Ecommerce Europe Position Paper on the Digital Omnibus

Overall, Ecommerce Europe is broadly supportive of the proposed EU Digital Omnibus package, as it is expected to deliver meaningful regulatory simplification and operational efficiencies across the GDPR, AI Act, and NIS2/DORA frameworks. However, efforts to simplify the EU data legislative framework must be coherent and workable in practice. Certain aspects of the proposed Regulation raise serious concerns, especially the proposed Articles 88a and 88b GDPR. While we welcome coherence and disentanglement between the GDPR and the ePrivacy Directive, the actual effect of these proposals would be detrimental on the e-commerce sector. In that regard, we would have appreciated for the public consultation process to take place before the publication of the legislative proposal by the European Commission.

Table of Contents

1. Article 88b GDPR

Mandating browsers to introduce automated, machine-readable consent mechanisms under the proposed Article 88b GDPR acts as a gateway to damaging centralised cookie management systems. Such systems have previously failed to gain agreement during ePrivacy Regulation negotiations and met widespread disapproval during the “Cookie-Pledge Initiative”. Ecommerce Europe continues to believe that these measures should be avoided and urges the Commission to carefully consider the industry’s consistent and longstanding feedback.

We fear that centralised cookie management systems would concentrate powers, undermine the competitiveness of digital companies, create new security risks, ultimately running contrary to the core objectives of enhancing Europe's competitiveness and innovation. We also oppose the mandatory binding nature of broad browser signals (e.g., "Reject All") without safeguards for service-specific context, as well as the fixed period of six months during which no new request for the same purpose may be made following a refusal of consent.

This proposal introduces fundamental changes to the ecosystem, with far-reaching consequences for the wider digital economy, yet it is being advanced without a comprehensive impact assessment. The

underlying technology remains unproven, and there is insufficient evidence to demonstrate that it could genuinely simplify compliance or deliver better outcomes for users. **Ecommerce Europe calls on the Commission to carry out a proper impact assessment to carefully evaluate all the legal, technical and economic implications of this proposal.**

Ecommerce Europe Recommendations on Article 88b GDPR: we strongly oppose Article 88b and request a proper impact assessment given the complexity of the issue and the resulting contradictory economic and technical consequences. Article 88b of the new GDPR should not be part of a simplification law.

- ### No proven consumer benefits

We fear that browser-level consent may actually complexify the user experience rather than simplifying it by resulting in a less convenient and intuitive experience that leads to significant consumer confusion. Centralised consent management system will also diminish users' level of control over their consent as it leaves little to no room for differentiation. In practice, user choices about their privacy are highly context-specific. Users make distinct decisions for each website and app based on the content or service, differentiating between large or unknown companies and local or smaller companies, with a certain goodwill factor playing an important role. How differentiation can be applied in practice under such a regime remains unclear. Centralised cookie management systems will also directly undermine the personalised experience that customers expect as a core feature of their online experience. Indeed, recent evidence[1] showed that 85% of consumers expect personalised experiences and that 80% consider the experience provided by a company to be as important as its products or services.

- ### A threat to e-commerce businesses

Centralised cookie management systems will prevent e-commerce companies from engaging directly with their customers to obtain consent or apply other legal bases. It is of paramount importance that EU law safeguards this direct relationship: this direct link is fundamental to businesses' ability to operate effectively, innovate competitively, and sustainably finance the development and delivery of their products and services.

There is a risk that Article 88b leads to a situation where consumers treat all services in the same way choosing to reject data sharing with blanket choices, driving systematic cookie rejection and leading to reduced flexibility in marketing, especially where users broadly opt for strict default settings. This will have a detrimental impact on advertising revenues, analytics and webshop optimisation. It will disproportionately disadvantage SMEs versus larger incumbents with extensive first-party data. Moreover, implementing machine readable signals will entail additional technological complexity and substantial costs, particularly during the transitional period, with a disproportionate impact on SMEs.

[1] Fevad, Les chiffres: Bienvenue dans l'ère de l'ultra-personlisation de l'expérience client – link

- ### A threat to European competitiveness

Introducing centralised cookie management systems will effectively create new intermediaries (the browser/central system) between a publisher and their audience. These systems will therefore concentrate power in the hands of access controllers, undermining the competitiveness of European businesses and running counter to the fundamental objective of increasing European competitiveness and innovation. As a result, existing gatekeepers, who often control the relevant browsers/operating systems, will be reinforced and will continue to obtain consent on a large scale. They will also gain control over how options are presented and which choices are switched on or off by default. These browser vendors are often competitors in the ad-tech space, and will be in a position to impose “Privacy by Default" settings that cut off the economic lifeline of free or personalised services, without reflecting the user's specific intent for the website they are visiting. Consequently, e-commerce companies will become totally dependent on external technical standards and settings, putting them at a structural and competitive disadvantage and undoing progress made by the Digital Markets Act (DMA).

- ### Additional remarks

Article 88b also raises concerns as to how the requirements would interplay with specific existing consent requirements, including those that are not intended to be amended by the Omnibus (*e.g.*, “consent” requirements under the GDPR, as well as the DMA). It would sanctify consent as the only basis to access personal data, freezing the status quo, despite the European framework offering multiple legal bases and exceptions. Consolidating consent state and identifiers into a central repository would also create a high-value target and single point of vulnerability/failure for cyber-attacks across all dependent services.

Moreover, there are significant legal uncertainties concerning the validity (from the GDPR perspective) of consent provided via centralised manner. In practice, Article 88b would not comply with the GDPR consent standard, which requires the consent to be freely given, specific and informed. Replacing individual consents with centralised signals would undermine the requirement that consent must be purpose-specific. As a result, Article 88b would make it very easy for users to provide an opt-out but more difficult and legally questionable to opt-in.

2. Article 88a GDPR

The integration of ePrivacy rules into the GDPR is a welcome step towards a One-Stop-Shop, but the proposed execution falls short of the needs of a modern digital commerce. The underlying concepts date back more than 20 years which overlooks the profound transformation of the digital ecosystem. A framework designed over two decades ago cannot adequately address current digital complexities. **Ecommerce Europe highly encourages policymakers to move beyond the rigid models of the past and embrace a flexible, forward-looking approach that protects users while reflecting the realities of today’s e-commerce and fostering innovation.**

Ecommerce Europe Recommendations on Article 88a GDPR: We call for full alignment of Article 5(3) ePrivacy Directive with the GDPR’s legal basis, in line with the Commission’s Data Union Strategy, and urge a broader, more practical set of exemptions that reflect the realities of e-commerce. In particular, we recommend exempting recognised Privacy-Enhancing Technologies

(PETs) from consent requirements and removing the rigid six-month consent renewal rule, ensuring a clearer, more workable framework for both businesses and users.

- ## Aligning ePrivacy with Article 6 GDPR legal bases

We would first like to request clarifications regarding the gap between the Digital Omnibus proposal and the Data Union Strategy set by the European Commission which clearly states that: "*The Omnibus will reform the rules on cookies currently in the ePrivacy Directive and bring them into the GDPR framework. It will propose practical solutions: cookies and similar technologies for certain low-risk purposes should be considered lawful,* ***while other purposes, the operators should rely on one of the legal bases under the GDPR.***"[2] This is contrary to what is proposed in Article 88a(1) GDPR which continues to rely on the binary 'consent vs. strict necessity' framework introduced in 2002, without reflecting how significantly the digital environment has evolved since then.

Ecommerce Europe has long campaigned[3] for a shift away from a consent-only approach for cookies/terminal-equipment access, towards a risk-based model aligned with the six legal bases of the GDPR. Bringing Article 5(3) of the ePrivacy Directive in line with the GDPR would make it possible to apply the GDPR's risk-based approach to cookies and similar tracking technologies, rather than relying exclusively on consent. Depending on the level of risk, the use of cookies or other tracking tools could be justified on the basis of legitimate interest (Article 6(1)(f) GDPR), provided that appropriate safeguards are ensured.

While the Digital Omnibus' proposal fails to align Article 5(3) of the ePrivacy Directive with Article 6 GDPR, we are concerned that the introduction of Article 88a into the GDPR framework would nevertheless subject any infringements to the Regulation's general enforcement regime. This means that supervisory authorities will be able to impose the same sanctions for violations of Article 88a as for other GDPR infringements, with fines of up to 20 million euros or 4 percent of global annual turnover. This is stricter than under the ePrivacy framework and increases compliance risks, particularly for SMEs with limited legal and technical capacity.

- ## Future-proof consent exemptions

Ecommerce Europe finds the list of proposed exemptions to be too narrow with essential e-commerce operations such as fraud prevention (beyond mere technical security) and A/B Testing (essential for UX optimisation and product development) being currently excluded, forcing them into a consent regime that renders them ineffective.

We call for materially broader and workable low-risk exemptions for service security and fraud prevention, audience measurement, and functional personalisation. In that regard, we suggest extending the scope of Article 88a(3)(c) GDPR to allow the storage of or access to personal data on a natural person's terminal equipment not only for the preparation of aggregated but also non-aggregated information on the use of an internet service for the purpose of measuring the audience of such a service. This exemption should also explicitly over audience measurement performed via a service provider acting on behalf of the controller

[2] European Commission, Data Union Strategy, p.14 – link
[3] Ecommerce Europe, Position Paper on Online Advertising – link

(i.e., a processor), to avoid limiting the exemption de facto to first-party/in-house tools. In addition, we would be cautious to avoid hard-coded consent UX mandates (e.g., prescriptive one-click mechanics or fixed re-prompt prohibitions) that risk creating new compliance burdens and legal uncertainty for SMEs.

Importantly, the proposal fails to seize the opportunity to reward Privacy by Design. **In that regard, Ecommerce Europe advocates for fully exempting the use of recognised Privacy-Enhancing Technologies (PETs) (e.g., on-device processing, differential privacy) from the consent requirement**, as the risk to the user is effectively neutralised. Implementing this approach would create a clear incentive for the adoption of PETs. It would provide a future setup which increases both the protection of users and makes data and knowledge available for innovation. It offers a scalable solution to one of the most fundamental challenges of ePrivacy: consent first which overwhelms users, but does not protect them, while at the same time removing data and knowledge from society, thus crippling innovation. PETs can turn this around: protecting users while making knowledge available for innovation.

In addition, we fear that the broader formulation of Article 88a, which concerns access to terminal equipment in general, may result in new or innovative techniques being brought more quickly under the consent requirement. This may have implications for marketing, personalisation, fraud prevention and analytics, especially as long as further guidance and case law are still lacking. How supervisory authorities interpret the exceptions for strictly necessary or low risk processing, whether broadly or restrictively, will be crucial for practical implementation. In that respect, we call for clear and harmonised guidelines across the 27 Member States, as some national data protection authorities (DPAs) tend to have stricter interpretations than others.

- ### 6-month consent renewal period

Ecommerce Europe strongly opposes Article 88a(4)(c) GDPR which would prevent controllers from requesting consent again for the same purpose for at least six months after a refusal. This requirement would lead to more extensive processing of personal data, which would run counter to the GDPR's principle of data minimisation. Data controllers would have to find technical solutions to ensure that the request for consent is not submitted to the same data subject when they change their device, which in itself means the application of new additional traceability measures and, at the same time, more personal data processing.

3. Article 88c GDPR

Regarding Article 88c and data processing in the context of AI, we overall welcome the statutory recognition of AI training and operation as a legitimate interest. However, common reliance on legitimate interest is highly evaluative and may result in legal uncertainty. It is therefore essential to ensure that the rules governing the use of legitimate interest for AI development and training remain clear, coherent, and readily understandable for businesses. To achieve this, the framework must preclude national laws from bypassing the GDPR with separate consent requirements and broaden the balancing test to explicitly include the interests of third parties. Additionally, the principle of data minimisation is difficult to adhere to, given that AI development often requires extensive datasets, making it hard for companies to assess the minimum necessary amount of data.

The right to be forgotten (Art. 17 GDPR) is technically challenging to execute for AI models. While input data can be deleted, erasing data from the models themselves is technically complex, akin to deleting

specific data from backup systems. A pragmatic solution would be to adjust Article 17 GDPR to include an exception based on the disproportion between the actions required (e.g., full model erasure) and the effects/risks. Establishing these adjustments and a separate legal basis would provide much-needed clarity on proper legal grounds for AI data processing.

4. Other GDPR provisions

We welcome the efforts to frame GDPR adjustments as rebalancing compliance toward proportionality by reducing administrative burden where processing is low risk, and focusing regulatory scrutiny on genuinely high-risk processing (e.g., large-scale profiling, sensitive inference, high-impact automated decisions). We also welcome encouraging practical tools to address abusive/repetitive rights requests while maintaining accountability safeguards and legitimate user rights. Streamlining transparency obligations in clearly low-risk contexts, particularly where a prior relationship exists and user expectations are reasonable, is welcome, as long as transparency for higher-risk processing remains robust. Finally, we support harmonising definitions with other directives and regulations (Articles 4(b)(32)-(37)), as consistent terminology across the digital rulebook is key to reducing legal fragmentation and easing interpretation for cross-functional compliance teams.

- ### Data Protection Impact Assessment (DPIAs)

We welcome the centralisation of DPIA requirements via harmonised EU-wide lists established by the EDPB. This avoids fragmentation due to different national lists of processing activities for which a DPIA must be carried out and reduces the administrative burden for cross-border companies operating in several jurisdictions. We would however be cautious to avoid a maximalist ‘checklist’ approach that would pull routine low-risk commerce processing into DPIA-by-default. In that regards, a sensible transition approach would help prevent destabilising established processing absent material change. Lastly, we would also recommend allowing existing DPIAs to satisfy the AI Act's Fundamental Rights Impact Assessment (FRIA) requirements where the DPIA covers the relevant fundamental rights considerations, and delete the mandatory FRIA notification obligation.

- ### Data Subject Access Request (DSARs)

The Commission’s explicit clarification that a controller may refuse an access request or charge a reasonable fee where the request is manifestly unfounded or excessive is very helpful. It codifies existing case law and supervisory practice and provides controllers with greater legal certainty. In practice, we observe that the right of access has increasingly been used with a view to economic gain, and therefore for purposes other than the protection of personal data. Handling such requests entails significant direct costs, for example because organisations often choose to settle out of caution, as well as indirect costs due to the time and capacity required to process access requests.

- ### Clarification of personal data and identifiability

Ecommerce Europe highly welcomes the codification of the SRB case law. This risk-based definition aligns with modern data architectures and incentivises investments in advanced pseudonymisation techniques by clarifying that data is not "personal" to a controller if they lack the reasonable means to re-identify it. Not only does this clarification bring greater legal certainty and better reflect technological and economic reality,

it also offers concrete opportunities in the area of fraud prevention. In practice, e-commerce companies increasingly make use of hashed or pseudonymised datasets to identify fraud patterns, without being able to identify individuals themselves. Where e-commerce players do not have access to re identification means and cannot reasonably obtain them, consulting such datasets can contribute to effective and privacy friendly fraud prevention. We would however call for a definition of the scope of "*means reasonably likely to be used*" to prevent restrictive DPA interpretations concerning advanced re-identification.

- ## Implementing Acts on Pseudonymisation

We support empowering the Commission to define technical standards for pseudonymisation. It will provide legal certainty for data sharing and incentivise the deployment of PETs by establishing clear criteria for when data is no longer considered personal. However, limiting this mandate solely to 'pseudonymisation' restricts the regulation's future viability. We urge to expand the scope to allow for the standardisation of other technical measures, most notably 'recognised PETs' (e.g., Synthetic Data, Differential Privacy). Restricting the standardisation power creates a 'certainty gap' for advanced technologies that often offer superior privacy protection compared to traditional pseudonymisation. A broader mandate ensures that any technical measure effectively mitigating risk can benefit from the same legal recognition. This incentivises investment in 'Privacy by Design' and ensures the GDPR keeps pace with technological progress, particularly in AI development.

- ## Automated decision making

Ecommerce Europe welcomes the clarification that automated decision-making is permitted for contractual necessity, even if a human could theoretically perform the task. This reflects the reality of high-volume e-commerce where scalability renders manual processing impossible, ensuring legal certainty for standard automated processes.

However, the current and proposed provisions do not work for preventing AI-generated fraud in e-commerce. Even with the proposed amendments, the provisions of Article 22(1) GDPR will continue to impede the efficient deployment of anti-fraud tools that rely on automated decisions with legal or similarly significant effects, as the existing exemptions remain too narrow. Such tools are essential in the online business environment, where fraudsters are increasingly using AI to create synthetic identities and deepfakes at scale. This renders traditional ID verification (IDV) methods inadequate and causes problems of providing false or edited evidence (e.g. AI-generated images of falsely damaged goods) or documentation (e.g. AI-generated fake drop off receipts). Synthetic identity fraud has increased by 183% since 2019, with AI-generated personas now featuring consistent backstories and fabricated identities capable of bypassing conventional checks, including government-issued ID documents and database verifications. The use of fake (AI-generated) documentation and evidence becomes a standard practice in fraudulent activity, often organised and conducted at scale. With the rapid advancement of AI, this trend is expected to continue, to the detriment of European businesses and online retailers. The current requirement for human intervention introduces significant delays when facing threats that operate at machine speed. Given that AI-enabled attacks can adapt within minutes, the ability to deploy automated systems capable of real-time threat response is critical. Ecommerce Europe would therefore recommend to further amend Article 22 GDPR to include an exception to permit automated decision making for the purposes of fraud prevention.

- ## Special categories of personal data

Ecommerce Europe supports the introduction of a specific legal basis for processing special categories of data for bias detection and correction. This is a pragmatic enabler for developing fair and non-discriminatory AI systems (e.g., inclusive sizing recommendations) that was previously hindered by strict prohibitions. However, this amendment treats the symptom, not the root cause. The core issue remains the overly broad judicial interpretation of Article 9(1) GDPR, which increasingly classifies data as "special category" merely because sensitive details could be inferred from it (even indirectly).

This extensive interpretation dilutes the protective purpose of Article 9: if innocuous behavioural data is treated with the same severity as medical records, the prohibition loses its normative force. To ensure Article 9 is taken seriously and applied effectively again, the legislator must clarify the definition itself. We urge a restriction to data that manifestly and explicitly reveals sensitive attributes, excluding mere potential inferences from the definition.

- ## Definition of scientific research

We strongly support a definition of scientific research that explicitly encompasses technological development and commercial innovation. This clarification is key to incentivise R&D activities in the private sector. However, legal uncertainty remains regarding the cumulative requirement to contribute to “society's general knowledge”. It is unclear whether this implies for instance a mandatory publication of results, which would conflict with the protection of trade secrets for private entities or even commercial research within the private sector would be covered at all. We suggest clarifying, for instance in a recital, that the "societal contribution" can also be achieved through the application of research results (i.e., through innovative products or services that enhance consumer wellbeing or sustainability), without necessitating the public disclosure of the underlying proprietary data or methodologies.

Regarding purpose limitation (Article 5(1)(b)), we welcome the clarification that further processing for scientific research is compatible with the original purpose. This enables sustainable, long-term learning and innovation from knowledge enshrined in data (e.g., for historical trend analysis or model improvement) while maintaining strict ethical standards, without requiring repeated consent.

- ## Information obligations

We welcome the Commission’s amendments to the information obligations under Article 13 GDPR. Where a controller has reasonable grounds to believe that the data subject already has the required information, the obligation to provide that information again no longer applies, unless there is a transfer to third parties, a transfer to third countries, automated decision making or a high risk to the rights of data subjects. This is a welcomed clarification and helps combat "information fatigue" for the user and allows for a cleaner, more user-centric UX design by removing redundant legal notices.

- ## Duties of the EDPB

We welcome the enhanced role of the EDPB (Article 57, 64, 70) in ensuring consistent application of the regulation. Stronger centralised EU-wide guidance is preferable to the current fragmented interpretation by national and regional authorities, fostering a true Digital Single Market. However, it is important that such

guidance is always drafted openly and transparently, taking stallholders' feedback into consideration and safeguarding the GDPR's principle of proportionality.

5. One-Stop Shop for incident reporting

Ecommerce Europe strongly supports the single point of contact for incidents. We also support the shift to a "high risk" reporting threshold and the extension of the deadline to 96 hours (Article 33 GDPR). This change prioritises quality over speed, reducing 'defensive reporting' and allowing security teams to focus on forensic analysis and effective mitigation of genuine threats. It also reduces administrative overhead and provides more manageable deadline. We would nonetheless advocate for a breach notification regime that focuses reporting on incidents likely to cause real harm and allows sufficient time for assessment/containment, and avoid introducing additional EU-level reporting layers that may increase complexity for smaller organisations.