Digital Omnibus and the Revision of the Digital Acquis

Prof. Oreste Pollicino, Pollicino AIdvisory
Dr. Federica Paolucci, Bocconi University

1. The spirit of the proposal

With the proposed Regulation on the simplification of digital legislation, presented by the European Commission on November 19, 2025, the Union intends to profoundly redefine the meaning of its digital sovereignty. Starting with the famous report commissioned from Mario Draghi and circulated last year, the Commission has begun to rewrite its relationship with risk, data, and, ultimately, fundamental rights, relaunching a new approach to competitiveness.

The Digital Omnibus proposal makes this transition clear. As a matter of fact, in the *Explanatory Memorandum* to the proposal, the Commission speaks of simplification *by design* aimed at "optimising the application of the *digital rulebook*." Behind this formula, therefore, there seems to be a different logic from that which inspired the GDPR at the time: not the affirmation of new rights, but the construction of an infrastructure capable of intervening quickly and uniformly, with the aim of making simplification a paradigm of governance.

2. Object of the proposal

Coming to the concrete terms of the proposal, the Explanatory Memorandum specifies that the purpose is to intervene with "immediate simplification measures.
Therefore, the Digital Omnibus proposal has two souls:

Proposal	Objects
Prosal Digital Omnibus, COM(2025) 837	The purpose is to simplify, consolidate and modernise the EU's data, privacy, cybersecurity and platform rules.
Proposal Digital Omnibus on AI, COM(2025) 836	The focus here is exclusively on the practical implementation of the **AI Act (Regulation 2024/1689)**, which has revealed structural challenges even before its core provisions become applicable.

The Commission presents both measures as a single political project, an attempt to shift the digital rulebook from a regime that had become stratified and cumbersome into one that is more coherent, predictable and administratively realistic. This dual structure has a very precise logic. The first proposal – namely, COM(2025) 837 – is the horizontal pillar. It intervenes across the entire "data acquis": the GDPR, the ePrivacy Directive, the Data Governance Act, the Free Flow of Non-Personal Data Regulation, the Open Data Directive, the Data Act, the NIS2 framework, DORA, CER and even the P2B Regulation. Its aim is to reduce fragmentation by consolidating what can be consolidated and clarifying what can be clarified. The second proposal – COM(2025) 836 – is, then, more vertical: it revises the implementation architecture of the AI Act to ensure that its ambitious requirements can be applied proportionately and in a way that matches the pace of standardisation, technological readiness and institutional capacity.

It is only by reading both proposals together that one understands the Commission's intent: the Omnibus is a two-engine reform, where data governance and AI regulation are aimed to be recalibrated simultaneously, allowing the Union to present a more integrated, innovation-compatible model of digital governance.

Dimension	Digital Omnibus (COM(2025) 837)	Digital Omnibus on AI (COM(2025) 836)
Regulatory scope	Data Act, DGA, ODD, FFDR, GDPR, ePrivacy, NIS2, DORA, CER, P2B	AI Act (2024/1689)
Core function	Structural consolidation and simplification	Implementation simplification and timing recalibration
Legislative technique	Repeal, integration, amendment	Targeted amendments only
Systemic effect expected	Single Data Act; modernised GDPR; single reporting channel	Readiness-based timeline; AI Office central oversight
Primary expected beneficiaries	Data holders, SMEs/SMCs, public sector bodies	Providers, deployers, SMEs/SMCs,

Pollicino AIdvisory
Via Visconti di Modrone 8
20122, Milano, Italy
info@pollicinoaidvisory.eu

		conformity assessment bodies

3. Data governance

The most structurally important transformation occurs on the **data governance side**. The proposal takes a disjointed ecosystem of data-related instruments and re-articulates them as a single legal architecture anchored in an expanded **Data Act**. The decision to repeal the **Free Flow of Non-Personal Data Regulation**, the **Data Governance Act**, and the **Open Data Directive**, folding their operative provisions into Regulation (EU) 2023/2854 through a single, enlarged framework, marks a decisive move toward legal consolidation. This shift is not cosmetic. The Commission recognises openly, in the narrative of the Digital Omnibus proposal and in the Staff Working Document, that the simultaneous coexistence of an Open Data Directive (governing general public-sector re-use) and a Data Governance Act Chapter II (governing re-use of restricted data) created both conceptual overlaps and practical confusion, particularly when anonymised data shifted from one regime to the other. The Omnibus responds by integrating the two frameworks into an entirely new Chapter of the Data Act, which now governs the re-use of both open and protected public-sector data through a single set of principles, definitions and procedures. The result is a markedly more linear and intelligible structure.

Instrument before Omnibus	**Fate under COM(2025) 837**	**Inside the New Data Act**
FFDR (Reg. 2018/1807)	Repealed	New Chapter VIIb.
DGA (Reg. 2022/868)	Repealed	New Chapters VIIa-c
Open Data Directive (2019/1024)	Repealed	Merged into Chapter VIIc.
Data Act (2023/2854)	Survives but extensively amended	Amended by Art. 1(1–33, 58)
ePrivacy Directive	Partially absorbed	New Arts. 88a–88b GDPR
NIS2, DORA, CER, eIDAS	Amended for single-entry reporting	New mechanisms via ENISA.

3.1 Main aspects

This consolidation is complemented by a series of targeted but substantive corrections to the B2G (business-to-government) access regime. Whereas the original Data Act allowed public authorities to request private-sector data under a broad condition of "exceptional need", the Omnibus introduces a new Article 15a that narrows this possibility strictly to public emergencies. The Staff Working Document describes the previous formulation as a source of profound legal ambiguity, something that businesses repeatedly warned could undermine trust in the new data-sharing system. By reframing B2G access around public emergencies alone, the Omnibus clarifies both the scope and the constitutional rationale of governmental access to privately held data.

Another element of transformation concerns trade secrets in IoT data sharing. Both the proposal and the Staff Working Document explain that data holders expressed strong fears regarding the mandatory sharing of co-generated data with entities in third-country jurisdictions whose legal frameworks do not ensure equivalent protection. The Omnibus therefore modifies Articles 4 and 5 of the Data Act to allow data holders to refuse disclosure where there is a demonstrable high risk of unlawful acquisition or exposure to such jurisdictions. The addition of this ground does not negate the Data Act's pro-sharing architecture but rebalances it in line with industry concerns and the Charter's protection of intellectual property.

A further simplification is the deletion of Article 36 of the Data Act, which imposed essential requirements for smart contracts used in data-sharing arrangements. Here, the Commission is explicit: "the elimination of Art. 36 would therefore promote the development and market introduction of new business models, foster innovation, and reduce barriers for emerging technologies" (Rec. 16).

A summary of these evolutions:

Area	Pre-Omnibus	Post-Omnibus
B2G access	"Exceptional need" (broad, ambiguous)	Public emergencies only (new Art. 15a)
Trade secrets	Mandatory sharing with confidentiality guarantees	Right to refuse if "high risk of unlawful exposure" to weak third-country regimes

Smart contracts	Art. 36 essential requirements	Article 36 **deleted**
Switching (cloud services)	One-size-fits-all regime	Lighter regime for custom-made, SMEs, SMCs
Data intermediation	Mandatory registration	Voluntary "trust-enhancing" framework

4. The impact on the GDPR

Running parallel to these structural reforms is a delicate but crucial update to the GDPR. The key innovation is the explicit introduction of entity-relative identifiability into Article 4(1). Under the proposed amendment, information is personal data only for entities that have the means "reasonably likely" to identify the individual. This change codifies the Court of Justice's interpretation in C-413/23 and directly addresses decades of debate around pseudonymisation, complementing it with a new mechanism, Article 41a GDPR, that empowers the Commission to adopt implementing acts on when pseudonymised data cease to be personal for certain types of recipients.

The GDPR also receives updates with the aim to simplify access to scientific research, clarifying conditions for automated decision-making, simplifying information duties for low-risk processing, and introducing a new "high-risk only" threshold for data breach notifications. Together, these adjustments do not reopen the GDPR but tune its operation for a more coherent application across Member States, a point repeatedly emphasised by the Commission throughout the Working Document consultation record.

GDPR	Pre Omnibus	Post Omnibus
Art. 4(1) definition	Identifiability includes indirect identification	Becomes entity-relative ("not personal for entities without reasonably likely means")
Art. 9(2)	Strict prohibition except enumerated cases	Adds biometric verification and residual AI processing exception
Art. 13	Information always required	Exemption for low-risk, clear relationship scenarios
New Arts. 88a/b	No GDPR rule	Introduces equipment access + machine-readable signals

Perhaps the most visible change for individuals is the integration of the ePrivacy Directive's terminal equipment rules into the GDPR through the creation of Articles 88a and 88b. The Commission takes aim directly at "consent fatigue", proposing a future ecosystem where standardised, machine-readable preference signals emitted by browsers and operating systems can serve as legally valid consent or refusal, with the additional effect of drastically reducing cookie banners over time. This change, long discussed and previously attempted in the 2017 ePrivacy Regulation proposal, is framed here as an overdue modernisation, aligned with Recital 66 of the 2009 amendment to the ePrivacy Directive.

5. The impact on cybersecurity

Running alongside the data and privacy reforms is a third component: the single entry point for cybersecurity and data breach reporting. The proposal also aims to amend NIS2, DORA, CER, eIDAS and GDPR so that entities fulfil all major incident-reporting obligations through a single interface operated by ENISA. This is not a reduction in substantive obligations but a reconfiguration of how regulated entities interact with authorities, something repeatedly highlighted as a burden by stakeholders in the Commission's consultations. The SWD is clear that this measure alone could generate hundreds of millions of euros in administrative savings while improving data quality, timeliness, and cross-sectoral coordination.

6. The impact on AI Act

If the first proposal reorganises the digital acquis, the second, as mentioned above, ensures that the Union's new flagship instrument, the AI Act, can be realistically applied. The Commission admits that delays in harmonised standards, gaps in technical guidance, and slow designation of national competent authorities risk leaving businesses without the tools needed to comply with the statutory deadlines. To address this, the Omnibus on AI introduces a mechanism that ties the entry into application of high-risk obligations to the availability of standards, Commission guidelines or common specifications. Instead of fixed calendar deadlines, the system becomes *readiness-based*. Still, this system may lack of precise guidelines for companies, and, therefore, fallback longstop dates are much needed to preserve legal certainty.

Equally significant is the extension of SME privileges to small mid-caps, a category newly defined in the AI Act. These companies, which often scale rapidly, faced a regulatory cliff-edge when transitioning out of SME status.

Moreover, the proposal amends Articles 11, 17, 99 and several procedural provisions to ensure proportionate treatment, in line with the findings of the Staff Working Document's SME and SMC consultation panels.

Finally, the Omnibus on AI centralises certain supervisory powers in the AI Office, particularly for AI systems based on general-purpose models or embedded in very large online platforms or search engines. This shift echoes a broader pattern in EU digital regulation: the gradual elevation of enforcement for cross-border and highly technical domains to the Union level. The Commission is careful, however, to preserve the role of national authorities for AI systems embedded in products already regulated by sectoral safety law.

The package also modernises the Act's innovation tools, with the purpose of easing access to national regulatory sandboxes, enabling cross-border real-world testing, and empowering the AI Office to operate an EU-level sandbox from 2028.

Component	Pre Omnibus	Post Omnibus
High-risk obligations	Apply on fixed date (2 Aug 2026/2027)	Apply when Commission confirms availability of standards, common specs, or guidelines; longstop dates still apply
GPAI transparency	Immediately applicable	Transitional alignment period for pre-existing systems
Registration of non-high-risk	Mandatory	Deleted
Sandboxes	National only	EU-level sandbox from 2028
SME regime	SME only	Extended to SMCs

7. Future outlook

What emerges from this dual reform is a coherent narrative: the European Union is not retreating from its role as a global regulatory pioneer, but it is adjusting the machinery beneath its rules to ensure they remain operable, predictable and innovation compatible. While the Omnibus on data rebuilds the foundations of the digital acquis, the other one ensures that the AI Act can sit securely atop that foundation. The two proposals are therefore not just parallel: they are mutually enabling. Only by simplifying the data environment

and making data obligations clearer can the Union sustain the demanding governance model of the AI Act; only by recalibrating the AI Act's implementation architecture can the Union ensure that its data reforms truly support, rather than hinder, the uptake of trustworthy AI across the single market.

Pollicino AIdvisory
Via Visconti di Modrone 8
20122, Milano, Italy
info@pollicinoaidvisory.eu