zalando

EDPB Consultation on the Draft Recommendations 2/2025

Zalando Contribution, February 2026

Introduction

Zalando SE ("Zalando") welcomes the opportunity to provide feedback to the European Data Protection Board (EDPB) on the draft Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites. We fully support a strong and consistent application of EU data protection law and share a foundational commitment to ensuring the highest level of protection for European customers' personal data.

At the same time, we are concerned that the current draft Recommendations risk exceeding the intended scope of the General Data Protection Regulation (GDPR) by promoting a mandatory "guest account" model. In substance, this approach moves toward an "Isolated Transaction Account" framework that may fundamentally alter integrated digital service models. The issue therefore extends beyond procedural checkout options; it raises broader constitutional and legal questions concerning entrepreneurial freedom, contractual autonomy, and the proper limits of data protection regulation. It is also not taken into account that user accounts are not optional features; they constitute essential infrastructure for contract performance, security, customer support, regulatory compliance, and overall user experience. Guest accounts should therefore remain a voluntary design choice, and not become a mandatory requirement.

By prioritizing a model that restricts the legitimate acquisition and lawful processing of data, the Recommendations risk departing from the GDPR's fundamental principles, creating unnecessary friction for digital-first consumers and a less adaptive regulatory environment. We encourage the EDPB to ensure that the draft Recommendations remain aligned with the GDPR's balanced structure, which enables the free flow of data while guaranteeing a high level of protection for individuals.

Operational and Security Implications of Isolated Transaction Accounts

The Recommendations are highly relevant to the digital economy, as they effectively establish a presumption in favor of guest mode while applying a strict interpretation of the necessity requirement under Article 6 GDPR as well as the concept of data minimisation. This presumption risks undermining lawful, consumer-friendly business models without adequately reflecting operational complexity, protective functions, or providing a comprehensive impact assessment or empirical evidence.

The push for mandatory isolated transaction accounts would have significant operational and security consequences. Modern digital platforms, online retailers, operate as sophisticated ecosystems, managing secure payments, customer service, and returns across various different brand partners and customers, with warranties and product safety requirements often extending over several years. In this environment, persistent user accounts serve essential security and integrity functions:

- **Enhanced Security:** Prevent account takeover and fraud. Treating every transaction as first-time interaction increases exposure to bot attacks, transaction fraud, and identity misuse.
- **Operational Efficiency:** Supports verification of returns, refunds, and post-contractual obligations.
- **Regulatory Compliance:** Enables platforms to meet mandatory EU security obligations under Article 32 GDPR.

Isolated transactions would also make it more difficult or even nearly impossible to verify returns from brand partners, ensure refunds are correctly processed, and maintain safeguards against fraud or identity misuse. Such limitations may reduce the reliability of consumer protection mechanisms and complicate the efficient handling of post-contractual obligations.

Primary GDPR Objective and Limits

The GDPR's primary objective is to facilitate the free flow of data within a framework that ensures a high level of protection for individuals' personal data. Under Article 16 of the Charter of Fundamental Rights of the European Union (CFR), companies enjoy the freedom to conduct a business, including the autonomy to define the nature and scope of their services and contractual structures. The GDPR establishes conditions for HOW data processing, but it does not authorize authorities to determine or impose the fundamental design of business models. Furthermore, the Court of Justice of the European Union (CJEU) has clarified in SAS Institute Inc. v. Wyeth (C-634/17) that the GDPR does not regulate economic activities as such, nor does it determine the business models undertakings may adopt. This jurisprudence confirms that data protection law governs processing within a chosen model, not the structural design of that model. Moreover, Article 5(1)(c) GDPR (data minimization) applies to processing in relation to defined purposes; it does not restrict the controller's discretion to determine legitimate purposes under Article 5(1)(b) GDPR.

Additionally, EDPB fails to identify any provision in the GDPR or related EU law that would compel marketplaces or traders to offer guest accounts. As aforementioned the GDPR establishes conditions for lawful processing of personal data but does not mandate specific business models or service designs. The attempt to derive such a mandate from principles like "data protection by default" (Article 25(2) GDPR) represents a legal overreach: Article 25(2) GDPR requires controllers to implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This principle applies to settings within a chosen service model, not to the fundamental design of the service itself.

Furthermore, EDPB's emphasis on "voluntariness" of consent is misplaced in this context, as any platform does not rely on consent (Article 6(1)(a) GDPR) as the legal basis for account creation. Instead, the processing is justified under Article 6(1)(b) GDPR as necessary for the performance of the Platform Usage Agreement. The

European Data Protection Supervisor (EDPS) has explicitly advised against using consent for contractually necessary data processing: "When a controller wishes to process personal data that are actually necessary for the performance of a contract, consent is not the appropriate legal basis." (EDPS Guidelines, para. 19)

National jurisprudence reinforces this interpretation. The Higher Regional Court (OLG) of Hamburg (Case No. 5 U 30/24) affirmed that the operational complexity of a digital ecosystem justifies mandatory registration in order to ensure efficient coordination of customer service and returns. The court recognized that the platform's legitimate interests in managing complex multi-party relationships may outweigh the comparatively limited interference associated with account creation.

Authenticated identity is therefore not a structural excess but a legally supportable and proportionate component of complex marketplace operations.

Regulatory Compliance and Consumer Protection

An overly narrow view on data minimization may overlook the significant impacts on the very users it seeks to protect. A data-restricted or guest-only environment can create substantial security gaps. Persistent user accounts are essential for detecting bot attacks, preventing transaction fraud, and ensuring secure interactions. They also enable traceability under, for example, the German Product Safety Act (ProdSG), which is critical for product recalls, warranty management, and consumer protection. Without an authenticated transaction history, platforms are unable to reliably protect consumers if products are later found to be defective.

From an operational perspective, de-contextualized guest transactions represent both a functional limitation and a regulatory risk. As a Very Large Online Platform (VLOP) under the Digital Services Act (DSA), Zalando must ensure platform safety, perform Systemic Risk Assessments, and implement effective mitigation measures against financial fraud and illegal content. Without persistent account data, platforms may be forced to rely on more intrusive friction in real time or external credit agencies, which can increase the overall volume of data processed for consumers rather than reducing it.

In contrast, the registered-only model actively promotes data protection and regulatory compliance. Persistent authentication enhances security, reduces account takeover risk, and provides the most efficient mechanism for exercising data subject rights under Articles 15–22 GDPR, as recognized by the Datenschutzkonferenz "The most data protection-friendly approach is considered to be remote access by the data subject to their own data, provided by the controller". Registered accounts also reduce redundant data processing, avoiding repeated identity verification for customer service or payment checks required under a guest-only model.

Beyond GDPR compliance, registered accounts facilitate adherence to additional regulatory obligations. These include anti-money laundering requirements under the Anti-Money Laundering Act (AML) where platforms like Zalando must maintain

continuous monitoring of business relationships (§ 10 Abs. 1 Nr. 5 GWG), which requires persistent customer identification, product traceability obligations under the ProdSG, and long-term retention for tax and accounting purposes. By enabling centralised management, the registered-only model strengthens operational efficiency, ensures compliance, and enhances the protection of users' personal data, demonstrating that persistent accounts can be both privacy-friendly and legally necessary.

Conclusion

Zalando fully supports a strong and effective regulatory framework; a framework that is effective, proportionate and fit for a modern Digital Europe. The current proposed Recommendations, by favoring an Isolated Transaction model, inadvertently undermine the protection, security, and experience of the European consumer. They appear to reflect an approach that confuses data minimization with data absence, whereas today's digital environment is considerably more nuanced and requires equally nuanced and carefully calibrated guidance.

We therefore recommend the following:

- **Respect entrepreneurial freedom under Article 16 CFR**, recognizing that service design falls within the constitutional autonomy of undertakings.
- **Ensure alignment with established case law**, including the jurisprudence of the CJEU and the decision of the OLG Hamburg, which clarify the limits of data protection regulation and recognize the operational realities of marketplace models.
- **Acknowledge the balanced structure and primary objective of the GDPR**, including Articles 6(1)(b) and 6(1)(f) GDPR, as legitimate legal bases for account-based service models.
- **Apply data protection principles to processing activities within a chosen service model**, rather than interpreting them as a basis for mandating alternative structural or business models.

We ask for the opportunity to continue protecting and serving our customers in a way that reflects their actual needs and the high standards of European data protection and innovation. High-level data protection and a competitive, innovative digital economy are mutually reinforcing. Achieving both requires guidance that is balanced, proportionate, and reflective of real-world digital services and business models.

******

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