces a single entry point for incident reporting, enabling entities to fulfil these obligations through one interface.

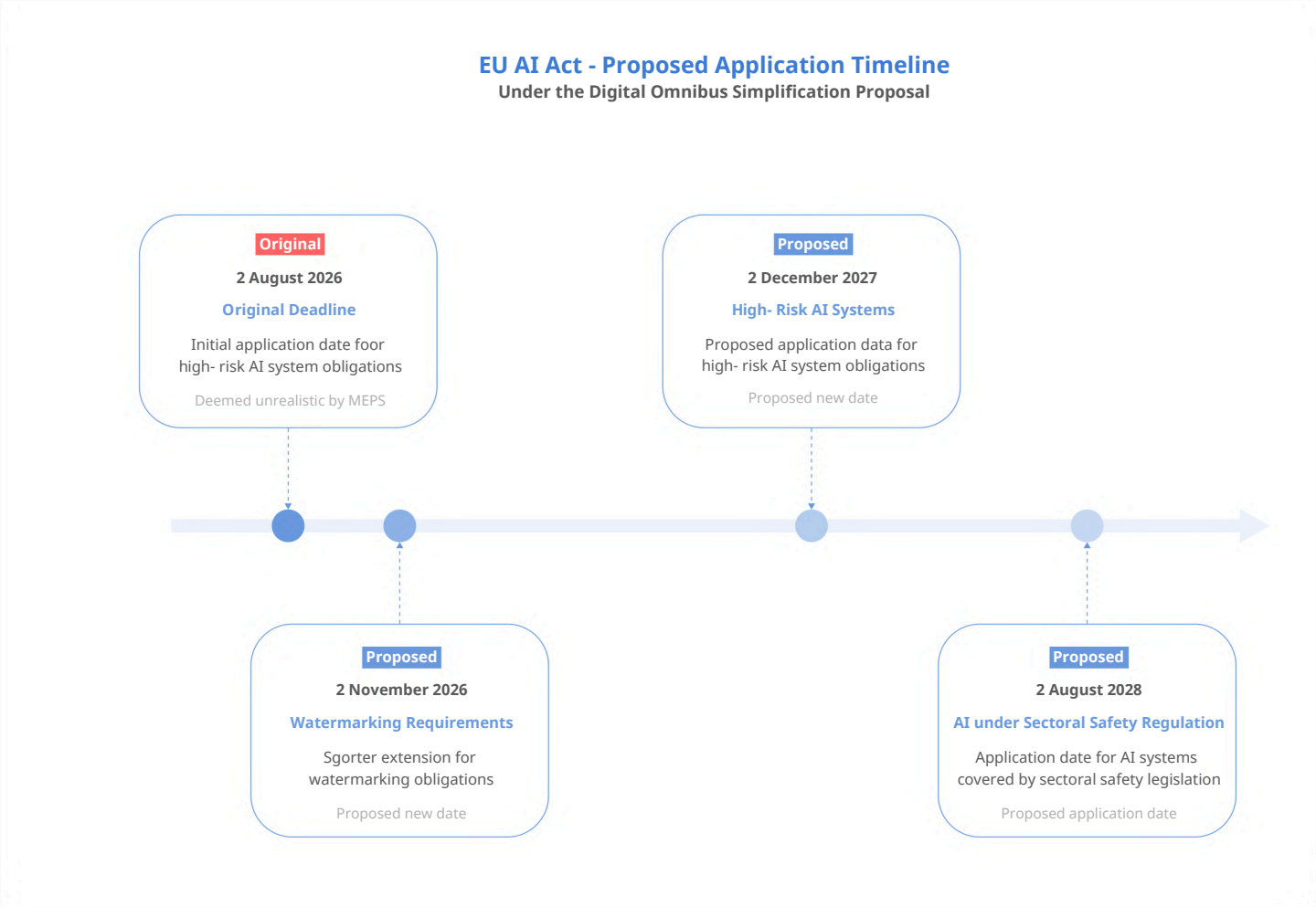
This "report once, share many" principle represents a shift toward integrated compliance infrastructure, reducing administrative burden while preserving the underlying regulatory requirements.



The AI Act

As the EU moves closer to implementing the AI Act, a gap has emerged between regulatory ambition and practical readiness. Key elements—such as harmonised standards, implementing acts, and additional guidance—are still under development, prompting calls to adjust the timeline and enable a more phased rollout.

This shift is already taking shape. Members of the European Parliament have supported postponing certain obligations for high-risk AI systems, recognising that the original 2 August 2026 deadline may not be realistic. Instead, they propose fixed application dates of 2 December 2027 for high-risk systems and 2 August 2028 for systems covered by sectoral safety legislation, alongside a shorter extension for watermarking requirements until 2 November 2026.



Taken together, this reflects a broader shift: the AI Act is not only being implemented, but actively recalibrated to align legal requirements with practical readiness.

However, the debate does not stop at timing. In the context of the Digital Omnibus, some proposals go further, raising questions about the structure of the AI regulatory framework itself.

A Proposal in Motion: Simplification Under Pressure

Although the Digital Omnibus is framed as a technical simplification exercise, it is unfolding in a much more complex political and regulatory context. The Omnibus sits at the intersection of multiple pressures. Policymakers are under increasing urgency to reduce regulatory burdens and support competitiveness, especially as businesses prepare for the implementation of major digital laws. At the same time, they are confronted with the risk that simplification—if taken too far—could undermine the coherence of the very framework it seeks to improve.

This tension becomes especially visible in the debate surrounding the AI Act.

The AI Act: The Horizontal Approach Under Debate

The AI Act was designed as a horizontal regulation, meaning that it applies across sectors with a single, unified set of rules for high-risk AI systems. This approach has been central to its logic: it ensures consistency, avoids duplication, and creates a common baseline for safety, transparency, and accountability.

Yet, proposals linked to the Omnibus suggest moving certain AI applications toward sector-specific regulation, effectively shifting them out of the core horizontal scope.

While this may appear as a form of simplification, it has triggered significant concern among stakeholders. In March 2026, a coalition of organisations warned against such a move, arguing that it risks creating regulatory fragmentation, legal uncertainty, and ultimately higher compliance burdens for companies operating across the single market.

Their concern is rooted in the nature of AI itself. AI systems are increasingly embedded across products and sectors—from medical devices to consumer electronics—yet many existing sectoral frameworks do not adequately address key AI-specific risks such as robustness, data governance, or transparency. A fragmented approach would require these requirements to be rebuilt across multiple regimes, potentially leading to inconsistent standards and timelines.

Moreover, in a global context defined by competition with other AI ecosystems, a unified European framework is seen as essential for enabling scale, reducing friction in cross-border operations, and strengthening Europe's position in global value chains.

A Turning Point for EU Digital Regulation

What emerges from these developments is that the Digital Omnibus is more than a technical adjustment—it is a moment of recalibration for EU digital policy

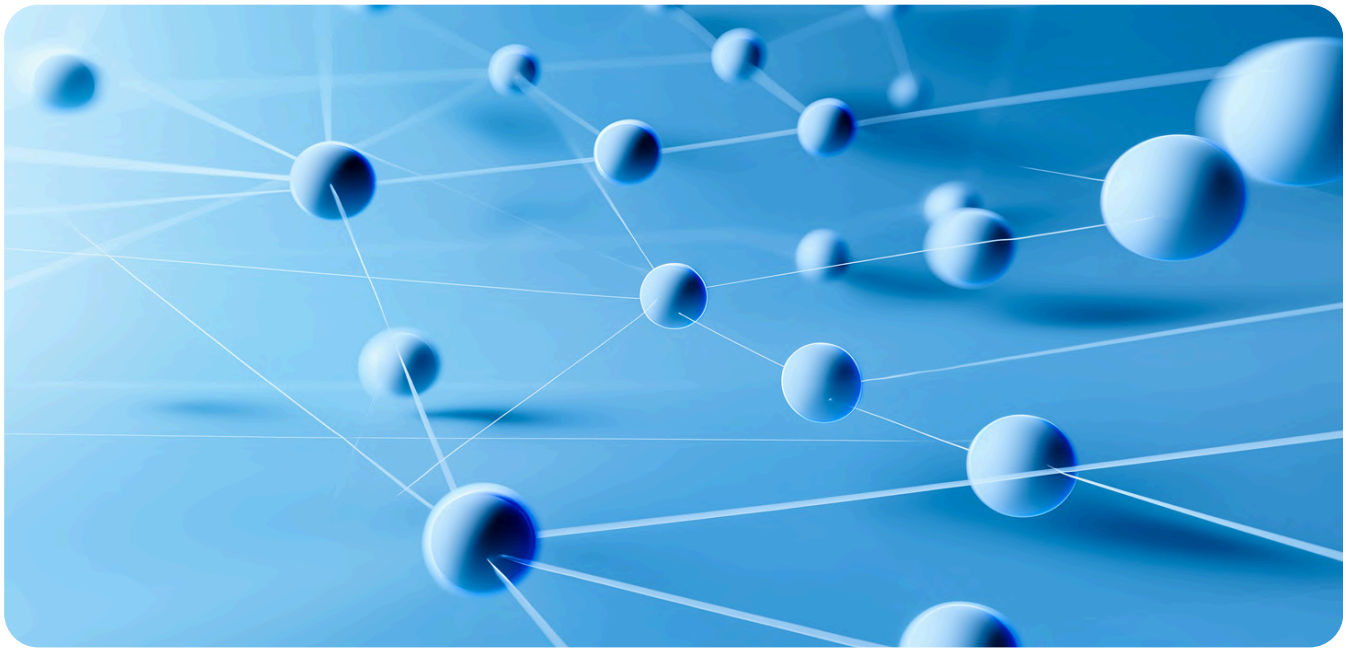
.

On one level, it seeks to streamline rules, reduce administrative burdens, and improve legal clarity. On another, it forces a deeper reflection on how to balance:

1. Simplification with regulatory coherence
2. Flexibility with legal certainty
3. Competitiveness with high standards of protection

For now, the proposal has no direct legal effect, and the original frameworks—GDPR, Data Act, and AI Act—remain the same. However, the direction of travel is clear.

The EU is entering a phase where the challenge is no longer to build regulation, but to make it function as an integrated system.



Looking Ahead

The Digital Omnibus marks a turning point in the evolution of EU digital regulation. It signals a move away from adding new layers of rules and toward refining, aligning, and operationalising the existing framework.

Its success will depend not only on its ability to reduce complexity, but also on how well it preserves the integrity of the system it seeks to improve. For organisations operating in this space, the challenge is no longer simply to comply with individual regulations, but to understand how these frameworks interact as a system—and how that system is evolving over time.

This is where a more integrated approach to compliance, risk, and assurance becomes essential. At Nemko Digital, we see this shift reflected in our work: supporting organisations not only in meeting regulatory requirements, but in navigating the intersections between AI, cybersecurity, data governance, and product compliance in a dynamic environment.

As the Digital Omnibus progresses, those who engage early—by aligning their systems, governance, and technical practices with regulatory developments—will be best positioned to demonstrate trust, resilience, and move faster and more confidently as requirements evolve.

About the author



Mónica Fernández Peñalver

Mónica leads Nemko Digital's work on governance, assurance, and standards implementation. Drawing on expertise in responsible technology, sustainability, and policy, she translates complex frameworks such as ISO 42001 into actionable strategies, enabling organizations to meet ethical, regulatory, and operational requirements.

Nemko Digital