February 2026

DOT Europe consultation response

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

DOT Europe welcomes the opportunity to comment on the EDPB's draft Recommendations 2/2025 on the legal basis for requiring the creation of user accounts.

Before turning to the substance of our recommendations, we would like to highlight a main overarching issue that, in our view, should be addressed with regard to cooperation between the EDPB and stakeholders. In particular, we note that the draft Recommendations appear to rely on an analysis about the necessity of account creation without this assessment being published. We respectfully encourage the EDPB to publish this analysis to provide clarity and transparency regarding the evidence base supporting these conclusions. Given the significant operational changes that these draft Recommendations would entail for the e-commerce sector, we believe that a robust and structured consultation with industry is essential. Such engagement would help ensure a shared understanding of the practical use cases in which account creation is necessary, not only for the completion of transactions, but also for consumer protection and the integrity of services.

Scope

DOT Europe is concerned about the lack of clarity regarding the scope of the recommendations. The definition of "online software application services" and the treatment of intermediaries, including app stores and other actors in complex digital supply chains, remain ambiguous. While certain services (such as online news or search engines) are explicitly excluded, the absence of a clear framework creates legal uncertainty and raises the risk of an overly rigid, one-size-fits-all application that does not reflect different business models or technical realities.

We, therefore, encourage the EDPB to ensure these definitions are precise to prevent unintended consequences for digital ecosystems where accounts are technical prerequisites for service delivery.

Data collection

The Recommendations appear to be premised on risk, such as excessive data collection or tracking, that are not inherent to account creation. These risks can arise equally in "guest" transactions where core GDPR principles, including purpose and storage limitation, are not properly respected. For example, a company may retain "guest" data after a transaction is completed, even in the absence of legal or regulatory requirements to maintain such data, or utilize it for other purposes (e.g. marketing or analytics) that are not explicitly disclosed.

Online user accounts do not inherently pose greater risks to customers than guest checkout. Account-based models do not necessarily involve the collection of additional personal data or longer retention periods, as both data scope and storage duration depend on the e-merchant's specific account design.

Avenue Marnix 17
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43

In practice, the only additional data point may be an authentication credential, which need not be a password where passkeys or other password-less solutions are used, and retention periods can mirror those applicable to guest orders, as they are typically driven by the same statutory tax and accounting obligations. Users also retain control through account deletion or automatic removal of inactive accounts.

It should also be noted that responding to customers' exercise of their rights under GDPR actually requires additional data with guest mode, when, for instance, customers no longer have access to the original method of ordering. In this case, an online user account can provide such remote access, which is encouraged in Recital 63 GDPR.

Rather than discouraging account creation, which can, in fact, enhance user transparency and control, the Guidance should focus on ensuring that these fundamental GDPR principles are applied consistently across all checkout modalities.

Security and fraud prevention

While we support the objective of ensuring compliance with the GDPR and promoting data minimisation, we have significant concerns regarding the recommendations' treatment of security and fraud prevention. In particular, the draft underestimates the role that verified, persistent accounts play in protecting consumers. By suggesting that risks such as malware, account abuse, or scalping can be addressed equally well through alternative tools (e.g. CAPTCHAs or one-off links), the guidance overlooks the complexity of modern threats. Verified account are often a critical layer in robust fraud detection and maintaining trust and integrity across digital ecosystems. By contrast, guest-checkout models may in fact increase exposure to deceptive communications, as order-related interactions necessarily rely on email and are easier for malicious actors to impersonate. By contrast, mandatory user accounts raise the barrier to automated abuse, as account creation and authentication are harder to scale and enable the detection of suspicious behavioural patterns that would remain fragmented and less visible across repeated guest transactions.

Moreover, the EDPB's assessment does not sufficiently acknowledge the security, user control, and personalisation benefits that well-designed account-based models can provide. In particular, it overlooks how modern account systems can embed privacy-by-design features, granular consent management, and data-minimisation practices that may, in practice, offer users greater transparency and control over their personal data than less structured guest-checkout flows, while remaining fully compatible with GDPR requirements.

Legal bases for online user accounts

A central concern relates to the treatment of legal bases for processing. The GDPR does not establish a hierarchy of legal bases; all grounds under Article 6 are equal and must be assessed in context.

Lawful bases for processing personal data in the context of online user accounts do exist, yet the Recommendations do not sufficiently reflect the relevance of Article 6(1)(b) GDPR (contractual necessity) in business models where services are offered as an integrated bundle accessed through a single contractual relationship via an account implemented through specific technical architectures.

Nor do they fully account for relevant legal obligations that may necessitate account-based access, or for the practical benefits that such accounts can provide to data subjects compared to guest transactions.

Article 6(1)(b) GDPR should not be interpreted overly narrow or effectively excluded through general assumptions disconnected from how services are actually delivered. Contractual necessity remains a legitimate and important legal basis, to be assessed on a case-by-case basis, subject to proportionality and data minimisation.

Freedom to conduct business

DOT Europe urges avoiding a prescriptive "one-size-fits-all" approach that would mandate guest modes regardless of the context. The GDPR is a principle-based Regulation and, as such, should not dictate rigid operational requirements that would restrict one of the fundamental freedoms under the Charter of Fundamental Rights: the freedom to conduct business.

Controllers must retain the flexibility to determine the most appropriate means to discharge their obligations and serve their customers. Whether an account is "strictly necessary" should be assessed on a case-by-case basis, factoring in the specific nature of the service, the relationship with the user, and the legitimate interest in building customer relationships, benefits that are often lost in a forced guest-checkout model.

Final recommendations

We therefore encourage the EDPB to:

- Pause this exercise to conduct more thorough and comprehensive consultation with industry stakeholders and publish the underlying analysis to ensure full transparency and clarity regarding the evidence base for these measures;
- Reconsider its assumptions on the security and fraud-prevention value of user accounts, taking into account industry practice and real-world risk management;
- Acknowledge that legal bases under the GDPR are relevant for online user accounts (Art. 6(1)(b), Art. 6(1)(c) and Art. 6(1)(f));
- Recognise the validity of case-by-case assessments based on business contexts; and
- Provide greater clarity on the material scope of these draft recommendations, including the role of intermediaries, to ensure legal certainty and proportional application across sectors.

We remain available for further dialogue and would welcome continued engagement on these important issues.