REGULATORY INSIGHT

The Simplification Paradox: What the Digital Omnibus Actually Asks of Regulated Firms

For most of the last decade, the trajectory of EU digital regulation has run in one direction: more instruments, more obligations, more overlapping authorities. The Digital Omnibus, the package of simplification proposals the European Commission published on 19 November 2025,[1] is the first serious attempt to run the other way. It is being marketed as relief — a reduction in compliance burden, a response to competitiveness concerns crystallised by the Draghi report.

For regulated financial entities, however, "simplification" is a deceptively comfortable word. A package that genuinely streamlines the rulebook still has to be read, mapped, and implemented — and until it is finalised, it creates uncertainty rather than removing it. This article sets out what the Digital Omnibus is, what it changes for firms already managing DORA, NIS2, the GDPR and the AI Act, and why the most disciplined response is, for now, a measured one.

What the Digital Omnibus Is — and Is Not

The package is in fact two proposals. The first, the Digital Omnibus, amends the data and cybersecurity acquis — the GDPR, the ePrivacy Directive, and the Data Act (into which the Data Governance Act, the Free Flow of Non-Personal Data Regulation and the Open Data Directive are being repealed and folded as new chapters), and elements of the EU's cyber laws including NIS2 and DORA. The second, the Digital Omnibus on AI, amends the AI Act.[2] Together they touch nearly every horizontal digital instrument a financial entity is subject to.

Two characterisations matter. First, this is not a rewrite. Most commentators read the package as a selective recalibration — an attempt to address inconsistencies and provisions that have not worked well in practice — rather than a reversal of the EU's regulatory architecture. The risk-based structure of the AI Act and the core principles of the GDPR are not being dismantled. Second, and critically, it is still only a proposal. The package is subject to the ordinary EU legislative process and is expected to be finalised over the course of 2026.[3] Several of its more consequential elements are already contested, and some are unlikely to survive in their original form.

That combination — broad in reach, modest in ambition, and not yet law — defines the planning problem for in-house teams.

The AI Act Delay: Breathing Room, Not a Reprieve

The most immediately significant development came through the AI strand. On 7 May 2026, after negotiations had nearly collapsed at the end of April, EU lawmakers reached political agreement on revisions to the AI Act.[4] The headline effect is a postponement of the high-risk obligations that had been bearing down on a fixed date of 2 August 2026.

The revised approach sets separate, fixed deadlines for the two main high-risk categories, to allow standards and guidance to be finalised first: 2 December 2027 for new or substantially modified high-risk systems listed in Annex III — the category that captures credit scoring and certain insurance use cases — and 2 August 2028 for AI embedded in regulated products listed in Annex I. The Annex I deferral is shorter measured in months of delay (roughly twelve months from the original Annex I baseline), although the resulting deadline still lands later than the Annex III deadline.[5] Transparency obligations for artificially generated content, such as watermarking, were delayed by a shorter period, with compliance expected by 2 December 2026.[6] All of these dates remain subject to formal adoption.

The temptation is to read this as a reprieve. It is not. The obligations are postponed, not cancelled; the agreement remains subject to formal adoption; and the delay is partly conditional on the availability of standards and support tools — meaning the clock effectively restarts rather than stops. Firms that paused their AI Act readiness in May 2026 will find that conformity assessments, technical documentation and governance arrangements take as long to build as they ever did. The sensible reading is that the runway has lengthened, not that the destination has moved.

One Portal, the Same Incidents

For operationally regulated firms, the most structurally interesting proposal is the single entry point for incident reporting. Today, a single serious event can trigger separate notification procedures under the GDPR, NIS2 and DORA — and further regimes including eIDAS and the Critical Entities Resilience Directive — each with its own template, timeline and recipient authority. The Digital Omnibus proposes to consolidate these into one reporting channel operated by ENISA.[7]

This is a real efficiency. But it is worth being precise about what it does and does not change. A single portal rationalises the *delivery* of notifications; it does not rationalise the *substance* behind them. A firm must still classify the event correctly, assess it against each regime's materiality thresholds, meet each regime's deadlines, and stand behind the accuracy of what it submits. The internal machinery — detection, triage, classification, escalation, decision-making under time pressure — remains exactly as demanding. A unified portal that receives a poorly classified report simply distributes that deficiency more efficiently. The proposal reduces friction at the last mile; it does not relieve the firm of the work that precedes it.

Consent and Cookies: A Genuine Operational Change

For firms with consumer-facing digital channels, the proposed changes to the consent and cookie regime are among the more tangible. The package moves the rules on storing and accessing information on users'

devices out of the ePrivacy Directive and into the GDPR through new Articles 88a and 88b, and recalibrates consent mechanics — single-click accept-or-reject choices, recognition of browser-level preference signals, and a six-month moratorium period after a user declines.[8]

For a bank, insurer or payment firm operating apps and websites, this is not a paperwork change. It implies revisiting consent interfaces, analytics configurations and marketing technology stacks. It is also an area where, if adopted, the reduction in fragmented national interpretation would be a genuine and welcome simplification — one of the clearer wins in the package.

The Moving Parts: Why Premature Action Is the Real Risk

The Digital Omnibus also illustrates why simplification packages demand caution. Its most contested element is a proposed refinement of the GDPR's definition of personal data — a contextual approach under which information might not be personal data for an entity that cannot itself identify the individual.[9] Data protection authorities have pushed back hard: the EDPB and EDPS, in Joint Opinion 2/2026 of 11 February 2026, urged co-legislators not to adopt the change, warning that it goes well beyond a technical amendment and would narrow the scope of EU data protection law.[10] Reported Council compromise texts circulated by the Cypriot Presidency in February 2026 suggest the provision may be removed or significantly altered.[11]

The lesson for compliance teams is direct. A proposal is not a safe harbour. A firm that reclassifies datasets, relaxes safeguards, or stands down a compliance workstream on the strength of the Omnibus as drafted is taking a position on legislation that does not yet exist and may not survive. The correct posture is to track the package closely, model its operational impact, and prepare to move quickly once text is settled — while continuing to comply fully with the law as it currently stands.

Practical Priorities for Regulated Firms

- **Treat the AI Act timeline as extended, not cancelled.** Maintain AI system inventories and governance work; the conditional, standards-dependent nature of the new deadlines means readiness still takes the same effort.
- **Map your incident reporting against the proposed single portal.** Identify where consolidation will change workflows — but invest now in the classification and escalation capability that no portal can replace.
- **Scope the consent and cookie changes against your digital estate.** For consumer-facing firms, treat this as a design and technology project, not a policy edit.
- **Do not act on the proposal as if it were law.** In particular, make no changes to data classification or safeguards premised on contested GDPR amendments.
- **Build a tracking and trigger plan.** Assign ownership for monitoring the legislative process, and pre-define the decisions the firm will take once each strand is finalised.

- **Brief the board on uncertainty, not just change.** The governance message is that the framework is in flux and the firm is positioned to respond — not that obligations are easing.

Conclusion

The Digital Omnibus is a genuine attempt to make the EU digital rulebook more coherent, and parts of it — a single reporting portal, a less fragmented consent regime — would be real improvements for regulated firms. But simplification is not the same as relief. A streamlined framework still has to be implemented, and a package this broad will absorb legal and operational attention for the whole of 2026 and beyond. The firms that handle it best will resist both complacency and premature action: they will treat the Omnibus as a transition to be managed, watch the text settle, and keep complying with the rules as they are until the rules as they will be are actually law.

References

1. European Commission, *Digital Omnibus Regulation proposal* (Shaping Europe's digital future), proposals published 19 November 2025.
2. Osborne Clarke, *"Digital Omnibus Package"*, describing the two proposals — the Digital Omnibus (data and cybersecurity acquis) and the Digital Omnibus on AI.
3. Lexology, *"EU Digital Omnibus Package: An Overview"* (5 February 2026).
4. Council of the European Union, press release, *"Artificial intelligence: Council and Parliament agree to simplify and streamline rules"* (7 May 2026); see also Travers Smith, *"EU Agrees to Delay Key AI Act Compliance Deadlines"*.
5. Council of the European Union (n 4); K&L Gates, *"EU and Luxembourg Update on the European Harmonised Rules on Artificial Intelligence — Recent Developments"* (20 January 2026).
6. Council of the European Union (n 4), on the four-month deferral of Article 50(2) transparency obligations to 2 December 2026.
7. European Commission (n 1); Usercentrics, *"What to Know About the EU's Digital Omnibus Package"* (11 February 2026).
8. Reed Smith, *"The EU Commission's Digital Package: Reforming GDPR, e-Privacy, Data Act, AI, and Cybersecurity"*; Osborne Clarke (n 2).
9. Hogan Lovells, *"EU Digital Omnibus — Where Simplification Is Likely and What Businesses Should Plan For"* (9 March 2026).
10. European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 2/2026 on the Digital Omnibus Regulation proposal* (11 February 2026); EDPB-EDPS Joint Opinion 1/2026 on the Digital Omnibus on AI (11 February 2026).
11. IAPP, *"EU Member States' Leaked Digital Omnibus Compromise Proposal Eliminates Revised GDPR Definition of 'Personal Data'"* (23 February 2026).