EDPB Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites
Response to the public consultation

Alliance Digitale

Summary

Alliance Digitale welcomes the opportunity to provide feedback on the EDPB's draft recommendations on the legal basis for requiring the creation of user accounts on e-commerce websites. **We strongly support such efforts to establish a European harmonised framework upholding high user privacy protection**, which is key to giving legal certainty to businesses operating by nature across different Member States.

However, the current draft recommendations rely on a theoretical and fragmented vision of user accounts that overlooks practical security benefits and operational realities. In particular, they rely on an internal assessment' assumptions about the necessity of account creation without a clear evidentiary basis. **Such analysis should be published** so as to ensure that the final guidelines are grounded in transparent, verifiable evidence regarding security risks.

As the leading trade body for digital advertising and marketing in France, **Alliance Digitale hence respectfully recommends to the EDPB to**:

1. **Rectify unproven assumptions regarding the security of guest mode versus user accounts:** such a stance overlooks significant risks inherent to fragmented transactions resulting from guest mode;
2. **Broaden the interpretation of legal bases to reflect modern service ecosystems**: the use of an excessively strict "necessity" test under Article 6(1)(b) on performance of a contract and (f) on legitimate interest under the GDPR fails to account for how services are actually delivered;
3. **Integrate business model diversity and technical architecture constraints**: the "one-size-fits-all" approach used ignores the diversity of today's e-commerce websites, where products can be sold by multiple sellers at once, professional (B2C) as well as non-professional (C2C), risking fragmenting the user experience while infringing on freedom to conduct business (Article 16 of the Charter) and raising issues regarding

regulatory consistency;

4. **Leverage user accounts to enhance the exercise of users' rights under interacting legal frameworks**: GDPR as well as consumer law obligations apply to businesses, with the European framework being one of the most protective ones for users. As such, user accounts can empower data subjects, minimise data collection, and support the right of withdrawal – unlike guest mode.

Introductory remarks

The Digital Marketing and Data Association - Alliance Digitale is dedicated to **representing all professions and professionals linked to data and digital marketing in France**, with the aim of promoting their development and defending their interests. Alliance Digitale's mission is to represent the views of all its **300 members**, regardless of their size or position in the value chain – media and consulting agencies, publishers and sales houses, logistics providers, data providers, tech solution providers (AdTech, MarTech), and brands. Our trade body is the **French representative of three emblematic international digital marketing and data networks: IAB, FEDMA and GDMA**.

Alliance Digitale welcomes the opportunity to provide feedback on the EDPB's draft recommendations on the legal basis for requiring the creation of user accounts on e-commerce websites, which would help in harmonizing the European framework for cross-border businesses, but **the current draft recommendations are missing the practical security benefits and operational realities user accounts bring to users**.

As a contribution to this discussion, **we respectfully suggest to the EDPB the following modifications:**

(1) rectify **unproven assumptions** regarding the security of guest mode versus user accounts;
(2) broaden the interpretation of legal bases to reflect modern service ecosystems;
(3) integrate business model **diversity** and technical architecture **constraints**;
(4) leverage user accounts to enhance the exercise of users' rights under **interacting legal frameworks**.

In addition, we note that the draft Recommendations appear to rely on assumptions about the necessity of account creation without a clear evidentiary basis. Although the text refers to an internal analysis, this assessment has not been made public. **Alliance Digitale respectfully encourages the EDPB to publish this underlying analysis to provide clarity on the rationale and evidence supporting these measures.**

1. Rectify unproven assumptions regarding the security of guest mode versus user accounts

Context: In these draft recommendations, the EDPB establishes a presumption that "guest mode" is inherently more protective and less risky for users than the creation of a user account. This position relies on **theoretical assumptions that do not reflect the technical realities of modern cybersecurity and fraud prevention**.

We identify several major flaws in this reasoning:

- **Increased phishing and social engineering risks**: Guest mode relies heavily on transactional links sent via email or text message. This practice conditions users to click on external links to manage their orders, making them significantly more vulnerable to phishing and social engineering attacks. Conversely, user accounts allow individuals to log in independently to a secure, authenticated environment to verify the status of a transaction, following best practices recommended by Member State agencies such as the German Federal Office for Information Security (BSI) which recommends to only enter personal information in already-familiar environments to avoid phishing[1];
- **Superiority of advanced authentication mechanisms**: The EDPB downplays the security potential of customer accounts. Verified accounts are the only practical way to implement robust security solutions such as Multi-Factor Authentication (MFA) and passkeys, which virtually negate the risks associated with password theft or credential stuffing;
- **Ineffectiveness against malicious bots and "scalping"**: The EDPB suggests that alternative measures like CAPTCHAs are sufficient to thwart bots or prevent automated “card testing” attacks. However, we would like to emphasise that verified accounts are a far more effective tool for monitoring suspicious behavior and preventing malicious bots from monopolizing stock for resale at inflated prices (scalping) or test whether stolen credit cards are still active for fraudulent purchases—a protection that is largely unavailable in guest mode where orders are processed in isolation. This level of protection is structurally impossible in a transient guest session. Therefore, a mandate for guest mode effectively removes a primary layer of fraud detection, harming both merchants and consumers.

Alliance Digitale’s proposals:

1. Modify paragraph 9 of the recommendations to **recognise that over-reliance on**

[1] "Only enter personal information in the usual way, for example on the online banking website", translated from German. Bundesamt für Sicherheit in der Informationtechnick (BSI), « Wie schützt man sich gegen Phishing? », bsi.bund.de, as seen on February 6, 2026. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing_node.html

email-based links in guest mode substantially increases the risk of successful phishing attacks;

2. Revise paragraph 10 to **acknowledge that account creation is a legitimate and effective instrument for combating malicious bots, "scalping," and stolen credit card testing** surpassing the technical capabilities of simple CAPTCHA tests;
3. Amend paragraph 11 by **highlighting that password-related risks are now largely mitigated by the increasing adoption of MFA and passkeys**: the EDPB should encourage these secure authentication methods rather than marginalizing user accounts.

2. Broaden the interpretation of legal bases to reflect modern service ecosystems

Context: The draft recommendations apply an excessively restrictive interpretation of the lawful bases for processing under Article 6(1) of the GDPR, particularly regarding "contract performance" and "legitimate interests".

We identify a **significant gap** between the EDPB's theoretical approach and the integrated nature of modern digital services:

- **The reality of holistic offerings**: Many e-merchants do not offer products in isolation. Instead, they provide a "holistic overall offering" where the user account serves as the core of a single, unified contract. In this context, the account itself can be considered a standalone service that binds together various features (subscriptions, exclusive offers) that are unsuitable for a guest mode. What is more, marketplaces' business models can vary greatly from one actor to another: attempting to fragment the legal basis of the account depending on whether the seller is a professional (B2C) or a non-professional (C2C) would artificially split a single service contract, while mandatory accounts are a binding legal obligation, and essential for maintaining trust and safety between individuals. Mandatory user accounts are not merely a commercial choice but a necessary legal and operational requirement for marketplaces. They are essential to ensuring trust, traceability and user safety between individuals, including dispute resolution, fraud prevention, as well as compliance with regulatory obligations such as cooperation with tax authorities and transaction reporting;
- **Operational and industrial constraints**: The EDPB's "strict necessity" test for contract performance is interpreted in an abstract manner, ignoring that modern e-commerce infrastructures (CRM, logistics, SAV) are natively and historically built around the user account. Forcing a guest mode alternative represents a disproportionate industrial and economic burden without necessarily providing a privacy gain, as systems would have to be entirely re-engineered at a high cost;
- **Facilitating legal rights and obligations**: Contrary to the EDPB's view, accounts are often necessary to fulfill legal obligations that require authenticated identity and traceability, such as age-gating, product recalls, or transparency requirements under the Digital

Markets Act (DMA). Furthermore, consumer laws (e.g., right of withdrawal) are better served by a secure personal space that ensures reliable identification and traceability, which transactional guest modes cannot reliably provide;

- **Legitimate interest in customer experience**: E-merchants have a legitimate interest in providing a consistent and unified customer experience. Splitting offerings into guest and account modes leads to customer confusion and less effective support, especially for purchases involving third-party sellers where communication must be centralised and archived.

> **Alliance Digitale's proposals:**
>
> 4. Amend Section 3.1 related to performance of a contract under Article 6(1)(b) of the GDPR to **acknowledge that for "holistic offerings", the user account constitutes the core of the contractual relationship and the primary means of delivering the service**, making it strictly necessary for the contract's performance;
> 5. Revise Section 3.3 related to legitimate interest under Article 6(1)(f)) of the GDPR to recognise that **ensuring a consistent customer experience and effective, secure customer support constitutes a valid legitimate interest** that justifies mandatory account creation;
> 6. Update Section 3.2 (Article 6(1)(c)) to **include a broader range of legal obligations that may require authenticated accounts**, such as compliance with consumer protection laws requiring robust traceability for withdrawals and returns;
> 7. Ensure that the **recommendations do not infringe on an e-merchant's right to define its own business model as per the freedom to conduct business principle** (Art. 16 of the Charter) in a competitive market where "guest mode" alternatives are widely available from other competitors.

3. Integrate business model diversity and technical architecture constraints

Context: The current draft recommendations adopt a **"one-size-fits-all" approach that fails to account for the technical and economic diversity of the digital ecosystem**.

By establishing a general presumption in favor of "guest mode," the EDPB overlooks several following industrial and operational realities:

- **Native IT architecture and industrial constraints**: Many e-commerce websites operate on technical architectures (including CRM, order management, and after-sales services) that have been historically and functionally built around the user account. Forcing an alternative "guest mode" is not a neutral change; it represents a disproportionate cost and a lack of operational efficiency. The "strict necessity" test must consider these real-world industrial and economic constraints rather than being interpreted in an abstract vacuum;

- **Technical and operational impracticability**: Modern e-commerce architectures are industrially designed around a unified user identity to manage CRMs, cross-seller shopping carts, and integrated logistics, fit for hybrid business models. As an example, forcing a guest mode specifically for B2C transactions on a platform that requires accounts for C2C safety and compliance would impose a disproportionate technical re-engineering burden. Such a "dual legal regime" would create fragmented and incoherent user journeys, significantly increasing operational overhead and the risk of technical errors in order management and fraud detection;
- **Ambiguity in scope and digital supply chain**: The recommendations lack clarity regarding their application to "online software application services" and intermediaries like app stores where the account is not merely for the “transaction” but is the technical mechanism that anchors the licence to the user rather than a temporary device. It is necessary to ensure portability across multiple devices, recovery (if a device is lost or replaced), or security updates. This ambiguity creates significant legal uncertainty for sectors that are not traditional e-merchants but fall within the complex digital supply chain;
- **Regulatory consistency**: Companies operate under multiple legislative frameworks, under which offering a guest mode for their own products while being unable to do so effectively for third-party sellers on their marketplace could lead to non-compliance. To avoid conflicts and for efficiency purposes, implementation of these frameworks should prevail over new provisions;
- **Infringement on the freedom to conduct business principle**: E-merchants should remain free to define their business models and technical setups. Restricting the ability to require an account—especially in a highly competitive market where consumers can easily switch to a competitor—violates this Charter principle;
- **Reduction of consumer choice**: Data subjects should be free to choose their preferred merchant, including based on guest account availability if it is a differentiating criterion to them. This would require leaving guest account availability to the decision of individual online service providers, instead of mandating it in an indiscriminate manner.

Alliance Digitale’s proposals:

8. **Introduce an explicit "case-by-case" approach** in the final guidelines acknowledging that the **user account is merely a modality for collecting data** whose necessity and compliance to the GDPR must be assessed for each and every actor with regards to its business model and in line with the accountability principle. This would also help prevent service fragmentation, ensure user safety while avoiding unintended impacts on intermediaries and non-retail digital services, including those combining **B2C and C2C activities** as well mentioned but yet to be defined "**e-commerce websites**" and "**online software application services**”[2];

[2] Such definitions of «e-commerce websites" and "online software application services would also be beneficial to the sector.

9. **Acknowledge technical and industrial feasibility as a relevant factor when assessing the "necessity" of account creation** under Article 6(1)(b) and (f) of the GDPR, ensuring that the transition to guest mode does not impose a disproportionate burden on existing IT infrastructures;
10. **Ensure regulatory consistency**, stating that compliance with data protection recommendations should not force businesses into practices prohibited under other legal frameworks.

4. Leverage user accounts to enhance the exercise of users' rights under interacting legal frameworks

Context: The draft recommendations operate under the **false premise that guest mode is inherently more compliant with the principles of data minimisation** and data protection by design and by default of the GDPR.

However, we identify here a significant "data minimisation paradox". For returning customers, guest mode frequently leads to more extensive and redundant data processing. In guest mode, the e-merchant must repeatedly collect the same information (name, delivery address, payment details) and perform new fraud preventions and credit checks for every single order, as there is no historical record to rely on. A properly designed user account avoids this fragmentation and redundancy by centralizing data in a single, manageable space.

What is more, user accounts are often the most effective tool for empowering data subjects:

- **Enhancing the exercise of GDPR rights**: Contrary to the EDPB's view that accounts are not necessary for exercising rights, secure accounts provide a reliable and autonomous environment for users to exercise their rights of access, to rectification, and erasure. Such views are hence incoherent with Recital 63 of the GDPR, which encourages the provision of "remote access to a secure system" for direct data access;
- **Reliability of identity verification**: Responding to a data subject's request in guest mode can be technically challenging and may actually require the collection of additional sensitive information such as ID documents to verify identity if the user no longer has access to the original email or phone used for a one-time purchase. User accounts, supported by strong authentication as mentioned before, are an appropriate "privacy by design" measure by ensuring the requester is indeed the account holder;
- **Consistency with consumer protection law**: Exercising consumer rights, such as the right of withdrawal or statutory warranties, requires robust traceability and reliable identification over time. Managing these legal obligations via ephemeral, transactional links is often less reliable for the consumer than a permanent personal space where all contractual documents and history are securely archived.

Alliance Digitale's proposals:

6. **Encourage data minimisation best practices such as (a) decoupling account creation from any non-essential tracking, advertising, or personalisation logic** to ensure that the account's primary purpose remains functional security and service integrity, **(b) limiting the personal data requested during registration to the absolute minimum required to provide the service and secure the transaction**, **(c) strengthening security standards** through the systematic implementation of advanced authentication methods (such as MFA and passkeys), and **(d) empowering users with effective control** by providing simple, transparent, and user-friendly mechanisms for the immediate deletion of the account and all associated personal data upon request.
7. Revise Paragraph 86 to **acknowledge that, for recurring customers, user accounts can be more compatible with the data minimisation principle** than guest mode by preventing data collection duplication and redundant fraud or credit checks;
8. Amend Section 3.1.5 ("After-sales services and exercise of rights") to incorporate the guidance of Recital 63 GDPR, **recognizing that mandatory accounts can serve as the recommended "secure system"** for providing data subjects with direct and autonomous access to their data;
9. Update paragraph 51 to **acknowledge that identity verification for GDPR rights in a guest mode environment may inadvertently lead to over-collection of data**, whereas authenticated accounts facilitate a more secure and privacy-friendly verification process;
10. **Refer to the "parallelism of forms" principle** in the final recommendations, ensuring that users who provide data electronically can also manage and delete that data through the same secure interface, thereby enhancing transparency and user control;
11. **Acknowledge the role of accounts in consumer law compliance**, stating that a persistent personal space is a legitimate tool for e-merchants to ensure the traceability and effectiveness of rights such as product recalls and legal guarantees.