SQUIRE PATTON BOGGS

EU Digital Omnibus: A Corrective and Pragmatic Initiative

EU – December 2025

The European (EU) Commission's November 19, 2025, Digital Omnibus Package, which was launched after a September call for evidence, is framed to simplify, streamline and align existing digital rules and regulations rather than create a new layer. It focuses on data, privacy and artificial intelligence (AI), with a parallel track of targeted AI Act amendments and cybersecurity simplification. A central aim is greater harmonisation, including a single entry point for breach and incident reporting across several frameworks to avoid duplicate reporting and harmonization procedures he Omnibus aims for legal clarity, cost reduction, and a more coherent legislative framework and the question is whether this will sharpen Europe's regulatory regime and support the development and use of digital and AI services in the EU. The following summarises the main regimes and proposed adjustments.

AI Act and AI Rules

In force since August 2024, the EU Regulation 2024/1689(the AI Act) combines bans, strict obligations for high-risk systems and transparency duties for others, including general-purpose and systemic-risk models. It sits alongside the General Data Protection Regulation (EU) 2016/679, (GDPR), the Cyber Resilience Act (EU) 2024/2847 (CRA), the Digital Services Act (EU) 2022/2065 (DSA) and sectoral rules, creating an overlap and administrative burden, particularly for fast-moving AI development teams. Stakeholders point to duplicative assessments and divergent national enforcement.

The Digital Omnibus proposes targeted amendments. AI literacy obligations shift from providers and deployers to the EU Commission and member states, who are now responsible for encouraging sector-appropriate training and support, rather than imposing a uniform mandate, though deployers of high-risk systems must still ensure trained oversight. A narrow exemption removes EU database registration for certain Annex III systems used only internally. Proportionality measures extend reliefs for small- and medium-sized enterprises (SMEs) and small mid-caps.

The application of high-risk requirements may be delayed for systems already on the market, up to 16 months for Annex III and 24 months for Annex I, reflecting delays in guidance and standards. Synthetic-content labelling is phased in until February 2027. Guidance rather than an implementing act will support post-market monitoring.

Enforcement for sensitive AI systems would be centralised in an enhanced EU AI Office, responsible for coordinating obligations for systems built on the same general-purpose model and for carrying out pre-market conformity assessments for such systems. These changes aim to improve consistency without weakening safety or fundamental-rights objectives, though some fear an overly permissive shift. The EU Omnibus Package also introduces a narrow exemption for residual special-category data in AI development and operation when protective measures are applied.

Data Act and Data Sharing

The EU Data Act (EU) 2023/2854 sits alongside the Open Data Directive (EU) 2019/1024, the Data Governance Act (DGA) (EU) 2022/868 and sectoral reuse rules. Together they aim to unlock value by granting user access to data generated by connected products, setting fairness requirements for certain business-to-business (B2B) contracts, defining public-sector access in exceptional cases and imposing switching and interoperability duties to reduce cloud lock-in. The cumulative result is highly complex, with overlapping transparency duties, trade-secret concerns and inconsistent reuse thresholds, as well as cloud-switching rules that interact unpredictably with cybersecurity and confidentiality requirements.

The Digital Omnibus adds structural refinements. It consolidates elements of the Open Data Directive and DGA with parts of the Data Act to create a more coherent system for public-sector access and reuse. Cloud-switching rules are recalibrated through narrow exemptions for customisable cloud services, as well as for SMEs and small mid-caps, supported by model clauses published in November 2025. Data-transfer safeguards are clarified: data holders may refuse mandatory Internet of Things (IoT) data sharing where there is a substantial risk of unlawful disclosure to third countries.

The regime for data intermediation services becomes voluntary, and the requirement to offer them through a separate legal entity is removed. These adjustments aim to reduce friction and create clearer conditions for portability and reuse, although many original ambiguities remain and new questions are likely.

GDPR and Data Protection

The GDPR remains the EU's core privacy framework, supported by national laws, European Data Protection Board (EDPB) guidance and case law. While globally influential, applying it alongside other digital legislation is difficult. The Digital Omnibus seeks more pragmatic interpretation and harmonisation, though some proposals were dropped after criticism.

A significant change is a more subjective and restrictive definition of personal data, reflecting Case C-413/23 P (in its judgment, the Court of Justice of the EU clarified that the obligation to inform about data transfers must be assessed from the controller's perspective at the time of data collection. While pseudonymised data does not automatically remain personal data for every recipient, this cannot circumvent the original transparency obligation towards the data subjects), focusing on whether a specific controller can reasonably re-identify an individual. This could expand opportunities for compatible reuse and move some pseudonymous data outside the GDPR's scope. Several AI-related exceptions are introduced under the legitimate-interest basis for development and operations, subject to safeguards, though applying legitimate interest consistently in operations may be difficult. Sensitive data in AI datasets may be retained when removal would be a disproportionate effort.

The package also tackles consent fatigue by replacing ePrivacy rules with the GDPR for natural persons using terminal equipment. Automated browser or operating system (OS) preference signals would normally need to be honoured, reducing banners, while news and media organisations retain an exemption for advertising-supported models.

A single EU breach-reporting portal run by EU Agency for Cybersecurity (ENISA) would streamline notifications under GDPR, Network and Information Security Directive (EU) 2022/2555 (NIS2), Digital Operational Resilience Act (EU) 2022/2554 (DORA) and related regimes, raising the threshold to high-risk breaches and extending the deadline to 96 hours. Clarifications confirm that automated decisions can be necessary for contractual performance, even if manual alternatives exist. Controllers may refuse access requests when used for purposes unrelated to data protection, though the burden of proof remains on the controller. A narrow Article 13 exemption removes the need for a privacy notice when the relationship is clear, risk is low and individuals can reasonably be assumed to know the information; transparency remains mandatory for recipients, transfers, automated decision-making or high-risk processing. DPIA requirements would be harmonised through EU-wide lists and an EDPB template.

These measures promise clearer interpretation and reduced duplication but raise concerns about a narrowed personal-data definition, AI-related exceptions, and possible weakening of protections.

NIS2, CRA and Cyber Rules

NIS2 expanded EU cybersecurity duties across essential and important entities, while the CRA imposed horizontal lifecycle-security requirements for digital products linked to CE marking. Incidents frequently trigger several regimes at once, with varying thresholds, authorities and national practices, resulting in duplication and confusion.

The Digital Omnibus supports consolidation by establishing a single incident-reporting entry point, developed and supervised by ENISA, covering severe incidents under the NIS2, the CRA, the GDPR and DORA, as well as available voluntarily for others. It builds on experience from the CRA platform. The package also signals guidance on interactions between the AI Act and cyber rules and considers adjustments to sandboxes and real-world testing to avoid parallel regimes. A unified alert system could significantly reduce burden, though its effectiveness will depend on ENISA's capacity and the security of the centralised portal.

Can the Corrective Approach Work?

The Digital Omnibus proposes targeted amendments to the EU's digital legal framework, like a streamlined business-to-government data access regime, amending the definition of personal data, updating breach notification procedures, and integrating cookie rules into the GDPR and the introduction of a single-entry point for incident and breach notifications.

The proposed amendments will likely be subject to changes during the legislative proceedings in the EU Council and the EU Parliament.

This is important because businesses generally favour clear and stable rules: privacy and security build trust, coherent AI and data rules reduce uncertainty and predictable frameworks to enable scaling. The EU's ambition to create a trustworthy, rights-respecting digital order enjoys broad support,

The Digital Omnibus can succeed if it removes real overlaps, aligns reporting and terminology and introduces narrow adjustments suited to the AI era, while maintaining strong rights protections. The Digital Omnibus is the servicing mission that may finally bring the digital rulebook into focus.

How We Can Assist

The proposed reforms would materially reshape how AI and data can be used and how disclosures must be designed. Going forward, companies may need to prepare a review of their processes and programmes update internal governance and prepare for a more prescriptive digital rule.

Our team can support by:

- Assessing impacts on existing product ranges, including mapping
- Preparing new documentation, compliance manuals, websites, periodic disclosures and assessing compliance
- Supporting engagement with EU institutions during the legislative process as the proposal evolves

Our team of lawyers and advisors is ready to assist with any questions and to support firms as they prepare for the future regime. Please do not hesitate to get in touch.

Contacts

Andreas Fillmann
Partner, Frankfurt
T +49 69 1739 2423
E andreas.fillmann@squirepb.com

Annette Demmel
Partner, Berlin
T +49 30 72616 8108
E annette.demmel@squirepb.com