EUROCHAMBRES

Position on the Digital Omnibus

Position on the Digital Omnibus

Eurochambres welcomes the Commission's Digital Omnibus as a necessary first step toward simplifying Europe's digital regulatory framework but warns that procedural adjustments alone will not address the cumulative compliance burden on businesses. While targeted improvements to the Data Act, GDPR, AI Act, and cybersecurity reporting are positive, genuine simplification requires structural burden reduction, harmonized enforcement, proportionate obligations for SMEs and small mid-caps, and a permanent mechanism to prevent regulatory overload that undermines EU competitiveness and digital sovereignty.

1. Executive Summary

The Commission's Digital Omnibus Simplification Package represents a welcome recognition that Europe's digital regulatory landscape has become fragmented, complex, and costly for businesses to navigate. Eurochambres supports the stated objectives of reducing administrative burdens, improving coherence across legislation, and fostering innovation while maintaining high protection standards.

Key positive elements include the extension of regulatory relief to small mid-caps beyond traditional SMEs, targeted GDPR clarifications that address consent fatigue and data subject rights abuse, streamlined data sharing through integration of the Data Governance Act and related instruments, extended AI Act transition periods tied to standards availability, and the creation of a single entry point for incident reporting under NIS2, GDPR, DORA and related legislation.

However, the proposal focuses predominantly on procedural adjustments rather than structural burden reduction. The cumulative weight of multiple overlapping digital acts remains excessive, particularly for micro and small enterprises lacking specialized compliance resources. Critical gaps persist: the single reporting point does not reduce notification volume, the repeal of the Platform-to-Business Regulation risks creating protection gaps for SMEs on non-gatekeeper platforms, enforcement harmonisation measures are insufficient to prevent fragmented national interpretations, and no permanent mechanism exists to assess and prevent future regulatory accumulation.

Eurochambres calls for measurable burden reduction, proportional obligations aligned with business size and risk, harmonized implementation and enforcement across Member States, realistic transition periods coordinated with authority readiness and standards development, and integration of simplification efforts within the broader EU industrial policy to strengthen digital sovereignty and competitiveness.

2. Detailed Comments on the Proposal

I. Data Act Amendments

Trade Secrets Protection (Articles 4(8) and 5(11))

The addition of a new exemption allowing data holders to refuse disclosure when there is high risk of unlawful acquisition, use, or disclosure to third countries with weaker data protection is positive for trade secret safeguards. However, the requirement that this risk persist "despite technical and organisational measures taken by the user" provided in exclusively in the original ground for permission may render the new provision ineffective in practice. Users seeking unlawful acquisition, use or disclosure will invariably claim sufficient protective measures. The condition should be removed from this exemption or limited to the original economic harm ground, ensuring the new protection against third-country risks operates independently.

Customer-Specific Data Processing Services (Article 31)

The simplified regime for customer-specific, non-standardized data processing services and for SME providers under contracts concluded before September 12, 2025, addresses legitimate business needs. Complex CRM systems, SaaS marketing automation tools, and similar offerings require months of implementation and customization, with costs amortized over contract duration. Clarifying that providers may agree contractual penalties for early termination prevents costly litigation and provides legal certainty. This provision is welcomed without reservation.

Data Governance Act Integration (Articles 32a-32c)

Simplifying registration requirements for data intermediation services reduces bureaucracy and may improve market acceptance and is therefore welcome. Integrating an explicit definition of data altruism organisations should be considered given the loss of certain provisions on data altruism organisations.

Article 32c(b) creates an inconsistency: it permits recognized data intermediation services to use metadata (date, time, geolocation) for service development, contradicting Article 4(13) which requires express contractual consent for such use. If this is intended as lex specialis, it is unclear why only data intermediation services should be privileged. Manufacturers need equivalent access to connected product data to comply with Article 9(4) and (8) of the EU Product Safety Regulation. Consequently, the provision should be generalized in Article 4(13) rather than created as a narrow exception.

Free Flow of Non-Personal Data Integration (Article 32h)

The proposed limitation of data localisation prohibitions to non-personal data only, removing personal data from scope, creates interpretive risk. While personal data localisation is already addressed by GDPR, the new differentiation could generate unintended readings, for example that the legislator deliberately affords weaker protection against localisation measures where data qualify as personal rather than non-personal. The provision should either be maintained without differentiation to preserve clarity.

Data Reuse Directive Integration (Article 32i)

The consolidated wording, particularly improvements from paragraph 3 onward regarding data protection and copyright, is welcomed and enhances legal certainty for data reuse.

II. GDPR Amendments

Pseudonymized Data and Personal Data Definition (Article 4(1) and Article 41a)

The contextual approach to personal data identification, clarifying when pseudonymized data should not be considered personal data, introduces operational flexibility. It allows a case-specific examination of identifiability (e.g. for IP addresses), so controllers are not forced to treat clearly non-identifiable datasets as personal data, avoiding unnecessary GDPR obligations in such cases while preserving full protection where identification remains realistically possible. Close attention needs to be paid to the implementing acts proposed under article 41a in which the commission will specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

Special Categories of Data (Article 9)

The new exceptions for processing special-category data are practical and justified, as they enable AI system development and operation where appropriate safeguards are implemented. Changes to the treatment of biometric data, however, are not strictly necessary, since such processing was already possible on the basis of consent. Further simplification would be welcome by clarifying that Article 9(1) and 4 (15) apply only to data that directly reveals health status and and are therefore within the scope of Article 9 (1).

Data Subject Rights and Abuse Prevention (Article 12)

The clarification that data subject access rights may not be abused for purposes unrelated to personal data protection is essential. In practice, these rights have at times been instrumentalised as a tactical litigation tool in disputes only tangentially linked to data protection, creating unnecessary burdens for authorities and businesses alike. This provision addresses a real enforcement problem and should be retained and clearly communicated to supervisory authorities.

Information Obligations (Articles 13-14)

Extended exceptions to information obligations in Article 13 are welcome. Additionally, businesses need explicit confirmation that public provision of Article 13 and 14 information via website privacy policies satisfies the obligation, avoiding individualized communication requirements for low-risk processing.

Automated Decision-Making (Article 22)

The clarifications, in particular that lit. a is independent of whether the decision could be taken otherwise than by solely automated means are viewed positively.

Data Breach Notification (Article 33)

Simplification of breach notification—requiring reporting only where high risk to rights and freedoms exists, extending the deadline to 96 hours, and creating a single-entry point—reduces compliance burden appropriately. The risk-based threshold aligns notification obligations with materiality while the extended deadline reflects operational realities of incident investigation.

Data Protection Impact Assessment (Article 35)

EU-wide harmonization of DPIA requirement lists is supported in principle, but existing national lists should be grandfathered to ensure legal certainty and business reliance. Businesses should retain the option to rely on current paragraphs 4 and 5 provisions to avoid disrupting established compliance processes.

ePrivacy and Consent Management (Articles 88a-88b)

The objectives of simplified consent processes harmonized legal frameworks, and technology-neutral standards are welcome. Eliminating dual GDPR/ePrivacy regimes could reduce complexity, though Article 5(3) of Directive 2002/58/EC remains applicable to non-personal information and legal entity data, limiting true harmonization.

Defining processing purposes not requiring consent, including website analytics, addresses longstanding market needs and is welcomed. However, serious technical challenges exist with browser-based consent management under the Interactive Advertising Bureau (IAB) Transparency & Consent Framework (TCF). The TCF requires renewed consent display when vendors or cookies change, yet Articles 88a-88b would prohibit re-obtaining consent for six months after refusal. Even users who consented would require re-prompting under TCF technical standards, creating regulatory-technical conflict.

Concentration of consent management in browsers controlled by large US corporations is not aligned with the EU's agenda on technological sovereignty and strategic autonomy and eliminates direct customer relationships for website operators and advertisers.
Differential treatment of media company websites (exempted under the European Media Freedom Act) versus other websites creates competitive distortions that need to be addressed. Namely, a disadvantage could arise for advertising industry and media companies if other websites do not display consent banners anymore.

If browser-based consent proceeds, strict equal treatment obligations on browser manufacturers through Commission-imposed standardization requirements are essential. Eurochambres believes that the proposed six-month transition period is insufficient for resolving these technical conflicts; a substantially longer implementation period is required.

AI and Personal Data Processing (Article 88c)

Introducing legitimate interest as a legal basis for certain AI-related processing of personal data (Article 9(2)(k) and Article 88c) addresses a genuine regulatory need and is a welcome development. However, the way data subject rights are applied to model training and operation needs to reflect what is technically and economically realistic for large AI systems.

The insertion of Article 88c will only be fruitful if Articles 12, 15-17 and 21 are changed to account for the technical specifications of large AI models.

For modern large models, personal data is not stored as discrete, retrievable records but is diffused across model parameters learned from many examples. Demanding exact, per-person "machine unlearning" via retraining or equivalent for every successful rectification or erasure request is therefore technically and economically infeasible at scale, even though research into unlearning methods is ongoing and can support more limited or approximate forms of forgetting.

A more workable and balanced approach would be to clarify, in the data subject rights provisions, that:

- Controllers must remove a person's data from future training or fine-tuning datasets and from structured logs under their control.
- Controllers must correct or suppress harmful outputs and profiling that affect the individual (for example by adjusting downstream systems, filters or business rules).
- Controllers are not required to perform technically infeasible per-request unlearning on already trained large models, provided they implement alternative safeguards that effectively protect individuals.

This clarification could be implemented through a general rule in Article 12, supplemented by targeted adjustments in Articles 15, 16, 17 and 21, so that the substance of access, rectification, erasure and objection is preserved but applied in a way that is compatible with AI system architecture. As a reference point, well-protected models should be treated more like anonymised data: what matters is that an individual cannot reasonably be identified or harmed via the model, rather than that every past contribution can be surgically removed from its parameters.

III. NIS2 Amendments

Single Entry Point for Incident Reporting (Article 23a)

Standardizing reporting obligations across GDPR, NIS2, DORA, CRA, CER, eIDAS and related instruments through a single-entry point is helpful for cross-border operators. However, timing is critical: NIS2 national implementation is ongoing, and companies are currently integrating reporting processes. Rapid implementation of the single-entry point is essential to avoid requiring process redesigns shortly after initial implementation. Alternatively, a generous transition period should be provided.

The single-entry point should genuinely replace, not supplement, existing reporting channels. Companies should fulfil all obligations (including under DORA) without additional effort beyond a single submission. Volume of notifications is not reduced—only channels are consolidated—so the system must minimize administrative friction through digital-by-default processes, structured templates, and information reuse.

IV. Platform-to-Business Regulation Repeal

Critical Protection Gaps

Eurochambres is of the opinion that DSA and DMA provisions do not fully replace the Platform-to-Business Regulation. While some overlap exists, the DSA and DMA pursue different objectives (illegal content moderation, gatekeeper competition) and apply graduated protections tied to platform size thresholds. Many marketplaces and comparison platforms used by SMEs fall below VLOP or gatekeeper designations, leaving commercial users without protections the P2B Regulation currently provides.

Eurochambres believes that the bureaucratic burden imposed by the P2B Regulation **does not justify its abolition**. At just 19 articles, the regulation is relatively streamlined and not particularly onerous compared to other EU frameworks.

Terms and Conditions Clarity (Articles 3 and 15)

The P2B Regulation provides precise requirements for B2B terms and conditions and changes to these, reflecting the distinct nature of commercial relationships versus B2C consumer protection. Article 14 DSA addresses terms and conditions but is designed for consumer-facing illegal content issues. Eliminating P2B protections could create loopholes in B2B contractual governance, particularly for SMEs negotiating with platforms possessing superior bargaining power.

Without the P2B's tailored rules on notice and statement of reasons for suspension or termination, platforms could more easily delist or cut off business users with shorter notice, less justification and fewer avenues to contest decisions, threatening business continuity for dependent SMEs.

The removal of explicit B2B transparency on ranking parameters and paid or self-preferential boosts would make it harder for SMEs to understand why their offers lose visibility and to detect discriminatory treatment, while the loss of specific constraints on most-favoured-nation (MFN)/parity clauses would increase pressure to accept wide parity terms that lock them into giving one platform the best conditions everywhere, reducing their ability to compete via better prices on their own channels or alternative platforms.

Finally, if representative action and structured internal complaint mechanisms tailored to business users are weakened or not fully replaced, SMEs would have fewer collective tools to challenge unfair platform practices, making enforcement more fragmented and costly at national level.

Account Suspensions (Article 4)

The proposal temporarily retains Article 4 on advance notice for account restrictions or suspensions. **This provision should be made permanent.** Neither DSA nor DMA provides equivalent early warning protection for business users against unexpected account suspensions that can destroy revenue streams overnight. SMEs dependent on platform access for market reach require this safeguard regardless of platform size.

Price Parity Transparency (Article 10)

P2B Article 10 requires platforms to disclose and justify any MFN clauses that restrict business users from offering better prices or conditions elsewhere (own website, competing platforms, other channels).

This transparency makes it easier for SMEs, regulators and courts to see when wide parity clauses are used, assess their competitive impact, and challenge those that lock retailers into giving a platform the best deal across all channels, compressing margins and restricting competition. By reducing information asymmetries and exposing MFNs to public and enforcement scrutiny, it helps deter the most harmful clauses, whereas the DSA and DMA contain no equivalent provisions on parity clauses for non-gatekeeper platforms, leaving this safeguard without replacement if P2B is repealed.

Complaint Systems (Article 11)

Article 11's complaint and mediation system should be fully retained. While the DSA includes complaint mechanisms, these are designed primarily for illegal content disputes. Business users facing commercial disputes—over rankings, contract terms, or unfair practices—need dedicated complaint pathways with appropriate expertise and remedies. Relying solely on DSA mechanisms risks inadequate handling of B2B commercial issues, costing companies time and money. In addition, any future framework should ensure simple, and unbureaucratic access for SMEs to external mediators, so that smaller business users can effectively enforce their rights in practice.

V. AI Act Amendments

General Assessment

The proposed amendments represent meaningful steps toward reducing AI Act compliance burdens, particularly for SMEs and small mid-caps. Key improvements include:

- shifting AI skills obligations from individual companies to Member States and the Commission.
- standardizing notification authority application and evaluation procedures
- establishing codes of conduct for national authority notification
- harmonizing cybersecurity requirement recognition
- creating EU-level AI sandboxes
- extending quality management system exemptions for SMEs to high-risk AI
- extending transition periods for high-risk systems from August 2, 2026 to December 2, 2027, and from August 2, 2027 to August 2, 2028 contingent on standards availability, and providing additional practical implementation guidance.

These are substantive improvements that acknowledge resource constraints facing smaller providers and align compliance timelines with the readiness of standards, authorities, and conformity assessment infrastructure. In supporting businesses in their use of AI, the commission and member states should focus on pragmatic compliance tools such as checklists and standardised classification aids. Any new requirements must be compatible with established standards (e.g. ISO 27001, NIS2).

In shaping and implementing the Digital Omnibus on AI, transparency obligations for AI providers should be designed to minimise risks in the AI supply chain, while open interfaces should be promoted to prevent vendor lock-in and support Europe's digital sovereignty.

Extension of Support Measures to Small Mid-Caps

The extension of certain relief measures from SMEs to small mid-caps is welcome. Particularly the support of these companies, which are in an early growth phase, must be strengthened to further enhance competitiveness. These small and mid-caps are especially affected by rigid threshold values, as even slight growth triggers an abrupt transition into full regulation (regulatory cliff). When considering size classes for mid-caps, the threshold values (aligned with, for example, procurement) should be discussed to be raised to 1,000 employees. Alternatively, a sliding transition phase for growing companies should be considered.

Real-World Testing and Regulatory Sandboxes (Article 60a (1)-(2))

Expanding real-world testing opportunities is supported in principle, but the proposed mechanism of voluntary bilateral agreements between individual Member States and the Commission creates legal fragmentation and unequal competitive conditions. No uniform criteria govern what these agreements may contain or how far exceptions can extend, raising constitutional and rule-of-law concerns.

Eurochambres recommends establishing a clear, exhaustive list of possible regulatory exceptions that Member States may elect to apply within their jurisdictions through transparent procedures. This approach—used successfully in other EU regulations (e.g., Regulation 2021/782 allowing Member States to decide whether passenger rights apply to urban transport)—preserves legal certainty and predictability while allowing national flexibility. Each Member State decides based on its legal system and innovation policy, but within defined parameters established at EU level. This would prevent ad hoc bilateral arrangements creating competitive distortions and ensures businesses can understand the regulatory environment in advance.

Public Administration Compliance Timeline (Article 111(2))

Extending public administration compliance to August 2, 2030—substantially longer than private sector deadlines—is unjustified. State deployment of AI, particularly in law enforcement, social services, and public security, often poses higher risks to fundamental rights than private sector applications. Differential treatment creates a problematic two-tier system where public authorities, who should model regulatory compliance, receive extended timelines while businesses face immediate obligations. Public and private actors should be subject to identical entry-into-force schedules to ensure equal protection and avoid undermining regulatory legitimacy.

Eurochambres – the association of European chambers of commerce and industry – represents more than 20 million businesses through its members and a network of 1700 regional and local chambers across Europe. Eurochambres is the leading voice for the broad business community at EU level, building on chambers' strong connections with the grass roots economy and their hands-on support to entrepreneurs. Chambers' member businesses – over 93% of which are SMEs – employ over 120 million people.

Previous positions can be found here.

Contact:
Eurochambres Policy Advisor
Mr Cornelius Knaack, Tel. +32 2 282 08 91, knaack@eurochambres.eu

Eurochambres Press and Communication Manager
Mrs Karen Albuquerque, Tel. +32 2 282 08 72, albuquerque@eurochambres.eu

Eurochambres Press Contact
Mr Alexander Maurer, Tel. +32 2 282 08 62, maurer@eurochambres.eu

@Eurochambres
@eurochambres.bsky.social
www.eurochambres.eu