Raúl Rubio

Proposal for a “Digital Omnibus” Regulation for the simplification of the EU digital acquis

I. Executive summary

In fulfilment of one of the key commitments of the new European Commission government team following the 2024 European elections, and after months of anticipation in specialist circles, on 19 November 2025, the European Commission presented a proposal for a “Digital Omnibus” Regulation that consolidates and simplifies the EU’s digital acquis in three main areas: data (consolidation in the Data Act and reduction of burdens for SMEs and SMCs), cybersecurity (single point of incident reporting) and artificial intelligence (clarifications under the GDPR for the development of AI). The proposal aims to reduce administrative costs by at least €1 billion per year and increase legal certainty without lowering standards of protection.

The proposal integrates and repeals multiple instruments to create a consolidated data framework around the Data Act, implements a "single-entry point" for incident reporting managed by ENISA, and amends the GDPR and the ePrivacy Directive to clarify key concepts such as personal data, thus facilitating the development of AI and simplifying cookie banners through automated, machine-readable signals.

The Commission estimates savings of at least €1 billion per year from the moment of the Regulation’s entry into force, with an additional €1 billion in one-off costs, totalling at least €5 billion over three years until 2029, arising from reduced administrative burdens, reduced regulatory duplication and lower compliance costs.

These rules will have a very broad cross-cutting impact, mainly affecting data operators, cloud providers, digital platforms, entities subject to NIS2/DORA/CER, public administrations, AI and digital media developers, but also any entity that processes personal data (due to the amendments to the GDPR) and organisations that develop or use AI systems, given the cross-cutting nature of these regulations. The burden reduction applies in particular to SMEs as well as to small mid-caps (SMCs).

SMCs are defined in accordance with Article 2 of the Annex to Commission Recommendation (EU) 2025/1099. This business category is distinct from and superior to traditional SMEs (micro, small and medium-sized enterprises as defined in Recommendation 2003/361/EC), and represents enterprises at an intermediate stage of growth between SMEs and large companies.

II. Analysis by rule: most significant changes

2.1. Data Act (EU Regulation 2023/2854) - Consolidated instrument

The Data Act has become the consolidated instrument of the European data framework, integrating the Free Flow of Non-Personal Data Regulation (2018/1807), the Data Governance Act (2022/868) and the Open Data Directive (2019/1024), which have been repealed.

Key changes:

- **Trade secrets:** The safeguarding of trade secrets has been strengthened, allowing access to data to be refused if there is a high risk of its unlawful acquisition, use or disclosure to entities in third countries, or entities established in the Union under direct or indirect control of such entities, which are subject to jurisdictions with weaker or non-equivalent protection to that provided by Union law.
- **B2G (Business-to-Government) applications:** Chapter V is limited exclusively to “public emergencies”, thus eliminating the broader concept of an “exceptional need”. Clear rules of necessity, proportionality and compensation have been established, thus allowing micro and small enterprises to claim compensation even in response to public emergencies.
- **Switching cloud:** A more light-touch regime has been established for bespoke services and for suppliers that are SMEs or SMCs in contracts entered into before 12 September 2025, while maintaining the gradual withdrawal of switching and egress fees. Proportional penalties for early termination are allowed to be included in fixed-term contracts.

- **Smart contracts:** Article 36 on essential requirements for smart contracts that execute data-sharing agreements has been completely removed, thereby avoiding the burdens and legal uncertainty that discouraged innovative business models.
- **Data intermediation and altruism:** The regime has been made completely voluntary, including EU labelling/registration and drastically simplified obligations. Mandatory legal separation has been replaced by functional separation with additional safeguards. Transparency and reporting obligations for data altruism organisations have been removed.
- **Free circulation:** The prohibition against non-personal data localisation requirements has been inserted directly into the Data Act as a new Chapter VIIb, thus maintaining the obligation to notify the Commission but eliminating the single national information point.
- **Re-use of public data:** The rules of the Open Data Directive and the Data Governance Act have been merged into a single chapter (VIIc), which contains principles of non-discrimination, non-exclusivity and harmonised payment rules. Higher special conditions and charges have been established for "very large enterprises" and gatekeepers appointed under the Digital Markets Act, based on objective criteria such as economic power and data acquisition capacity.

2.2. GDPR (EU Regulation 2016/679) - Targeted amendments

The GDPR has received targeted amendments to clarify key concepts and reduce administrative burdens on low-risk processing.

Key changes:

- **Definition of personal data:** It has been clarified that information is not personal with respect to a particular entity if the entity has no means that it is reasonably likely to use to identify the natural person to whom the information relates. It has been specified that information does not become personal with respect to that entity simply because a potential subsequent recipient has a reasonably likely means of identifying the natural person.
- **Special categories (Article 9):** Two new exemptions have been introduced: (i) the processing of biometric data necessary to confirm the identity of a data subject (verification) where the biometric data or the means necessary for verification are under the sole control of the data subject, and (ii) the residual processing of special categories in the context of the development and operation of AI systems, subject to appropriate technical and organisational measures to prevent the collection of such categories and, where identified, to delete them or, where deletion would require a disproportionate effort, to protect them effectively from use in the generation of results or disclosure to third parties.
- **Information to the data subject (Article 13):** The exemption is allowed where the personal data has been collected in the context of a clear and limited relationship between data subjects and the controller engaged in a non-data-intensive activity, and there are reasonable grounds to assume that the data subject already possesses the information, except in cases of high risk, transfers to third countries or automated decisions. An exemption has also been added for scientific research where the provision of information is impossible or involves a disproportionate effort.
- **Automated decisions (Article 22):** It has been clarified that decisions based solely on automated processing are permitted when specific conditions are met. To assess whether a decision is "necessary" for the conclusion or performance of a contract, it is not required that the decision can only be made by automated means. The fact that the decision could also be made by a person does not prevent the data controller from making the decision by exclusively automated processing.
- **Notification of breaches:** The threshold has also been raised to "high risk" for notifying the supervisory authority, thereby aligning with the threshold for communication to data subjects; the deadline has been extended to 96 hours, and a common template prepared by the EDPB and the mandatory use of the single-entry point once it is operational have been established.
- **Impact assessments (DPIA):** Single harmonised lists have been introduced at EU level to replace existing national lists, and specify which processing operations do or do not require an assessment. Furthermore, a common template and common methodology prepared by the EDPB and adopted by the Commission through implementing acts have also been introduced.
- **AI and legal basis:** It is established that the processing of personal data necessary for the development and operation of AI systems may pursue legitimate interests under Article 6(1)(f) of the GDPR, with appropriate safeguards such as data minimisation, enhanced transparency and the unconditional right of objection of the data subjects.

2.3. ePrivacy Directive (2002/58/EC) - Alignment and cookies

Article 4 of the ePrivacy Directive has been repealed, and terminal processing is aligned with the GDPR.

Key changes:

- **New Articles 88a-88b of the GDPR:** Article 88a provides that storage or access to personal data on terminal equipment is only allowed with the consent of the data subject, and provides a closed list of exempted purposes (transmission of communications, provision of requested services, aggregated audience information for own use, and maintenance of security). Article 88b introduces automated and machine-readable signals that will allow data subjects to consent/refuse and exercise the right to object automatically. Data controllers must respect these signals once harmonised standards are available. A specific exception has been established for audiovisual media service providers.
- **Adjustment to Article 5(3) of the ePrivacy Directive:** An exception has been added to Article 5(3) of the ePrivacy Directive, which states that it shall not apply where the subscriber or user is a natural person and the information stored or accessed constitutes or leads to the processing of personal data, thus avoiding regulatory duplication with the new GDPR regime.

2.4. Single-Entry Point (SEP) for reporting incidents

A single incident reporting point managed by ENISA has been established.

Key changes:

- **Development and operation:** ENISA will develop and maintain a single point for reporting incidents under multiple Union legislative acts, with technical, operational and organisational specifications to ensure interoperability, compatibility with European Business Wallets, and the ability for entities to retrieve previously submitted information.
- **GDPR Integration:** The GDPR channels notifications of breaches via the SEP.
- **Other frameworks:** It will also be mandated for eIDAS, DORA and CER, with the possibility of incorporating other sectoral reporting obligations through amendments to delegated and implementing acts.
- **Implementation period:** Mandatory use of the SEP within 18 months of the entry into force, with a possible extension to 24 months if the Commission determines that adequate functioning, reliability, integrity and confidentiality have not been ensured.

2.5. P2B Regulation (EU 2019/1150) - Repeal

The P2B Regulation has been repealed due to its overlap with the DSA/DMA. Certain provisions (definitions in Article 2, restrictions and derogations in Article 4, the internal complaint handling system in Article 11, and the application of Article 15) will be maintained until 31 December 2032 to avoid legal uncertainty in acts containing cross-references.

III. Timeline for implementation

The Regulation shall enter into force three days after its publication in the Official Journal; the application shall take place on the following day, with exceptions.

Key dates:

Provision	Application deadline
General entry into force	Three days after its publication
Single-Entry Point	18 months from the entry into force (extendable to 24 months if the Commission's assessment is negative because adequate functioning, reliability, integrity and confidentiality cannot be ensured)
Switching cloud–contracts prior to 12/09/2025	Application of specific regimes for bespoke services and SME/SMC providers
P2B References	To be maintained until 31/12/2032
Respecting automated signals	24 months after the entry into force (for data controllers); 48 months for web browser providers

IV. Sectors affected

The proposed Digital Omnibus Regulation has a cross-cutting scope that affects practically all economic sectors, with a particular impact on the most digitally intensive sectors:

Sectors with a direct and significant impact:

- **Technological and digital:** Cloud providers, digital platforms, data intermediation services, AI developers, cybersecurity companies and trusted service providers.
- **Financial services:** Entities subject to DORA for ICT incident reporting, payment processors and digital financial services.
- **Telecommunications:** Operators of electronic communications networks and services under NIS2, and providers of digital identity services.
- **Energy and critical infrastructure:** Essential and important entities under NIS2 and CER, especially in the energy, transport and water sectors.
- **Media and communication:** Audiovisual media service providers (except for automated signals), digital publishers and content platforms.
- **Public administration:** Public sector bodies for the re-use of data, authorities responsible for registration and supervision.

Sectors with cross-cutting impact:

- **Health:** Processing of health data under the amended GDPR, medical AI systems, and the exchange of health data.
- **Education and research:** Research institutions for open data and data altruism, universities as public bodies.
- **Automotive Industry:** Connected device manufacturers, digital mobility services, and connected vehicle data.
- **Retail and e-commerce:** Trading platforms, personal data processing, intermediation services.
- **Industrial and manufacturing:** Industry 4.0, industrial IoT, data exchange in supply chains.

All sectors are affected by the amendments to the GDPR regarding the processing of personal data, especially those that develop or use artificial intelligence systems. The facilities for SMEs are also extended to small mid-caps (SMCs) in the data framework.

V. Strategic considerations and impact analysis

5.1. Overview of the proposed changes

The proposed Digital Omnibus Regulation represents a paradigm shift in the European regulatory approach from incremental regulatory accumulation towards systematic consolidation and simplification. With estimated savings of at least €1 billion per year and €5 billion by 2029, the initiative seeks to balance three key objectives: reducing the administrative burden, maintaining high standards of protection and strengthening Europe's competitiveness in the global digital market.

The proposed changes follow a rationale of horizontal consolidation that cuts across the digital regulatory framework: from the merging of five legislative acts into two main instruments, to the creation of common digital infrastructures such as the Single-Entry Point and the European data intermediation registries.

A. Impact on the EU market and competitiveness

» **Positive effects on competitiveness:** The regulatory simplification can generate significant competitive advantages for European companies, especially SMEs, by reducing compliance costs and facilitating access to data markets. Consolidating the regulatory framework into fewer legal instruments reduces fragmentation and improves legal certainty for cross-border investors and operators.

» **Strengthening digital sovereignty:** The new safeguards for trade secrets and restrictions on transfers to inadequately protected third countries reinforce Europe's strategic autonomy, although they may generate trade frictions with international partners.

- **Energising the data market:** The voluntary regime for data intermediation and altruism, together with the differentiated rules for large companies on the re-use of public data, may affect the balance of market power and create new opportunities for emerging players.

B. Criticisms and risks

- **Risk of fragmentation in implementation:** The dependence on future technical standards (especially for automated signals in the field of digital advertising) and the complexity of transitional periods may lead to an inconsistent application by Member States. Factors such as the divergent interpretation of key concepts ("bespoke services", "high risk", "jurisdictions with inadequate protection"), differences in national technical capacities to implement the Single-Entry Point, and the maintenance of decentralised supervision through national competent authorities may create new barriers to the single market, at least during the transitional phases.
- **Underestimated transition costs:** Although significant savings are projected, technological and organisational adaptation costs can be substantial, especially for medium-sized companies that do not qualify for exemptions but lack the resources of large corporations.
- **Data protection tensions:** The amendments to the GDPR, although technical, may lead to debates on the balance between innovation and the protection of fundamental rights, especially in the context of AI and the processing of special categories of data.

C. Positive highlights

- **Technical and calibrated approach:** The proposal maintains the underlying objectives of the existing legislation while optimising its implementation, respecting the principle of proportionality and preserving high standards of protection of fundamental rights.
- **Innovation in compliance/reg-tech tools:** The Single-Entry Point and common templates represent significant advances in the digitisation of regulatory compliance, with potential for replication in other regulatory areas.
- **Specific attention to SMEs:** The extension of exemptions to SMEs and the differentiated regimes demonstrate sensitivity to the needs of growing companies, a crucial factor for the European innovation ecosystem.
- **Democratisation of access to public data:** The consolidation of the rules on the re-use of public data into a single framework (merging the Open Data Directive and the Data Governance Act into Chapter VIIc of the Data Act) significantly expands the opportunities for access to public information. High-value datasets will be made freely available via APIs and bulk download, while increased differentiated conditions and charges for "very large enterprises" and gatekeepers under the DMA create a more level playing field that favours SMEs, startups, SMCs and new entrants in the data market.
- **Promoting innovation in AI:** Clarifications on the use of legitimate interest for the development and operation of AI systems, together with exemptions for residual processing of special categories of data, reduce legal uncertainties that were holding back innovation. Modifications in automated decisions remove unnecessary restrictions while maintaining safeguards for fundamental rights.

5.2. Implementation considerations

The complexity and cross-cutting scope of the proposed amendments create a need for multidisciplinary legal advice that goes beyond traditional sectoral compliance:

- **Large-scale review of contracts:** Changes in switching cloud, differentiated regimes for 'bespoke' services and new transparency obligations require the auditing and renegotiation of entire contractual portfolios, especially in technology and digital services sectors.
- **Assessment of geopolitical risks:** New safeguards for trade secrets require the development of methodologies to assess third-party jurisdictions, documented refusal protocols and risk mitigation strategies in global supply chains.
- **Redesign of data governance:** Amendments to the GDPR, especially in AI and special categories, require a comprehensive review of privacy by design policies, impact assessment procedures and automated consent/objection frameworks.

- **Integration of reporting systems:** The implementation of the Single-Entry Point requires coordination between legal, technical and cybersecurity teams to ensure interoperability with internal systems and multi-jurisdictional compliance.
- **Strategic advice on regulatory innovation:** Beyond reactive compliance, companies need to have a strategic legal vision that allows them to seize new opportunities (data intermediation, differentiated regimes) and turn compliance into a sustainable competitive advantage.

VI. Next steps in the legislative procedure

The proposed Digital Omnibus Regulation will follow the ordinary legislative procedure laid down in Article 294 of the Treaty on the Functioning of the European Union, with an estimated timetable for final adoption in 2026 and progressive entry into force from 2027.

Phases of the Procedure

- **Institutional transfer:** The proposal has been sent to the European Parliament, the Council of the EU, national parliaments (8 weeks for subsidiarity control), the European Economic and Social Committee and the Committee of the Regions for their respective advisory opinions.
- **First parliamentary reading:** Consideration in the ITRE (lead), IMCO and LIBE (opinion) committees, with amendments and plenary voting.
- **Council position:** Technical analysis in specialised working groups and the adoption of a common position of the Member States.
- **Trilogues and final adoption:** Trilateral negotiations between the Commission, the Parliament and the Council to reach a final compromise.

Opportunities for Participation and Consultation

While the Commission has already conducted extensive prior public consultations (718 responses in the first round, 513 in the second), further opportunities for participation are expected during the parliamentary and Council process, including sector-specific consultations, dialogues with business associations and feedback from civil society organisations.

The stakeholders can influence the process through technical position papers, participation in parliamentary hearings, dialogue with national competent authorities and coordination with European sectoral associations.

VII. Our strategic support services

- **Specialised legislative monitoring:** Detailed monitoring of parliamentary amendments, analysis of national positions in the Council and early warnings on relevant sector-specific amendments.
- **Stakeholder engagement strategy:** Preparation of specialised technical position papers and coordination with European sectoral associations.
- **Participation in public consultations:** Drafting of specialised technical responses, sector-specific impact analysis and coordination of collective responses with other market actors.
- **Implementation advice:** Development of compliance frameworks, identification of future delegated and implementing acts, and transition strategies.

We are available to provide any clarifications or specific advice on the application of these rules to your business.

Contacts

Raúl Rubio
Partner, Intellectual Property and Technology

rrubio@perezllorca.com

T: +34 91 353 45 59

Adolfo Mesquita Nunes
Partner, Administrative Law

adolfomesquitanunes@perezllorca.com

T: +351 912 585 103

Andy Ramos
Partner, Intellectual Property and Technology

aramos@perezllorca.com

T: +34 91 423 20 72

Sara Molina
Partner, Intellectual Property and Technology

sara.molina@perezllorca.com

T: +34 91 423 67 31

Offices

Europe

Barcelona
Brussels
Lisbon
London
Madrid

America

Bogotá
Medellín
Mexico City
Monterrey
New York

Asia-Pacific

Singapore