EuroCommerce
Retail & Wholesale

Position Paper
08 June 2026

Position Paper on the Digital Omnibus

Key recommendations

1. Deliver clear, consistent and predictable rules across the data acquis. The Omnibus should remove fragmentation by ensuring uniform definitions, roles and supervisory practices under the Data Act, so businesses can rely on one coherent framework across the Single Market.

2. Modernise cookie and tracking rules through a risk-based, practical model (Art.88a & 88b GDPR). Europe needs rules that address consent fatigue, support innovation while upholding consumer rights. This requires:

- **Introducing a truly risk-based approach to cookies and tracking**, allowing low-risk and essential processing to take place without unnecessary consent requirements, and recognising the role of privacy-enhancing technologies (PETs);
- **Avoiding mandatory browser-level automated and machine-readable consent indications**, which risk creating new gatekeepers, and
- **Rejecting rigid rules such as the six-month ban on renewed consent**, and instead promoting flexible and proportionate approaches to reducing consent fatigue

3. Deliver meaningful GDPR simplification and reduce compliance burdens, particularly for SMEs. The Omnibus should ensure effective and risk-based simplification. This includes clarifying that information is not personal data where an individual cannot reasonably be identified, as providing clear guidance on anonymisation and the proportionate treatment of low-risk data.

4. An effective EU level Single-Entry Point (SEP) for cybersecurity incident reporting. The SEP must become a true **"report once" system**, with harmonised thresholds and templates, to provide full interoperability with national regulatory authorities, and clear allocation of responsibilities so businesses can operate with certainty and comply efficiently across GDPR, NIS2, DORA, CRA and CER.

Retail and wholesale are essential enablers of Europe's digital transformation, generating around 10% of EU GDP and accounting for one in three European companies, the vast majority of which are SMEs. As the main interface with consumers and a major deployer of digital tools across supply chains and operations, the sector plays a decisive role in ensuring that EU digital legislation delivers practical impact on the ground. A predictable and coherent regulatory environment is therefore critical to enable investments and maintain EU's global competitiveness in an increasingly digital and competitive market.

The Digital Omnibus offers an opportunity to **simplify, streamline and future-proof the EU's digital rulebook** so that businesses, particularly SMEs, can focus on innovation, security and competitiveness rather than navigating duplicative or inconsistent requirements.

1. The data acquis (Data Governance Act, Free Flow of Non Personal Data Regulation, Open Data Directive)

The consolidation of the EU data framework into the Data Act can potentially reduce fragmentation and improve legal certainty, provided that the resulting rules are **clear, predictable and applied consistently across Member States**. Retail and wholesale rely on long-term data arrangements for supply-chain operations, digital services, product support and compliance. Ambiguity in definitions, roles or supervision creates risks and undermines investment.

1.1 Clarity and consistency across Member States

The consolidation of the data acquis into the Data Act can only deliver genuine simplification if definitions, roles and supervisory responsibilities are applied consistently across the Single Market. Retailers and wholesalers operate in complex, multi-actor and cross-border value chains, and therefore require clear and uniform guidance on key concepts such as the source provider, the scope of cloud-switching obligations, and the respective responsibilities of competent authorities. Without such clarity, companies face fragmented national interpretations, legal uncertainty and increased compliance costs, undermining the intended benefits of the Digital Omnibus.

To ensure predictable application, the enforcement landscape must also be coherent. This requires effective designation of national authorities, transparency regarding their mandates, and clear information on penalty regimes to avoid inconsistent or disproportionate enforcement across Member States.

- Ensure clarity on roles, including the concept of source provider (Art. 25 Data Act), switching obligations and supervisory responsibilities, critical for businesses operating in complex digital value chains.
- Guarantee effective and transparent appointment of competent authorities, including clear information on applicable penalty regimes to provide legal certainty for businesses.

1.2 Platform Regulation (P2B)

The Commission plans to repeal the P2B Regulation while retaining a limited set of provisions for legal certainty. We believe that **key P2B safeguards remain essential for business users, particularly SMEs**, and which **cannot be fully replaced by the DSA or DMA**, whose objectives and scope differ from the P2B Regulation, and many provisions only apply to very large platforms or designated gatekeepers.

EuroCommerce therefore calls for the retention or effective integration of core P2B safeguards, in particular:

- Article 4 (unexpected account suspension), which provides a critical early-warning protection not replicated elsewhere;
- Article 10 (transparency on pricing, ranking and parity clauses), which is not covered by the DSA or DMA;
- Article 11 (complaint handling and access to dispute resolution), including the possibility for business users to turn to independent external dispute resolution bodies where internal mechanisms fail. Access to external dispute resolution under the current framework can be administratively burdensome for SMEs, removing this safeguard would be counterproductive. Instead, any successor framework should ensure simple, low-threshold and unbureaucratic access to external dispute resolution, preserving a crucial protection while improving its practical usability for SMEs.

2. Rules on cookies and other tracking technologies (articles 88a & 88b GDPR)

The Digital Omnibus proposal represents an opportunity to modernise Europe's outdated cookie rules and move towards a **harmonised, risk-based and user-friendly approach**.

We strongly support the European Commission's proposal to bring cookie enforcement within the remit of the GDPR and its one-stop-shop mechanism where personal data is involved. Currently, Article 5(3) of the ePrivacy Directive does not specify how enforcement jurisdiction should be allocated among Member States, and divergent approaches by national supervisory authorities have resulted in an inconsistent enforcement landscape that undermines the coherence of the Digital Single Market. The GDPR's one-stop-shop mechanism, by contrast, provides coordinated enforcement through a single lead supervisory authority based on an organisation's country of main establishment, offering the predictability and legal certainty that cross-border operators require. EuroCommerce considers this alignment a priority element of the Digital Omnibus.

At the same time, Articles 88a and 88b GDPR introduce significant operational, competitive and practical concerns that risk undermining simplification efforts across the Single Market.

2.1 A risk-based framework is essential (Art. 88a)

EuroCommerce strongly supports a shift towards a risk-based framework, consistent with the GDPR and its legal bases for processing of personal data, allowing controllers to rely on legitimate interest for low-risk, essential processing activities. The current proposal does not sufficiently reflect the realities of modern retail and e-commerce operations, where a wide range of low-risk processing is integral to security, service reliability, fraud prevention, product maintenance, aggregated analytics, software updates, contextual advertising and personalisation based on first-party data. In this context, we encourage the development and deployment of Privacy-Enhancing Technologies (PETs). Where such technologies effectively reduce risks to individuals, such as on-device processing, differential privacy, or other privacy-by-design techniques, requiring consent does not provide additional protection, but instead discourages their use. A risk-based framework under Article 88a should therefore explicitly support PET-based processing to reduce consent fatigue while strengthening data protection outcomes.

EuroCommerce therefore calls for:

- Explicit alignment of Article 88a with all Article 6 GDPR legal bases, enabling low-risk processing to rely on appropriate legal bases, including legitimate interest;
- The establishment in Article 88a of a general, risk-based exemption for low-risk processing, based on clearly defined indicators that create a rebuttable presumption of low risk, in line with the GDPR's risk-based approach and technology-neutral principles. This should include the use of cookies or similar technologies for security, service reliability, fraud prevention, product maintenance, aggregated analytics, software updates, contextual advertising and personalisation based on first-party data.

2.2 Mandatory browser-level, machine-readable consent indications (Article 88b GDPR) pose major risks

EuroCommerce recognises the goal of simplifying user choices, but Article 88b GDPR, which mandates browser-level automated and machine-readable consent indications, presents major risks for both consumers and businesses, and would significantly undermine the competitiveness of retailers.

This approach would centralise control over consent in browsers and operating systems, effectively creating digital "consent" gatekeepers and weakening retailers' and e-commerce companies' ability to engage directly with their customers. Such systems cannot provide valid, specific and informed GDPR-compliant consent, since consent must reflect a controller and purpose-specific context, something a blanket browser signal cannot do. This model would result in undifferentiated decisions, reduce users' ability to tailor preferences per service, and disproportionately harm SMEs that rely on more customised user interactions. Finally, assessments underscore the technical unworkability of implementing consistent overrides, distinguishing exempted media services, and managing frequent changes in service providers.

EuroCommerce therefore does not support introducing mandatory browser-level consent mechanisms. Any future consideration of such systems must be preceded by thorough impact assessment on retail competitiveness, innovation and investment, strong safeguards against market concentration, and clear evidence that they would improve, not degrade, user experience and compliance feasibility.

2.3 Six-month prohibition on renewed consent is disproportionate

Prohibiting controllers from re-requesting consent for the same purpose for at least six months would be counterproductive. This rigid rule can:

- force additional tracking to ensure the rule is respected;
- prevent users from changing preferences in evolving contexts;
- break essential operational flows, particularly where user settings vary by device;
- adds unnecessary complexity for SMEs.

EuroCommerce supports the intention to reduce consent fatigue, but urges legislators to adopt a flexible, risk-based approach rather than a fixed six-month timeframe. Controllers should be able to design proportionate mechanisms that respect users' choices without introducing technical burdens or new risks.

3. GDPR simplification and burden reduction

The targeted amendments to the GDPR introduced by the Digital Omnibus offer a welcome opportunity to improve legal certainty, reduce unnecessary compliance burdens, and support a more proportionate, risk-based approach to data protection compliance. Retailers and wholesalers operate in diverse and complex data environments involving multiple supply-chain actors, digital services, and operational data flows. Fragmented national practices, overlapping reporting requirements and inconsistent interpretations continue to generate high compliance workloads, particularly for SMEs.

Retailers across the EU face increasing operational challenges linked to theft, fraud and the protection of property, which can have wider economic implications, including on investment capacity and consumer prices. In this context, a clear and consistent application of Article 6(1)(f) GDPR is important to ensure that businesses can rely on legitimate interests for proportionate and necessary processing related to security and loss-prevention purposes. Divergent interpretations across Member States can create legal uncertainty and limit the effective use of such measures in practice. A more coherent and

predictable EU framework, consistent with the GDPR's risk-based approach, would help ensure an appropriate balance between legitimate business interests and fundamental rights, while reducing fragmentation across the Single Market. The Omnibus proposal marks a positive step by clarifying core concepts, harmonising breach-reporting thresholds, simplifying obligations for low-risk processing, and EU-wide compliance tools. However, this will only work if it is implemented consistently across the Single Market and supported by practical guidance.

3.1 Meaningful, risk-based simplifications for SMEs

SMEs make up 99% of retail and wholesale businesses and regularly face disproportionate burdens even when processing is routine or low-risk. Existing exemptions are too often theoretical, as SMEs remain embedded in complex supply chains that require extensive documentation, contractual due diligence and reporting. EuroCommerce calls for:

- Meaningful SME exemptions that reflect real operational realities rather than theoretical carve-outs;
- EU-level digital tools (privacy notice templates, processor agreement templates, DPIA models, record-keeping tools) to reduce reliance on costly consultancy and ensure scalability for SMEs.

3.2 Clarifying the scope of personal data, anonymisation and pseudonymisation

The Omnibus clarification that **information is not personal data for a given entity if it cannot reasonably identify an individual is a crucial step to prevent over-expansive interpretations**. This reflects well established case law and is strongly supported by members. This is particularly important for low-risk operational and business data i.e. technical identifiers, supplier contacts, pseudonymised anonymised and encrypted datasets where excessive classification as "personal data" adds burdens without providing meaningful safeguards.

Retailers increasingly rely on anonymisation and pseudonymisation techniques to enable analytics, innovation and operational efficiency. However, ongoing uncertainty as to whether anonymisation processes themselves require a legal basis or specific justification can act as a barrier to their deployment. EuroCommerce therefore supports clarifying that the process of anonymization, understood as irreversibly removing the link to an identifiable individual, should not require a separate legal basis, provided that appropriate technical and organisational safeguards are in place.

At the same time, such clarifications must be accompanied by clear EU-level guidance and assessment criteria, to avoid legal uncertainty and preserve a high level of fundamental rights protection. Guidance should address the application of technical safeguards, security obligations, contractual responsibilities between controllers and processors, and breach notification duties in complex data-processing chains. EuroCommerce supports:

- The clarification of the legal definition of identifiability;
- Complementary EU-level guidance to ensure uniform Member State interpretation;
- A proportionate, risk-based approach to low-risk business data supported by appropriate technical and organisational safeguards.

3.3 Clarifying the scope of the right of access (Article 15)

Retailers increasingly receive broad or abusive access requests that include incidental metadata or internal communications, creating heavy workloads without meaningful added value for data subjects. This goes beyond the legislators' original intention and places a burden on companies without any discernible added value for data subjects. The Omnibus improves the ability to reject excessive or abusive requests, but further clarity is needed to ensure consistent enforcement. EuroCommerce supports:

- Clarifying that Article 15 applies to personal data actually used to make decisions about an individual, not incidental or irrelevant internal information.

3.4 Alignment of GDPR obligations with AI-related processing (Article 88c GDPR)

Article 88c introduces a new legitimate-interest basis for processing personal data in the development and operation of AI systems, which we broadly welcome as a step toward greater legal certainty. However, its effectiveness will depend on clearer guidance: **the concepts of "necessity"** and the balancing test remain open to divergent national interpretations, national laws may still override legitimate interest by re-imposing consent, and practical issues such as the technical impossibility of deleting model-embedded data must be realistically addressed.

An unconditional right to object under Article 88c, going beyond the existing GDPR framework, could impose disproportionate operational burdens on SMEs.

For example, a small retail company may use a simple AI-based tool to group customers based on their likelihood to reorder or require follow-up. If a customer exercises an unconditional right to object, the company may be required to remove that individual's data from the model and ensure it no longer influences outcomes. In practice, this could require retraining or significantly modifying the model. For SMEs lacking dedicated data science resources, such obligations are often technically unfeasible and economically disproportionate. These risks discouraging the use of even low-risk, basic AI tools, undermining the Digital Omnibus' objective of supporting innovation and competitiveness, particularly among smaller operators. This illustrates the need for Article 88c to remain firmly anchored in the GDPR's risk-based and proportionality principles, with safeguards that avoid creating obligations that are technically unrealistic or economically prohibitive for SMEs.

To ensure Article 88c genuinely supports innovation while maintaining robust safeguards, **coherent EU-level guidance and alignment with the AI Act are essential.**

EuroCommerce supports:

- Recognising legitimate interest as a valid basis for AI-related processing under Article 88c;
  Providing EU-level guidance to ensure harmonised interpretation of "necessity" and the balancing test across Member States.

3.5 Simplifying records of processing (Article 30)

The Omnibus simplifies obligations by raising thresholds and removing unnecessary triggers, enabling companies to focus resources on higher-risk processing. EuroCommerce urges to:

- Support raising the threshold for record-keeping and removing the "occasional processing" criterion, ensuring all low-risk processing benefits from simplified requirements regardless of company size;
- Encourage the development of EU digital tools to help SMEs meet documentation obligations efficiently.

3.6 Harmonising breach reporting (Article 33)

The shift to a high-risk notification threshold and the extension of the reporting deadline to 96 hours represent meaningful improvements, reducing defensive reporting and allowing businesses to prioritise incidents that genuinely pose risks. Members also welcome alignment with the future Single-Entry Point for incident reporting. EuroCommerce supports:

- The new **high-risk reporting threshold and the extended 96-hour deadline**, which improve consistency and reduce unnecessary administrative burdens.

3.7 Guidance on overlaps with sectoral and horizontal digital legislation

Retailers must navigate overlapping obligations under GDPR, NIS2, DORA, the Cyber Resilience Act, CER and the AI Act. Without coordination, these parallel requirements lead to duplicated assessments, inconsistent reporting expectations and fragmented enforcement. EuroCommerce supports:

- Clear EU-level guidance on the interaction between GDPR and sector-specific legislation.
- Applying the once-only principle for risk assessments and reporting across legislation, supported by harmonised templates and cross-regulatory mapping.

3.8 Art. 40-41: clarify rules for Codes of Conduct

The requirements for drawing up a GDPR code of conduct are cumbersome. The GDPR states in Art. 41(1) that “monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority”. The EDPB and Dutch DPA have interpreted the word 'may' of the GDPR as an obligation to establish a monitoring body of the Code of Conduct. This has created an additional barrier to the drafting and use of codes of conduct. This body must have extensive financial resources to be able to absorb a fine. We ask clarification that the monitoring body is not mandatory.

3.9 Biometric data: 1:1 verification and 1:N identification

We welcome the clarification introduced by the Digital Omnibus distinguishing between biometric verification (1:1 authentication) and biometric identification (1:N identification). By confirming that biometric data processed exclusively for identity verification, where the data or means remain under the sole control of the data subject and appropriate safeguards apply, does outside the general prohibition of Article 9 GDPR, the proposal provides much-needed legal certainty for low-risk and widely used authentication use cases. At the same time, high-risk biometric identification remains subject to Article 9 safeguards. This clarification aligns the GDPR with the AI Act’s risk-based approach and is an important step toward proportionate, technology-neutral data-protection rules, while its practical application will depend on consistent and workable interpretation of the “sole control” requirement.

4. Cybersecurity related incident reporting obligations

The current framework requires businesses to report similar incidents under multiple acts (NIS2, GDPR, DORA, CRA, CER) via different portals, in different formats and languages, and on conflicting timelines often during crisis response. This leads to duplication, administrative burden and operational challenges.

4.1 Single-Entry Point (SEP) for Incident Reporting

EuroCommerce strongly supports the Digital Omnibus proposal to simplify cybersecurity incident reporting and to create an EU-level Single-Entry Point (SEP) operated by ENISA, enabling entities to submit one report to satisfy multiple legal obligations ("report once, share many"). To ensure that cybersecurity delivers on its promise, EuroCommerce highlights the following essential elements:

- **Harmonised templates, thresholds and definitions are indispensable**: Key concepts such as "significant impact", incident classification categories, required data fields and thresholds for early notification must be aligned across NIS2, GDPR, DORA, CRA and CER. This is essential for avoiding conflicting or duplicative obligations, making the SEP operational, and for supporting consistent application across Member States.
- **Interoperability at national and European level is critical:** The SEP must integrate with national authorities' systems through APIs and machine-readable formats to ensure seamless rerouting of incident data. This alignment is particularly important given differing national readiness levels for NIS2 implementation and to resolve divergent interpretations of core concepts.
- **Targeted reporting based on legal relevance**: The SEP should, by-design, ensure that incident notifications are shared only with the authorities and legal frameworks that are actually concerned by the incident. Companies should not be required, nor incentivised, to notify data protection or information-security authorities of incidents that are clearly not reportable under the applicable legal framework.
- **Clear allocation of responsibilities between companies and authorities**: The SEP should confirm that once a company submits a complete notification, responsibility for onward transmission and coordination between competent authorities lies entirely with the authorities, not with companies. Companies' interactions with the SEP should generate an auditable information trail, supporting their overall compliance posture.
- **Avoidance of multiple sanctions for the same incident:** Clear safeguards are needed to prevent the imposition of multiple fines or penalties for a single incident reported via the SEP, depending on the reporting route or legal basis.
- **Prior testing involving industry before launch:** To ensure confidence in the SEP and to avoid creating cybersecurity risks arising from centralization of incident reporting material, companies should be involved in the testing and evaluation of the SEP to build trust among users. The SEP's architecture must incorporate robust resilience and security safeguards, including redundancy mechanisms and regular security audits, to ensure it does not become a single point of failure.
- Language and usability considerations must be addressed. For urgent notifications, the use of common EU working languages should be permitted, with clear rules for translation of follow-up reports. This is essential for cross-border operators who must report the same incident in multiple jurisdictions.

Automation-ready processes should be mandated, including APIs, interoperable taxonomies and formats, secure identity and authentication mechanisms, and a company dashboard enabling entities to retrieve submissions, acknowledgements, follow-up requests and closure notices. This reduces manual work and error risks.

EuroCommerce
Retail & Wholesale

Position Paper

Contact:
Helene Paterson | Adviser Digital Transformation, **paterson@eurocommerce.eu**

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 27 countries and 5 million companies, including leading global players and many small businesses. Over a billion times a day, retailers and wholesalers distribute goods and provide an essential service to millions of business and individual customers. The sector generates 1 in 7 jobs, offering a varied career to 26 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector.