Swedish Commerce Position Paper – Digital Omnibus

1. Introduction

Swedish Commerce welcomes the European Commission's Digital Omnibus initiative as an opportunity to simplify, harmonise and future-proof the EU's digital regulatory framework. For retail and wholesale—sectors that sit closest to consumers and depend on scalable, cross-border digital services—effective simplification must yield clearer responsibilities, less duplication, and genuinely risk-based requirements that are workable in practice.

While the EU's digital rulebook has strengthened trust in the single market, overlapping obligations and fragmented interpretation have increased administrative burdens and legal uncertainty. The Digital Omnibus, together with the Digital Fitness Check, should therefore focus on reducing duplication and improving coherence across key instruments (GDPR, the ePrivacy framework, AI Act, Data Act, cybersecurity reporting obligations), while preserving high standards of protection.

A priority for Swedish Commerce is that reforms on cookies and tracking technologies—particularly Articles 88a and 88b—reduce consent fatigue, enable low-risk processing necessary for secure and functional services, and avoid shifting market power to a few dominant gatekeepers.

Retail-specific context: unlike most sectors, retail and wholesale often operate simultaneously across multiple regulated domains (e.g., energy production via rooftop solar, healthcare/medicines, food, chemicals, finance/payments). As a result, retailers can be subjected to several parallel supervisory regimes for the very same internal cybersecurity and data governance systems. The Omnibus must address this supervision sprawl through coordination and once-only compliance principles.

2. Fundamental Principles

Swedish Commerce believes the Digital Omnibus should be guided by four principles:

- **Clarity and Legal Certainty —** Rules must be precise, implementable, and supported by timely guidance and standards. Ambiguity leads to over-compliance, inconsistent enforcement, and barriers to innovation.
- **Harmonisation and Competition Neutrality —** Digital rules must work uniformly across the Union and avoid design choices that advantage certain actors (e.g., operating system or browser providers) at the expense of businesses and consumers.

- **Proportionate, Risk-Based Requirements —** Obligations should reflect actual privacy, security, and consumer risks—not theoretical worst cases. Low-risk processing should not trigger high-burden compliance.
- **Genuine Burden Reduction —** Simplification must reduce duplication and administrative load. New templates, portals, and documentation requirements should streamline compliance rather than expand it.
- **Retail-Specific Proportionality —** Recognise that retailers/deployers often lack leverage to modify standardised digital services. Compliance architectures and accountability must therefore place realistic duties on providers and intermediaries, not only on controllers at the end of the value chain.

European retailers compete in a global digital environment where many core technology providers and platforms are non-European. The Digital Omnibus must therefore ensure that simplification efforts primarily benefit European companies, rather than inadvertently granting third-country providers an additional competitive advantage. If obligations continue to fall disproportionately on deployers at the end of the value chain—while global platforms face lighter duties or weaker enforceability—EU businesses risk structural disadvantages. Retailers have limited influence over the design of standardised digital services and depend on providers setting global, non-negotiable terms. To safeguard Europe's competitiveness, obligations must follow actual control, avoid deepening dependence on dominant gatekeepers, and enable European retailers to build secure, data-driven and innovative services without administrative burdens that global competitors do not face.

3. GDPR – Definitions, Roles, and Practical Application

3.1 Definition of personal data and pseudonymisation

Clarify the notion of identifiability using an actor-relative, 'reasonably likely' test, aligned with existing guidance on anonymisation and pseudonymisation. This avoids both over-inclusion and gaps where actors deny responsibility by asserting that data is not personal despite realistic linkage risks for others. Provide concrete implications for pseudonymised data sharing (e.g., whether DPIAs, TIAs and SCCs are required when recipients have no realistic means of re-identification).

3.2 Controller/processor and joint controllership

Strengthen and clarify responsibilities of standardised service providers acting as processors. Where providers exert material influence over purposes or means through non-negotiable designs, joint controllership or heightened processor obligations should apply. Deployers should not bear sole accountability where they lack practical control over technology design or operational safeguards.

3.3 Purpose limitation and compatible purposes

Provide practical guidance on ‘compatible’ further processing in common business contexts—especially processing objectively linked to delivering a secure, reliable and improved service within users’ reasonable expectations.

3.4 Information duties and abusive requests

Discourage abusive or tactical use of data-subject rights and calibrate information duties to risk and practical relevance, so accountability remains meaningful rather than formalistic.

3.5 Documentation – simplify and align

Set clearer minimum documentation expectations and model structures usable across multinational groups, enabling efficient governance while remaining audit-ready.

4. Cookies and Tracking Technologies – A Risk-Based Modernisation

4.1 Article 88a – Consent should target genuine high-risk processing

Differentiate clearly between high-risk tracking (e.g., cross-site profiling, behavioural advertising, sensitive inference) and low-risk processing required to operate, secure and improve services. Explicitly allow, without consent, processing strictly necessary for: (i) security and fraud prevention; (ii) basic functionality and user-requested features; (iii) performance and reliability (caching, load balancing); and (iv) aggregated, non-individual output analytics used solely to improve the controller’s own service.

4.2 Article 88a – Practical consent mechanics

Clarify how long consent can be relied upon for the same purpose, and how rules apply when services, vendors, or configurations change. Encourage interoperable consent-management implementations so controllers can adopt conforming CMP solutions without bespoke development.

4.3 Article 88b – Machine-readable signals must not create gatekeeper dominance

Design machine-readable signals as open, interoperable standards—not as mechanisms for unilateral control by a few browsers or operating systems. Avoid double-layer consent experiences, ensure competition-neutral implementation duties for intermediaries, and align application timelines with the availability of harmonised standards.

4.4 Scope of exemptions

Provide clear guidance on which analytics and statistical tools fall under low-risk exemptions and where aggregated insights end and high-risk profiling begins—reducing fragmentation and ensuring consistent user experiences across the Union.

5. AI Act – Clear Value-Chain Roles and Practical Safeguards

5.1 Provider vs deployer responsibilities and "substantial modification"

Establish objective criteria for 'substantial modification' so standard integration, configuration or limited customisation by deployers does not trigger provider responsibilities or misclassification.

5.2 Sensitive data for bias detection (Article 4a)

Maintain a narrow, strictly-necessary basis to process special-category data for bias detection/mitigation in high-risk AI, with documentation, strong safeguards and deletion once the purpose is fulfilled. Require deployers to demonstrate that less intrusive measures (e.g., PETs, synthetic data) are inadequate before relying on special-category data.

5.3 Transparency to deployers on risk classification

Require providers to share documentation justifying why Annex III systems are—or are not—high-risk, and to update deployers when changes may alter the risk profile. This improves procurement certainty and liability allocation.

5.4 Retail use-case: loss prevention and staff safety

Clarify the boundary between legitimate, proportionate AI-supported loss-prevention measures in stores (to combat theft, fraud and threats to staff) and prohibited law-enforcement uses. Provide criteria to enable responsible deployment while protecting fundamental rights.

6. Data Act – Role Allocation and Legal Certainty

Clarify responsibilities in complex supply chains and coordinate supervision and sanctions to deliver predictable accountability where multiple actors contribute to connected products, services and data-sharing arrangements.

7. Cybersecurity – Harmonised Incident Reporting and Once-Only Compliance

Reporting obligations remain fragmented across multiple instruments. Swedish Commerce supports harmonised reporting: aligned definitions and thresholds, coherent timelines, a common EU portal (once-only principle), and clear guidance on minimum internal documentation—including language expectations that enable consistent group-wide documentation (often in English).

Retail-specific supervision sprawl: retailers frequently fall under several sectoral regimes simultaneously for the same core security management systems. Examples include payment card obligations (PCI DSS), medicines and healthcare distribution, food supply chains, chemical

products, energy generation (e.g., rooftop solar), finance/insurance services, general GDPR security duties, and forthcoming product security under the Cyber Resilience Act. This multiplicity translates into overlapping audits by different authorities and assessors, diverting resources from real risk mitigation.

Ask: coordinate supervision across sectors, recognise cross-regime equivalence of controls, and implement once-only audit/incident reporting wherever possible.

8. Standardisation and Technical Coordination

Accelerate open, industry-driven standardisation. Use common specifications to complement—not replace—standards. Where machine-readable consent signals are envisaged (Article 88b), ensure open, interoperable standards with practical implementation guidance to avoid divergent interpretations and gatekeeper-driven solutions.

9. Recommendations to the European Commission

1. Clarify the definition of personal data and practical implications for pseudonymised data sharing and related obligations.
2. Strengthen processor duties and clarify joint controllership where standardised providers determine practical means or influence purposes.
3. Modernise terminal-equipment rules (Article 88a) with explicit low-risk exemptions for functionality, security, performance and aggregated service-improvement analytics.
4. Design Article 88b to be competition-neutral, avoiding double-layer consent and preventing gatekeeper dominance; align obligations with standards availability.
5. Establish objective criteria for “substantial modification” in the AI Act; require providers to share risk-classification documentation with deployers.
6. Enable responsible retail loss-prevention AI with clear boundaries that protect fundamental rights.
7. Harmonise cybersecurity reporting and supervision using once-only portals and cross-regime control equivalence; address retail’s multi-sector exposure explicitly.
8. Ensure genuine simplification—avoid new administrative burdens through overly prescriptive templates and duplicative assessments.

The Digital Omnibus is a key instrument for creating a simpler, more competitive, and more functional digital single market. For the retail sector, it is vital that the regulatory framework is clear, risk-based, and coordinated.

Swedish Commerce remains committed to contributing constructively to the continued legislative process.