Public Consultation: R02/2025

Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites

The EDPB Recommendations 2/2025 offer an important clarification on the limits of mandatory user account creation in e-commerce and rightly emphasise the principles of necessity, data minimisation, and data protection by default. The strong conclusion that mandatory accounts are lawful only in very limited circumstances, such as genuine subscription services or restricted communities, represents a significant step toward curbing excessive data collection practices. The promotion of guest checkout as the default and most privacy-protective option is particularly welcome.

However, certain aspects may benefit from a more nuanced, operationally grounded approach. First, the strict application of the necessity test under Article 6(1)(b) GDPR may overlook scenarios where structured user environments support consumer protection. For example, high-value electronics retailers often rely on customer accounts to manage multi-year warranties, safety recalls, and proof of purchase. While the Recommendations suggest that after-sales services should function without accounts, fragmented ad hoc communication may increase legal and safety risks for both consumers and controllers.

Second, the treatment of legitimate interest in fraud prevention appears overly dismissive of persistent identifiers. Although the EDPB correctly stresses proportionality, it consistently finds that mandatory accounts fail the necessity test. In practice, however, large marketplaces use long-term behavioural patterns across user profiles to detect organised fraud schemes involving repeated high-value orders, address changes, and coordinated abuse—capabilities that guest-only systems may significantly weaken.

Third, the Recommendations frequently assume that less intrusive alternatives are equally effective. For instance, for conditional purchasing of professional-grade equipment, temporary verification forms are proposed as substitutes for verified accounts

While privacy-friendly, such solutions may create repeated manual checks, operational delays, and higher costs, whereas a verified professional account could offer both proportional data use and efficiency.

Fourth, the strong endorsement of guest mode leaves limited guidance for repeated transactions in regulated or safety-sensitive contexts. For example, online pharmacies relying exclusively on guest purchases may struggle with recall notifications, adverse

effect reporting, and continuity of consumer protection obligations, where limited persistent relationships could enhance public safety without excessive data retention.

Finally, the distinction between genuine “closed communities” and simple marketing-based registrations remains partly ambiguous. Loyalty-based early-access programmes or referral-restricted memberships fall into grey areas where the legality of mandatory registration may vary in interpretation, risking inconsistent enforcement across Member States.

In conclusion, while the Recommendations strongly and appropriately reaffirm that business convenience cannot justify intrusive data infrastructures, a more context-sensitive and risk-based application of necessity and legitimate interest could improve legal certainty. Greater attention to operational realities, fraud mitigation, consumer safety, and hybrid business models would help ensure that privacy protection and practical compliance evolve in a balanced and effective manner.

Marco Costantini