Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Examining EU Data Watchdog's E-Commerce Account Guide

By **Vera Lukic, Ahmed Baladi and Hermine Hubert** (February 18, 2026, 3:24 PM GMT)


Vera Lukic


Ahmed Baladi


Hermine Hubert

On Dec. 3, the European Data Protection Board, or EDPB, adopted recommendations addressing the legal basis for requiring users to create accounts on e-commerce websites.[1]

This guidance marks a significant intervention by the EDPB into a commercial practice that affects controllers in the e-commerce sector operating within the European Economic Area or otherwise subject to the General Data Protection Regulation.

The recommendations were open for public consultation until Feb. 12, and stakeholder input may influence the final guidance.

This article examines the scope and practical implications of the EDPB's recommendations, analyzing when mandatory account creation may — and more often, may not — be justified under the GDPR. The discussion addresses the EDPB's assessment of each potential legal basis, highlights the risks that regulators have identified with forced account creation, and concludes with actionable takeaways.

Context and Scope of the Recommendations

The EDPB recommendations follow an ongoing debate among European supervisory authorities on guest checkout requirements. The recommendations apply to e-commerce websites, web applications and mobile applications where controllers require users to create online accounts before accessing offers or completing purchases.

The EDPB defines an online user account as a personal online space assigned to a user, accessible through an authentication mechanism using an identifier and password. Notably, the guidance excludes social media services, online marketplaces connecting nonprofessional individuals, search engines, audiovisual media services and news websites, as well as the offering of regulated products and services.

In accordance with the EDPB's central finding, imposing mandatory account creation would be justified only for a "very limited — though non-exhaustive — set of purposes," such as subscription services or access to genuinely exclusive offers. In the vast majority of common e-commerce scenarios, the practice would fail to satisfy the lawfulness requirements under Article 6 of the GDPR.

Rationale of Recommendations

According to the EDPB, mandatory accounts would encourage the development of so-called logged-in environments, where data subjects are systematically identified, resulting in greater volumes of personal data being collected, including data produced or inferred by the controller.

Accounts would also entail retention of personal data on active databases for periods exceeding what is strictly necessary for purchase and delivery, creating tension with the storage limitation principle under Article 5(1)(e) of the GDPR. The EDPB notes that unmanaged or so-called orphaned accounts present heightened vulnerability to unauthorized access and security breaches.

The EDPB also considers that logged-in environments would facilitate tracking of browsing habits for commercial targeting purposes, particularly through the combination of data across purchasing channels. The account creation process itself would also create opportunities for controllers to deploy deceptive design patterns, especially when account creation is requested between shopping cart validation and payment to extract last-minute consent for purposes unrelated to the transaction.

Analysis of Legal Bases Under Article 6 of GDPR

Performance of a Contract

The EDPB applies a strict interpretation of the necessity requirement under Article 6(1)(b) of the GDPR.

For one-time sales, the EDPB concludes that mandatory account creation cannot be justified under Article 6(1)(b) of the GDPR. The availability of guest checkout options demonstrate that personal data necessary for sales contract execution can be collected without requiring accounts.

The analysis differs for subscription services involving long-term contractual relationships requiring frequent identification. Where account functionality enables subscribers to access content, track deliveries throughout the subscription period, communicate securely with the merchant, or modify subscription terms, the EDPB is of the view that mandatory accounts may satisfy the necessity test — but only for the subscription's duration and where an actual, valid contract exists.

Access to exclusive offers presents a more nuanced scenario according to the EDPB. It distinguishes between genuinely restricted communities established through coopting, referral, invitation, member selection, or verified professional status, and offers that are notionally exclusive but are accessible to anyone willing to provide personal data. Only the former category would justify mandatory accounts.

Conditional purchasing scenarios — where purchases require proof of specific status, such as student or professional certification — would also fail the necessity test. The EDPB observes that controllers can verify status through secure online forms allowing one-time data collection and document upload, with deletion once verification is complete.

The recommendations explicitly reject the argument that a separate contract for personalized shopping recommendations can justify mandatory account creation at the point of purchase. According to the EDPB, where account creation is demanded after items are placed in the cart and checkout has begun, demonstrating consumer awareness and agreement to anything beyond the purchase itself appears unlikely.

Finally, the EDPB also considers that e-merchants cannot rely on Article 6(1)(b) of the GDPR to require account creation for after-sales services or rights management, as the necessity test is unlikely to be met when alternative identification methods, e.g., email, are available.

Compliance With Legal Obligation

The EDPB swiftly dispatches arguments that legal obligations, such as tax, accounting or regulatory requirements, necessitate mandatory account creation. According to the EDPB, processing and storage for tax and accounting purposes typically concerns specific documents like invoices, not the broader personal data associated with user accounts, and such obligations can be satisfied without accounts and without prejudice to users' ability to exercise their GDPR rights.

The legal basis under Article 6(1)(c) of the GDPR requires that obligations be "clear and precise" with foreseeable application, and that no less intrusive, equally effective means exist. The EDPB considers that these conditions will rarely be met for mandatory accounts.

Legitimate Interest

As developed in the EDPB guidelines on legitimate interest, controllers relying on Article 6(1)(f) of the GDPR need to pass the three-part test (legitimate interest, necessity, and balancing).[2] In that respect, the EDPB describes various purposes for which controllers may not rely on legitimate interest to justify the requirement to create an account.

For example, while order tracking functionality may benefit consumers, the EDPB considers that the purpose can be achieved through less intrusive means, such as emailed tracking numbers and hyperlinks. Similarly, order modification before dispatch can be offered through customer service or time-limited links included in order confirmations.

In the same way, for customer loyalty-related purposes, the EDPB is of the view that requiring data subjects to create an account does not seem strictly necessary to build a customer database for such purposes, since there may be other means to pursue such purposes, such as one-time collection of data, in particular an email address, through a guest mode or the creation of a voluntary online user account.

The EDPB emphasizes that personalized content "should result from an active choice of the data subject," rather than being presumed.

The EDPB also takes the position that the facilitation of subsequent orders argument fails because future purchases depend entirely on consumer decisions not yet made. At the point of initial purchase, data subjects would not reasonably expect their information to be retained beyond contract fulfillment, causing their fundamental rights to take precedence over the controller's commercial interest.

Finally, while fraud prevention may constitute a legitimate interest, the EDPB concludes that mandatory accounts are not necessary for this purpose. Many e-commerce sites would operate without mandatory accounts, and mandatory accounts would actually increase fraud risk by creating additional attack vectors through stored credentials and orphaned accounts.

Guest Mode Alternative and Data Protection by Design

The EDPB considers guest checkout as the privacy-protective default, consistent with the GDPR obligations regarding data protection by design and by default. Guest mode would allow order completion through simple form submission without authentication credentials, avoiding the creation of persistent personal digital environments.

The EDPB takes the view that offering a genuine choice between account creation and guest checkout enhances transparency by requiring controllers to articulate the distinct purposes and implications of each option clearly.

Users selecting guest mode would understand that processing serves only contract fulfillment, while those opting for accounts can be informed of additional services, such as facilitated subsequent purchases, loyalty programs and personalized offers.

Repeated guest purchases do not cause data duplication, according to the EDPB, if the controllers properly comply with purpose limitation principles. Tax and accounting records are retained regardless of checkout method, while other data should be deleted from customer relationship management systems, absent a valid legal basis for retention.

Implications for Businesses and Key Takeaways

The EDPB recommendations lack clarity. Key terms remain unsettled, and the use of hedging language, such as "unlikely," leaves practitioners uncertain as to the practical implications. As with other EDPB recommendations, the document presents the most obvious use cases, while failing to address more complex scenarios that reflect genuine business realities.

The core challenge remains the same — reconciling extremely strict, at times almost absolutist, regulatory expectations with a business environment that is far more nuanced than the EDPB's analysis suggests.

While the EDPB recommendations are nonbinding instruments, they remain highly influential in practice because supervisory authorities regularly follow them when interpreting the GDPR and making enforcement decisions.

Therefore, the publication of the final version of the recommendations should be tracked by stakeholders, and, in anticipation, a checkout architecture assessment may be carried out, including identifying where mandatory account creation is currently imposed and evaluating whether any justification applies.

In addition, to prepare for the potential strict reliance on these recommendations by supervisory authorities, practitioners could start reviewing privacy notices and legal bases documentation, ensuring each processing activity is individually justified with specific purposes rather than generic references.

Particular attention should be paid to the timing and presentation of account creation prompts, as requests made between cart validation and payment may raise heightened concerns regarding deceptive design and invalid consent.

Fraud prevention mechanisms should also be assessed independently of account creation requirements, evaluating whether alternative measures such as completely automated public Turing test to tell computers and humans apart, known as CAPTCHA tests, device fingerprinting or transaction monitoring

can achieve equivalent protection.

Finally, practitioners should prepare for strategic discussions to anticipate enforcement risks and help develop alternatives.

Vera Lukic is a partner at Gibson Dunn & Crutcher LLP.

Ahmed Baladi is a partner and co-chair of the privacy, cybersecurity and data innovation practice group at the firm.

Hermine Hubert is an associate at the firm.

[1] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/recommendations-22025-legal-basis-requiring_en.

[2] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, adopted on 8 October 2024.