zalando

Digital Omnibus Regulation Proposal

Zalando contribution, January 2026

Zalando SE, Valeska-Gert-Straße 5, 10243 Berlin | eingetragen beim / registered with: Amtsgericht Charlottenburg, HRB 158855 B | USt-IdNr. / VAT registration number: DE 260543043 | Vorstand / Management Board: Robert Gentz & David Schröder (beide Co-Vorstandsvorsitzende / both co-Chairs of the Board), Dr. Astrid Arndt, Anna Dimitrova, David Schneider | Aufsichtsratsvorsitzender / Chairperson of the Supervisory Board: Kelly Bennett | Sitz / Registered Office: Berlin | WEEE-Reg.-Nr. DE /WEEE-Reg.-No GER: 72754189

Introduction

Zalando welcomes the European Commission's Digital Omnibus Package, particularly the proposed modernisation of the General Data Protection Regulation (GDPR), as a timely and necessary strategic step towards strengthening European competitiveness. We support the Commission's objective to reduce administrative burdens and further harmonise Europe's digital rulebook, acknowledging that the previous regulatory fragmentation has too often constrained innovation. The emphasis on a risk-based, relative definition of personal data, alongside clarified definitions for scientific research, represent vital "innovation enablers". If implemented effectively, these changes can provide the legal certainty required for European tech companies to invest in applied innovation, advanced data architectures, and AI models with confidence.

At the same time, "simplification" must be consistent and operationally viable. While we support the integration of ePrivacy rules into the GDPR (through a One-Stop-Shop), aspects of the current proposal risk introducing new rigidities that could threaten the user experience and the economic viability of digital platforms. Specifically, static time-limits on consent and the mandatory acceptance of broad browser signals ignore the nuanced reality of modern e-commerce. Moreover, we strongly oppose the introduction of mandatory, centralised browser-level consent signals. Embedding consent decisions at the infrastructure level would weaken the direct relationship between users and service providers, effectively creating new gatekeepers. Such mechanisms risk undermining genuine user choice and creating distortion of competition. Instead of relying on rigid prohibitions, the framework should incentivise "Privacy by Design" by explicitly rewarding the adoption of standardised and recognised Privacy-Enhancing Technologies (PETs).

The proposal also presents an opportunity to clarify the definition of special categories of personal data, addressing the root cause of legal uncertainty in this regard. Current extensive judicial interpretation, which risks classifying innocuous behavioral data as "sensitive" based on theoretical inferences, dilutes the protective purpose of Article 9. To truly unlock innovation, we urge for a clarification that prevents this "inference trap," balancing robust protection for genuinely sensitive data with the ability to provide meaningful, valuable and appreciated services to our customers.

Zalando sees significant potential in the Digital Omnibus and a clear step in the right direction. We support a robust framework that protects fundamental rights while enabling European digital companies to scale and compete globally. For Digital Omnibus to fully achieve this, we outline our key recommendations below.

Our key recommendations

I. Align ePrivacy with GDPR Framework and recognise the use of PETs (Article	**1) Align ePrivacy with Article 6 GDPR & eliminate parallel consent regimes:** To end the fragmentation between data protection and ePrivacy rules, we call for full alignment of ePrivacy with GDPR framework and shift beyond the outdated "consent vs. strict necessity" dichotomy, allowing the legal bases in Article 6 GDPR (specifically Legitimate Interest) to govern use of data in the

88a)	context of access to terminal equipment. **2) Ensure Legal Viability for Critical Use Cases**: Data processing for essential functions should be explicitly named and permitted as critical use cases, such as fraud prevention, audience measurement, and A/B testing (essential for UX optimization and product development) so that those are not forced into a consent regime that renders them ineffective. The current list of exceptions is too narrow and static, failing to reflect the operational realities of modern digital services. The proposal therefore prevents important knowledge required in a modern society to learn and turn knowledge and learning into innovation. **3) Incentivise the use of Privacy-Enhancing Technologies (PETs):** We propose that the use of Privacy-Enhancing Technologies (PETs) (e.g., on-device processing, differential privacy) should exempt controllers from the consent requirement, as the risk to the user is effectively neutralized. 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. The current proposal misses the chance to reward "Privacy by Design", PETs can change that.
II. Introduce Technical Standards for PETs to create a Future-Proof Legal Framework (Article 41a)	We strongly support the introduction of Implementing Acts for technical standards but urge the legislator to broaden the scope. The scope should extend beyond pseudonymisation to **include standards for Privacy-Enhancing Technologies (PETs)**. This would create a scalable, future-proof framework that provides legal certainty for advanced privacy tools without requiring constant legislative revision.
III. Ensure Legal Certainty for Special Categories of Personal Data (Article 9)	To unlock innovation, we need to eliminate legal ambiguity in core definitions. Therefore we call in **Art. 9** for a clear definition of what constitutes special categories of personal data to prevent the "inference trap": data should only be classified as "special category" if it **manifestly reveals** sensitive information or is **intentionally used to infer** them.

IV. Provide Clarity of the legal definition for Scientific Research (Articles 4)	The definition of "Scientific Research" must be free of undefined "ethical standards" (which belong in compliance obligations) to avoid a "definition trap". Additionally, it should explicitly include "applied research" and clarify that "societal contribution" can equally be achieved through **market-facing innovations** (products and services) as well as through rather than a mandatory publication of data.
V. Protect Fair Competition and genuine User Choice (Article 88b)	**Stop mandatory, centralised browser-level consent mechanisms from becoming new gatekeepers** We ask for removal of the proposed centralised browser level consent. Mandatory browser-level consent mechanisms should not become the default or exclusive compliance model under Article 88b, as they: ● Reduce genuine user choice by replacing service-specific decisions with one-size-fits-all settings; ● Distort competition by embedding compliance decisions at the infrastructure level, rather than allowing diverse business models to compete on equal terms; ● Entrench dominant players, undermining a fair competition.
VI. Prevent Security Loopholes in AI Regulation (Article 88c)	We ask for the **removal of the proposed unconditional right to object** to data processing in AI systems. By allowing a blanket opt-out, Article 88c inadvertently empowers malicious actors to evade essential fraud detection and security monitoring tools. Instead of creating new risks, the regulation should rely on the proven, proportionate framework of **Art. 21 GDPR**, which balances individual rights with the necessity of maintaining secure and resilient platforms.

I. Align ePrivacy with GDPR Framework

Modernise Data processing in the terminal equipment (Art. 88a)
While the integration of ePrivacy rules into the GDPR is a welcome step towards a One-Stop-Shop, the current proposal falls short of the needs of a modern, digital-first society. The underlying concepts date back more than two decades, and the digital world has changed fundamentally since then. Carrying ePrivacy forward "as-is" would not reflect two decades of regulatory and technical developments, nor ensure a future-proof legislative framework.

Our recommendations:

1) Align ePrivacy with Article 6 GDPR & eliminate parallel consent regimes
The current proposal largely reflects the historic "consent vs. strict necessity" approach established in 2002, rather than fully building on the regulatory and technical developments that have shaped the GDPR over the past two decades.

As a result, it introduces an unintended dual regime by differentiating between personal and non-personal data stored on terminal equipment. In practice, this means that non-personal data becomes a subject to more restricted, fragmented legacy ePrivacy rules (offering fewer exceptions), while personal data benefits from the broader flexibilities and One-Stop-Shop mechanisms under the GDPR. This incoherence risks creating legal uncertainty and inefficiency, including the tendency to treat low-risk data as personal solely to benefit from clearer governance, while increasing consent prompts and user fatigue through double cookie banners. A full alignment of the ePrivacy with the GDPR framework would help address these challenges. Applying the legal bases set out in Article 6 GDPR to all data accessed on terminal equipment, regardless of its classification, would not only enhance coherence and legal certainty but also support a proportionate, risk-based approach that is consistent with the objectives of both legal instruments.

2) Ensure Legal Viability for Critical Use Cases (fraud prevention, analytics)

As digital services continue to evolve, it is important that the regulatory framework adequately reflects current operational needs and remains adaptable over time. While the proposal introduces helpful clarifications, the list of exceptions is too narrow and static; it does not reflect well the current needs of a digital environment and more importantly, it is not future proof. Functions such as Fraud Prevention (beyond mere technical security) and A/B Testing (essential for UX optimisation and product development), which play a key role in improving user experience, products and safety are currently subject to disproportionate barriers. This limits the ability of companies to generate insights that support service quality, security, and innovation, to the detriment of both businesses and users. From an implementing perspective, further clarification is much needed regarding analytical data processing activities carried out by processors on behalf of the controller, as this reflects standard and well-established industry practice. Likewise, the requirement that certain security-related processing be "requested by the user" could be reconsidered, given that effective fraud detection and security measures often need to operate independently of user action, particularly in the context of malicious behaviour. The current proposal therefore prevents important knowledge required in a modern society to learn and turn knowledge and learning into innovation. Furthermore, in practical terms, the proposed obligation to respect a user's refusal for a period of six months raises questions about technical feasibility. Controllers may not always be able to reliably link a refusal across multiple devices, distinguish between different users on a shared device, or recognise returning users after identifiers have been deleted or reset.

3) Incentivise the use of Privacy-Enhancing Technologies (PETs)

A further opportunity lies in more actively promoting "Privacy by Design" within the regulatory framework. The use of recognised Privacy-Enhancing Technologies (PETs), such as on-device processing or differential privacy, can significantly reduce or neutralise risks for users and therefore merits positive recognition. Creating clear incentives for the adoption of such technologies would strengthen privacy protection while allowing responsible data use to support innovation. From a systemic perspective, encouraging PETs offers a scalable response to one of the long-standing challenges in ePrivacy: an over-reliance on consent mechanisms that can overwhelm users without necessarily delivering meaningful

protection. By contrast, PETs embed safeguards directly into processing operations, protecting individuals while preserving access to data and insights that are essential for learning, service improvement, and innovation. To make this approach operational and future-proof, the regulation should empower the Commission to define the technical criteria for "recognised PETs" through Implementing Acts. Mirroring the governance structure of Article 41a would allow new and emerging technologies to be recognised as state of the art over time, without requiring repeated revisions of primary legislation. This would help shift the framework from a purely compliance-driven model toward one that actively rewards higher privacy standards and technological progress.

More broadly, there is widespread agreement that simply carrying forward regulatory concepts developed more than two decades ago risks overlooking the profound evolution of the digital ecosystem. While views may differ on the role of consent, there is a shared interest in ensuring that the framework remains dynamic, risk-based, and capable of balancing strong user protection with the practical realities of modern, innovation-driven services.

II. Introduce Technical Standards for PETs to create a Future-Proof Legal Framework

Broaden the scope of Art. 41 (a) to include standards for Privacy Enhancing Technology (PET's)

Building on the goal of harmonisation and legal certainty, Zalando strongly welcomes the introduction of Article 41a and the empowerment of the Commission to define technical standards via Delegated Acts. This mechanism represents an important step toward a more coherent and future-oriented framework, offering clarity for data sharing and supporting the deployment of privacy-preserving solutions. At the same time, we would encourage consideration of a broader scope for this standard-setting mandate. Limiting technical standards solely to pseudonymisation risks constraining the framework's long-term effectiveness, particularly given the rapid evolution of privacy-enhancing technologies. Expanding the scope to include recognised Privacy-Enhancing Technologies (PETs), such as synthetic data or differential privacy, would help ensure that advanced technical measures that effectively mitigate risks can benefit from comparable legal recognition. A broader approach would close existing certainty gaps for technologies that may offer stronger privacy protections than traditional techniques, while incentivising investment in Privacy by Design. It would also allow the regulatory framework to remain responsive to technological progress, particularly in areas such as AI by enabling standards to evolve over time without requiring repeated legislative intervention.

III. Ensure Legal Certainty for Special Categories of Personal Data

Provide a clear definition of what constitutes Special Categories of Personal Data in Art. 9 GDPR.

To complement future-proof legal framework, we welcome the introduction of a specific legal basis for processing special categories of data in the context of the development and operation of AI systems. 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 targeted amendment does not

fully address the underlying challenge. The core hurdle remains; the overly broad judicial interpretation of Article 9 (1), which increasingly classifies data as "special category" merely because sensitive details could be inferred from it, even if the controller has no intention of doing so. This extensive interpretation dilutes the protective purpose of Article 9: if innocuous behavioral data is treated with the same severity as medical records, the prohibition loses its normative force, thereby weakening the protective purpose of Article 9 itself.

To restore clarity and ensure effective application, we would therefore encourage a clarification of the definition itself. In particular, data should fall under the strict regime of Article 9 only where it manifestly and explicitly reveals sensitive attributes, or where it is intentionally used to infer such attributes. This would reinforce the risk-based logic of the GDPR while preserving robust protection for genuinely sensitive data.

IV. Provide Clarity of the legal definition for Scientific Research

Introduce clear and workable definition of “Scientific Research” (Art. 4 (38))

Alongside special personal data categories, clear and workable definition of scientific research is essential to support innovation. Therefore, Zalando welcomes the EU Commission’s objective to harmonise the definition of scientific research and explicitly link it to innovation. However, to effectively incentivise private sector investment in research and development (R&D), the current drafting requires adjustments to avoid unintended legal risks.

Our recommendations:

- **Separate Definitions from Compliance:** We recommend maintaining a clear separation between definitions and compliance obligations. While adherence to ethical standards is fundamental, embedding undefined ethical concepts directly into the definition risks creating legal ambiguity. Disputes over interpretation could retrospectively call into question the legal basis for processing, undermining predictability. For this reason, the definition should remain objective and descriptive, with ethical compliance addressed through dedicated governance and accountability mechanisms.

- **Recognise Applied Research as Societal Contribution**: The definition should explicitly include "applied research" and "privately funded research" to reflect the reality of industrial innovation. Crucially, the requirement for "societal contribution" should be understood to encompass the practical application of research outcomes, including innovations such as safer, more sustainable products or enhanced consumer experiences and deliver direct benefits to society and "consumer wellbeing." This approach supports the full innovation lifecycle while robustly protecting trade secrets and commercially sensitive know-how.

Provide clarity on Purpose Limitation (Art. 5)

In addition, we also welcome the clarification that further processing for scientific research is compatible with the original purpose (Art. 5). This provides an important foundation for long-term learning and innovation, enabling responsible reuse of data for activities such as historical trend analysis while maintaining strict ethical standards, without requiring repeated permission.

V. Protect Fair Competition and genuine User Choice

Automated and machine-readable indications (Art. 88b)

Equally important is the preservation of fair competition and meaningful user choice to have a future-proof and robust legal framework. While we support user-friendly mechanisms that enhance transparency and control, the proposed approach to automated browser signals raises important practical and structural considerations. We oppose the mandatory binding nature of broad browser signals (e.g., "Reject All") without safeguards for service-specific context.

Our recommendation is:

- **Stop mandatory, centralised browser-level consent mechanisms from becoming new gatekeepers:** Mandatory browser-level consent mechanisms should not become the default or sole compliance model under Article 88b, as they risk replacing service-specific choices with one-size-fits-all settings, concentrating power in the hands of a few dominant players, and distorting competition, ultimately undermining both genuine user choice and a competitive, open digital ecosystem.

VI. Prevent Security Loopholes in AI Regulation

Data processing in the context of AI (Art. 88c)

The statutory recognition of AI training and operation as a legitimate interest represents an important and welcome step forward. It provides much-needed legal clarity for the development and deployment of AI systems in Europe, helping to address long-standing uncertainties around the appropriate legal basis for model training and operation.

At the same time, careful consideration is warranted regarding the proposed introduction of an unconditional right to object. While the protection of individual rights is essential, an absolute opt-out risks unintentionally weakening the effectiveness of AI systems that play a critical role in areas such as fraud prevention, abuse detection, security monitoring, and overall operational resilience. Unlike the established and balanced approach under Article 21 GDPR, an unconditional right to object could limit the ability of controllers to address misuse and malicious behaviour, potentially increasing risks for users and platforms alike.

To safeguard both individual rights and user safety, we therefore encourage retaining the well-established proportional framework of Article 21 GDPR. This approach preserves a meaningful right to object, while ensuring that essential security-related processing can continue to function effectively and responsibly.

******

Core Provisions to Preserve in the EU Digital Omnibus

Zalando welcomes several elements of the EU Digital Omnibus that enhance legal certainty, streamline operational processes, and support a user-centric digital ecosystem. In particular, the package introduces pragmatic improvements to information transparency and data subject rights, strengthens enforcement mechanisms, and promotes consistent governance across the EU. These developments collectively reduce administrative burdens, improve operational feasibility, and provide clearer guidance for companies while safeguarding fundamental rights.

I. Zalando welcomes proposed practical Clarity and Operational Legal Certainty for Data Processing

Definition of Personal Data (Art. 4 (a))

We welcome the codification of the "relative" approach to personal data, reflecting the standing CJEU jurisprudence, e.g. the latest SRB decision (C-413/23 P). This ensures alignment with modern data architecture and provides legal certainty for investments in advanced pseudonymisation techniques. This risk-based definition clarifies that data is not "personal" to a controller if they lack the reasonable means to re-identify it. In addition, we support the harmonization of definitions with other legislative acts. A coherent terminology across the digital rulebook is essential to reduce legal fragmentation and interpretation costs for cross-functional compliance teams.

Modalities for data subject rights (Art. 12)

A more balanced approach to manifestly unfounded or excessive requests is a welcomed new development. We welcome the strengthened ability of controllers to reject or charge for manifestly unfounded or excessive requests, particularly where the right is abused for non-privacy purposes. This introduces a necessary balancing of fundamental rights with the increasing exploitation of data subject rights (e.g., in litigation contexts), allowing resources to be focused on genuine privacy inquiries.

Information Obligations (Art. 13)

Reducing information duties where data processing is self-evident or within a "clear and circumscribed" relationship is a pragmatic improvement. This helps solve "information fatigue" for the user and allows for a cleaner, more user-centric experience and design by removing redundant legal notices.

Automated decision making (Art. 22)

Clarifying that automated decision-making is permitted for contractual necessity, even if a human could theoretically perform the task, reflects operational reality and is a very much welcomed development. For high-volume e-commerce where scalability renders manual processing impossible, this clarification provides and ensures essential legal certainty for standard automated processes.

II. We support streamlined Enforcement and Consistent Governance

Notification of personal data breach (Art. 33)

The move to a *high-risk* reporting threshold, combined with an extended 96-hour deadline, is a necessary, proportionate reform and strongly supported by Zalando. For the following reasons:

- **Capacity of Authorities:** Data Protection Authorities are currently overwhelmed by the sheer volume of low-risk notifications. Raising the threshold is essential to allow authorities to focus their limited resources on the investigation and remediation of serious data breaches that actually threaten fundamental rights.
- **Quality of Reporting:** The extension of the deadline is equally crucial. This results in more accurate, meaningful, and actionable notifications, rather than rushed submissions designed solely to meet procedural deadlines. A 96-hour window allows security teams to conduct proper forensic analysis, resulting in more accurate and actionable notifications.

However, a single incident often triggers parallel reporting obligations under different legal instruments such as GDPR, the Network and Information Security Directive (NIS 2.0), the Cyber Resilience Act (CRA), or financial regulations (such as the Digital Operational Resilience Act (DORA)), each with conflicting timelines. Notification requirements must be consistent across these regimes. We recommend therefore to align the GDPR deadline as it is crucial to prevent fragmented compliance and ensure resources remain focused on incident resolution rather than navigating mismatched administrative hurdles.

Data protection Impact Assessment (Art. 35)

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.

Duties of the Board (Art. 57, 64, 70)

Another step in the right direction is strengthening the European Data Protections Board's (EDPB's) role in ensuring consistent application of the Regulation. More centralised guidance reduces divergent national practices and supports a genuinely harmonised data protection framework across the EU

Conclusion

Zalando welcomes the modernisation of the GDPR within the Digital Omnibus Package as an important step toward strengthening the Digital Single Market. Efforts to harmonise the digital rulebook, enhance consistency through a stronger role for the EDPB, and further embed a risk-based approach to personal data reflect the growing maturity of the EU's digital regulatory framework. Together, these elements reinforce legal certainty, which remains a key enabler of responsible innovation. At the same time, fully delivering on this ambition will depend on ensuring that the framework aligns closely with technical and operational realities. Simplification should not be understood as the

preservation of concepts developed for a very different digital environment, but rather as an opportunity to modernise rules in a way that remains effective in practice. The long-term success of the package will therefore rest on its ability to function smoothly on the ground, including safeguarding essential security measures, avoiding unnecessary consent fatigue for users, and ensuring that regulatory design does not inadvertently concentrate influence in the hands of a small number of technical intermediaries.

With targeted refinements, in particular through a pragmatic approach to ePrivacy and a clearer role for Privacy-Enhancing Technologies, the EU can further strengthen a framework that both protects fundamental rights and supports a competitive, innovative digital economy. Zalando stands ready to engage constructively with policymakers and stakeholders to help shape a regulatory environment that is robust today and resilient enough to support the innovations of tomorrow.

******

About Zalando

Founded in Berlin in 2008, Zalando is Europe's leading online multi-brand fashion destination. We are building a pan-European ecosystem for fashion and lifestyle e-commerce, along two growth vectors: Business-to-Consumer (B2C) and Business-to-Business (B2B). In B2C, our two brands Zalando and ABOUT YOU, provide an inspiring, high-quality multi-brand shopping experience for fashion and lifestyle products reaching more than 61 million active customers across 29 markets. In B2B, we offer a unique e-commerce operating system with ZEOS, Tradebyte and SCAYLE, leveraging our logistics infrastructure, software, and service capabilities to support brands and retailers in managing and scaling their entire e-commerce business, across Europe.

For further information, please visit: corporate.zalando.com/en