MACEDO VITORINO

THE EU DIGITAL OMNIBUS

ENSURING REGULATORY COHERENCE IN AI, PLATFORM, AND DATA GOVERNANCE

Cláudia Fernandes Martins

ABSTRACT

The European Commission's "Digital Omnibus" package (COM(2025) 837 final) and the parallel "Digital Omnibus on AI" proposal (COM(2025) 836 final) mark a shift from regulatory expansion towards regulatory consolidation in EU digital governance.

Rather than introducing new substantive duties, the package seeks to reduce duplicative compliance burdens, clarify interfaces between overlapping instruments, and enhance enforcement coherence across the EU's digital rulebook.

This paper analyses the legal technique and policy rationale of the Digital Omnibus and assesses its implications for three intersecting domains: (i) data regulation (Data Act and the broader data acquis), (ii) data protection and privacy (GDPR and ePrivacy), and (iii) governance of AI systems and platforms (AI Act, DSA, and P2B). It argues that the initiative's effectiveness will depend on whether simplification is achieved through genuine alignment of procedures and supervisory coordination, while maintaining the level of protection required by the EU Charter of Fundamental Rights.

Keywords: Digital Omnibus; AI Act; GDPR; Digital Services Act; Data Act; enforcement; Portugal..

INTRODUCTION

THE EU'S "AGILE DIGITAL RULEBOOK" AGENDA

EU digital regulation has evolved rapidly from sector-specific measures to a dense horizontal framework covering data protection, online platforms, digital markets, cybersecurity and artificial intelligence. Core instruments include the GDPR, the DSA, the DMA, the Data Governance Act (DGA), the Data Act, and the AI Act. While each instrument pursues distinct objectives, their cumulative application has produced overlaps in definitions, documentation requirements, incident

reporting and supervisory competences – raising compliance costs and creating legal uncertainty for cross-border operators.

The Digital Omnibus package is framed as a first "targeted" step towards an "agile digital rulebook". The Commission's Explanatory Memorandum emphasises that the amendments are technical in nature, seek to lower compliance costs, and aim to preserve underlying policy objectives and standards of fundamental-rights protection. The package also sits alongside a broader "digital fitness check" intended to map cumulative impacts and identify further alignment opportunities during the legislative mandate.

LEGAL TECHNIQUE, SCOPE, AND STRUCTURE OF THE PACKAGE

Legally, the Digital Omnibus follows a classic omnibus technique: a single proposal amending multiple regulations and directives, combined with targeted repeals of instruments deemed redundant or superseded. COM(2025) 837 final proposes amendments to the GDPR (Regulation (EU) 2016/679), the Data Act (Regulation (EU) 2023/2854), and selected cybersecurity and privacy instruments, and repeals, inter alia, the Free Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807), the P2B Regulation (Regulation (EU) 2019/1150), the DGA (Regulation (EU) 2022/868), and the Open Data Directive (Directive (EU) 2019/1024). In parallel, COM(2025) 836 final proposes amendments to the AI Act (Regulation (EU) 2024/1689) and sectoral legislation (including Regulation (EU) 2018/1139) to facilitate implementation.

The package therefore has a dual character. First, it consolidates and simplifies parts of the data and privacy acquis (including incident reporting). Second, it introduces implementation-focused adjustments for AI governance. For regulated entities, the practical question is whether procedural alignment will enable re-use of compliance artefacts (e.g., risk assessments, reporting templates) and reduce the risk of parallel investigations triggered by the same event or system.

Table 1. Selected Digital Omnibus Measures

Domain	Baseline instruments	Omnibus measure (indicative)	Compliance / enforcement implications

Data acquis	Data Act; DGA; Open Data Directive; Free Flow of Non-Personal Data	"One Data Act" consolidation; targeted exemptions for smaller firms; model clauses	Fewer parallel regimes; standardised contractual tools; reduced switching burdens for smaller actors
Data protection & privacy	GDPR; ePrivacy Directive	Clarifications on (pseudo)anonymisation; streamlined DPIA / breach reporting; cookies policy modernisation	Potential reduction in documentation duplication; material sensitivities re lawful basis and consent design
AI implementation	AI Act; sectoral safety law (e.g., aviation)	Targeted amendments to facilitate staged application; proportionality for SMEs / small mid-caps; governance support	Implementation predictability; adjusted compliance timelines; supervisory capacity-building
Platforms	DSA; P2B Regulation; DMA (adjacent)	Repeal of P2B as redundant within platform rulebook	Potential simplification for platform-to-business transparency, but risk of gaps depending on DSA coverage
Incident reporting	NIS2; CER; GDPR breach notice (adjacent)	Single reporting mechanism for cyber and data incidents	Lower duplicative reporting; requires careful competence allocation and information-sharing rules

DATA REGULATION: TOWARDS "ONE DATA ACT"

A central pillar of the Digital Omnibus is the restructuring of the "data legislative acquis". The Commission identifies legal complexity driven by partially superseded rules and unaligned definitions. COM(2025) 837 final proposes repeal of Regulation (EU) 2018/1807 (Free Flow of Non-Personal Data) on the basis that switching obligations are now addressed in the Data Act. It also proposes repealing the DGA and the Open Data Directive, while integrating their functional content into a restructured Data Act framework. This consolidation has potential benefits: a single normative anchor

for data access, sharing and intermediation; reduced interpretive friction across instruments; and simplified compliance mapping for industry.

The Commission's Staff Working Document anticipates simplification through, inter alia, narrowing scope in specific areas (such as business-to-government access in emergencies), removing or adjusting requirements considered administratively burdensome, and extending proportionality measures beyond SMEs to "small mid-cap enterprises". The inclusion of model contractual terms and standard clauses seeks to operationalise the framework by providing templates that can be adopted at scale, potentially reducing negotiation and compliance costs in cloud and data-sharing arrangements.

DATA PROTECTION AND PRIVACY: CLARIFICATIONS WITH HIGH CONSTITUTIONAL STAKES

The Digital Omnibus is unusual in that it does not only streamline procedures but also proposes targeted adjustments to the GDPR and the privacy rulebook. The Staff Working Document explicitly identifies the definition of personal data and the treatment of anonymisation and pseudonymisation techniques as areas where greater clarity is sought. In addition, it addresses the processing of personal data for the development and operation of AI systems and models, and it proposes streamlining data breach notification and the "notion of high risk" for the purposes of data protection impact assessments.

From a doctrinal perspective, any recalibration of GDPR concepts requires careful assessment against the EU Charter of Fundamental Rights, in particular Articles 7 and 8, and the proportionality principle. Simplification that reduces uncertainty is desirable; however, simplification that materially lowers substantive safeguards may intensify constitutional litigation risk and create divergent enforcement approaches pending Court of Justice clarification. The proposal also addresses "consent fatigue" by modernising cookie consent mechanics and aligning elements of the ePrivacy regime with the GDPR. While improved user experience and reduced banner fatigue are plausible benefits, the compliance impact will hinge on how exemptions are defined and how preference signals are standardised and evidenced.

PLATFORM GOVERNANCE: REPEAL OF P2B AND THE CONTINUING DSA–DMA DUALITY

For platform operators and business users, the proposed repeal of Regulation (EU) 2019/1150 (P2B) reflects a policy judgment that parts of the platform-to-business transparency regime have been

superseded by the DSA's horizontal framework. Yet the legal and practical consequences of repeal depend on whether DSA coverage fully substitutes for the removed obligations, particularly for smaller platforms not designated as VLOPs or VLOSEs.

More broadly, the Omnibus does not eliminate the structural duality between the DSA (systemic risk and content governance) and the DMA (market power and contestability). Enforcement remains multi-level: the Commission holds exclusive competence over certain VLOP/VLOSE due diligence obligations, while national Digital Services Coordinators supervise other DSA obligations and ensure national coordination. This architecture may generate procedural duplication when platform conduct simultaneously implicates consumer protection, data protection, and competition rules. A key question for the Omnibus agenda is therefore not only alignment of reporting templates, but also alignment of supervisory cooperation and information-sharing rules across authorities.

THE "DIGITAL OMNIBUS ON AI": IMPLEMENTATION, PROPORTIONALITY, AND INSTITUTIONAL CAPACITY

COM(2025) 836 final proposes targeted amendments to Regulation (EU) 2024/1689 (AI Act) to address implementation challenges identified during early application phases, including delays in standards and the establishment of national governance and conformity assessment frameworks. The proposal maintains the AI Act's risk-based logic but seeks to facilitate smooth and predictable application, including by extending certain support and proportionality measures to "small mid-cap enterprises". It also amends Regulation (EU) 2018/1139 to integrate high-risk AI requirements into the aviation safety framework, illustrating the broader challenge of embedding AI governance into sectoral safety regimes.

For businesses, the most salient dimension is legal certainty: implementation-focused simplification can reduce the transaction costs of compliance planning, particularly where application dates are linked to the availability of harmonised standards, guidance, and supervisory tools. For authorities, the Omnibus underscores capacity constraints: AI governance is highly technical, and enforcement effectiveness will depend on coordinated guidance and consistent interpretation across Member States.

MACE DO VITO RINO

ENFORCEMENT COHERENCE AND PORTUGAL: COORDINATION RISKS IN A MULTI-AUTHORITY ENVIRONMENT

The Digital Omnibus explicitly seeks to reduce fragmentation not only in EU rulemaking, but also in how EU digital law is administered and enforced.

Portugal provides a clear illustration of the coordination challenge because several supervisory "nodes" intersect. GDPR supervision is carried out by the Comissão Nacional de Proteção de Dados (CNPD), an independent administrative authority with powers of authority that operates alongside the Assembleia da República. Platform supervision under the DSA, in turn, requires a designated Digital Services Coordinator; in Portugal, ANACOM, the National Communications Authority, has been appointed as the competent authority and Digital Services Coordinator. ANACOM's remit has recently expanded further. In 2025, Decree-Law No. 125/2025 designated ANACOM as the National Sectoral Cybersecurity Authority for electronic communications and postal services. Decree-Law No. 2/2025 also designated ANACOM as Portugal's competent authority for data intermediation services under the Data Governance Act and as Portugal's representative on the European Data Innovation Board.

These competences will often converge in practice. Depending on the service model and its legal qualification, a single AI-enabled product feature (for example, automated content ranking, biometric onboarding, or targeted advertising optimisation) may engage: (i) GDPR requirements (lawfulness, transparency and DPIAs), (ii) AI Act requirements (risk management, documentation and governance controls), and – where the service falls within the DSA's scope – (iii) DSA duties (transparency, systemic-risk assessment and mitigation). Absent strong coordination mechanisms, a single incident – such as an algorithmic failure, unlawful biometric processing, or a data breach – can generate multiple notification channels and parallel proceedings across authorities, each operating under different procedural frameworks and timelines.

Recent CNPD intervention regarding biometric data collection underscores the practical importance of rapid supervisory action in Portugal. in March 2024, the CNPD adopted an urgent provisional measure restricting the collection of biometric data (iris/face) associated with Worldcoin's enrolment activities in Portugal. Importantly, the factual trigger was not "platform content moderation" as such, but the rapid scaling of a high-risk biometric processing operation linked to a digital service ecosystem. The episode shows how interim supervisory action can materially limit exposure while a full assessment proceeds – and why coordination becomes critical when the same underlying product stack can simultaneously engage data protection enforcement, cyber incident response expectations, and (where applicable) digital-service governance obligations.

For regulated entities, the enforcement exposure is therefore not limited to the substantive standards under each instrument. It also includes the procedural burden of concurrent investigations, potentially inconsistent remedial measures, duplicative information requests, and conflicting timelines. Any Omnibus-driven "single reporting point" for incidents will therefore require robust rules on allocation of competence, confidentiality, and onward transmission of information, to avoid both under-enforcement and needless duplication.

CONCLUSION

The Digital Omnibus signals a mature phase in EU digital regulation: a recognition that an ambitious digital rulebook requires coherent interfaces, proportionate procedures, and enforceable governance structures.

The package's consolidation of the data acquis into a more unified Data Act framework, its procedural streamlining of privacy compliance, and its implementation-focused adjustments to the AI Act offer plausible pathways to reduce duplicative burdens. Yet the initiative also carries legal risks. Where simplification affects core GDPR concepts or consent structures, constitutional scrutiny and litigation risk may increase.

The success of the Omnibus will therefore depend on precision in drafting and on the quality of supervisory coordination – both at EU level and within Member States such as Portugal.

REFERENCES

- European Commission, Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 19 November 2025.
- European Commission, Proposal for a Regulation amending Regulations (EU) 2024/1689 and (EU) 2018/1139 (Digital Omnibus on AI), COM(2025) 836 final, 19 November 2025.
- European Commission, Commission Staff Working Document accompanying the Digital Omnibus proposals, SWD(2025) 836 final, 19 November 2025.
- European Commission, A simpler and faster Europe: Communication on implementation and simplification, COM(2025) 47 final, 11 February 2025.

- Regulation (EU) 2016/679 (General Data Protection Regulation).
- Regulation (EU) 2022/2065 (Digital Services Act).
- Regulation (EU) 2022/1925 (Digital Markets Act).
- Regulation (EU) 2024/1689 (Artificial Intelligence Act).
- Regulation (EU) 2023/2854 (Data Act).
- Regulation (EU) 2019/1150 (Platform-to-Business Regulation).
- Regulation (EU) 2022/868 (Data Governance Act).
- Decree-Law No. 20-B/2024 of 16 February (Portugal) – designation of the competent authorities and the Digital Services Coordinator (DSA).
- Decree-Law No. 2/2025 of 23 January (Portugal) – implementation of Regulation (EU) 2022/868 and designation of ANACOM as the competent authority for data intermediation services.
- Decree-Law No. 125/2025 of 4 December (Portugal) – legal framework for cybersecurity and designation of ANACOM as the National Sectoral Cybersecurity Authority for electronic.
- Comissão Nacional de Proteção de Dados (CNPD), official website and public information portal.
- ANACOM, "Digital services" (DSA) – designation as Digital Services Coordinator in Portugal.
- European Commission, "Digital Services Coordinators" (DSA cooperation framework) – policy page.

MACEDO VITORINO

ABOUT MACEDO VITORINO

MACEDO VITORINO is a leading Portuguese law firm. We advise domestic and foreign clients in a wide range of business sectors, including banking, distribution, industry and projects. We are known for our professional and client-oriented approach to complex and difficult matters.

Since the incorporation of the firm in 1996, we have been involved in several high-profile transactions in all of the firm's fields of practice, including banking and finance, capital markets, corporate and M&A, energy, real estate, project finance, complex disputes and restructurings.

ABOUT THE AUTHOR

Cláudia Fernandes Martins is a Partner at MACEDO VITORINO and Head of the Compliance Group, a position she has held since 2019. She leads the MVCOMPLIANCE project and advises national and international companies on the design, implementation and monitoring of compliance programmes, with a particular focus on regulatory compliance, data protection and privacy (including GDPR), corporate integrity and risk management, as well as related matters of competition and European Union law, consumer law and information technologies.

IMPORTANT NOTICE

The opinions expressed in this article are of general nature and should not be considered as professional advice. Should you need legal advice on these matters you should contact a lawyer. If you are a client of MACEDO VITORINO, you may contact us by email addressed to mv@macedovitorino.com.