

Bitkom on the EDPB Recommendations 2/2025

on the legal basis for requiring the creation of
user accounts on e-commerce websites

At a glance

Bitkom on the EDPB Recommendations 2/2025

Initial position

The EDPB Recommendations 2/2025 provide important guidance on mandatory user accounts in e-commerce. While strengthening user choice, the draft introduces a de facto presumption in favour of guest mode that risks overlooking established, lawful and user-friendly and secure digital business models.

Bitkom rating

Goes in the right direction: The focus on user choice and privacy by design is welcome. However, the Recommendations apply an overly strict necessity test and risk creating a one-size-fits-all approach that limits innovation, security and flexibility in the digital economy.

The most important takeaway

Bitkom represents both digital-native providers and companies closely connected to traditional commerce. Our paper therefore outlines balanced compromise lines:

■ **Guest mode should remain voluntary, not mandatory**

Optional guest mode can enhance trust and conversion as a part of companies service design. However, making guest mode a regulatory obligation is unnecessary, as market dynamics already reward services in line with user preferences.

■ **Contractual freedom and private autonomy must be preserved**

The Recommendations should respect the parties' freedom to decide whether and how contracts are concluded. A mandatory guest mode would be neither necessary nor proportionate, as it disregards private autonomy and fails to adequately account for the freedom to conduct a business under Article 16 of the Charter of Fundamental Rights of the European Union.

■ **User accounts are often necessary and beneficial**

For integrated offerings, high-value products, subscriptions and marketplaces, user accounts are essential for contract performance, security, customer service and compliance. They can be implemented in a GDPR-compliant and user-protective manner.

■ **Differentiation and flexibility are key for platforms and marketplaces**

The Recommendations should clearly distinguish between buyer and seller sides and allow diverse business models. Flexibility enables competition on privacy and usability while safeguarding security, compliance and consumer trust.

Content

I. General assessment and relevance for the digital economy	4
II. General remarks on the structure and approach of the Recommendations	4
III. Differentiation as a market-based solution – not a regulatory mandate	5
IV. Guest mode is not inherently more data-minimising	5
V. User accounts do not inherently increase risks or lead to unlawful processing and deceptive actions	6
VI. Combined sale of hardware and digital subscription services	7
VII. Timing of account creation and customer expectations for high-value products	7
VIII. Marketplaces: clear distinction between buyer and seller side	8
IX. Available legal bases for user accounts	8
1. Performance of a contract (Article 6 Abs. 1 lit. b GDPR)	8
2. Compliance with legal obligations (Article 6 Abs. 1 lit. c GDPR)	8
3. Legitimate interests (Article 6 Abs. 1 lit. f GDPR)	9
X. Data subject rights	9
XI. Conclusion and recommendations	10

I. General assessment and relevance for the digital economy

The European Data Protection Board's (EDPB) Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites address a core element of digital business models. User accounts are not merely optional features, but frequently constitute an essential infrastructure for contract performance, security, customer support, regulatory compliance, and user experience.

The Recommendations are therefore of considerable practical relevance for the digital economy. By effectively establishing a presumption in favour of «guest mode» and applying a very strict interpretation of the necessity requirement under Article 6 GDPR, the draft guidance risks calling into question established, lawful and consumer-friendly business models, without sufficiently reflecting their operational complexity or protective functions or providing a comprehensive impact assessment or empirical evidence to support this view.

The Recommendations allude to an assessment conducted by the Board regarding why mandatory accounts may – or may not – be necessary, but this analysis remains unpublished. Bitkom encourages the EDPB to release this underlying assessment to provide clarity on the Board's rationale and ensure the guidance is grounded in transparent, verifiable evidence. Access to this analysis is vital for the industry to understand how specific risks, particularly regarding security and fraud, were weighed against the proposed guest mode mandates.

Bitkom supports the objective of ensuring a high level of data protection and preventing unlawful or manipulative practices. At the same time, the Recommendations should be further developed to ensure that they are practical, technology-neutral and proportionate, and that they adequately reflect the diversity of digital business models, as well as the interests of consumers, businesses and the overall digital ecosystem, including their private autonomy to decide whether to offer or conclude contracts, including their private autonomy to decide whether to offer or conclude contracts.

II. General remarks on the structure and approach of the Recommendations

The Recommendations effectively establish a general presumption that e-commerce services should offer a guest mode and that mandatory user accounts are permissible only in narrowly defined exceptional cases. This approach significantly raises the burden of justification for businesses and risks marginalising lawful processing based on contract performance and legitimate interests.

Such an approach may:

- unduly narrow the scope of Articles 6(1)(b) and 6(1)(f) GDPR;
- disregard legitimate and well-established business interests;

- and insufficiently take into account the freedom to conduct a business under Article 16 of the Charter of Fundamental Rights of the European Union.

A more differentiated assessment is required to avoid a «one-size-fits-all» outcome that does not reflect market realities.

III. Differentiation as a market-based solution – not a regulatory mandate

The possibility to shop without mandatory registration has become an important element of competition and trust-building in e-commerce. Where consumers value such an option, the market already provides strong incentives for businesses to offer it.

From Bitkom's perspective, the Recommendations should be understood as a confirmation of user choice and guest mode as a competitive instrument, not as a justification for imposing rigid structural requirements on all e-commerce services.

A mandatory requirement to offer guest mode is neither necessary nor proportionate, as:

- it disregards the diversity of business models and customer expectations;
- it disregards the private autonomy of the parties involved;
- it risks reducing innovation in user experience and service design;
- and it overlooks that user preferences already function as an effective corrective mechanism.

Allowing flexibility enables companies to compete on privacy, usability and trust, while still fully complying with the GDPR. Companies that choose to offer guest mode do not lose anything under a flexible framework, whereas a mandatory approach would unnecessarily constrain others. Thus, the Recommendations should recognize that the purposes of data processing (Articles 6(1)(b) and 6(1)(f) GDPR) follow the contract concluded between the parties and not vice versa.

IV. Guest mode is not inherently more data-minimising

The Recommendations assume that guest mode is generally more data-minimising. This assumption does not hold true in practice. Orders placed via guest mode typically require the processing of the same categories of personal data as orders placed via a user account, including:

- identity and contact data;
- delivery and billing information;
- payment data;

- data required for returns, warranty and guarantee management (often over several years);
- data necessary to comply with data subject rights under the GDPR.

Guest mode therefore does not automatically lead to less data processing. On the contrary, it would result in duplicative data collection, additional identity verification steps, additional fraud prevention steps and increased organisational complexity, particularly for returning customers or in warranty cases. Furthermore, guest mode does not automatically reduce storage durations of personal data as storage durations in the context of user accounts can be aligned with durations that would be required for orders via guest mode.

V. User accounts do not inherently increase risks or lead to unlawful processing and deceptive actions

Bitkom considers the assumption that user accounts inherently increase risks for users to be insufficiently substantiated.

Well-designed user accounts can:

- enable strong authentication methods (e.g. passkeys, multi-factor authentication);
- reduce phishing risks by allowing users to verify communications directly within their account;
- limit automated abuse and scalping;
- support effective and proportionate fraud prevention mechanisms.

By contrast, guest mode often relies more heavily on email-based communication, which may increase phishing risks. Moreover, fraud prevention checks may need to be repeated for each guest order, whereas returning customers with accounts can benefit from established trust signals. Guest mode interfaces, by design, lack the friction of authentication. This makes them a preferred target for automated "card testing" attacks, where malicious actors test thousands of stolen credit card credentials rapidly.

Furthermore, user accounts do not inherently result in unlawful processing of personal data and deceptive actions since user accounts can well be established and run within a lawful framework, complying with GDPR requirements.

Accounts enable controllers to perform risk analysis based on account history and behavior (e.g., detecting sudden changes in shipping addresses or device fingerprints), this view being impossible in a transient guest session.

The Recommendations should therefore clarify that securely implemented user accounts do not per se (i) create higher risks, but can form part of a robust security architecture that benefits both consumers and businesses (ii) lead to unlawful processing of personal data and deceptive actions.

VI. Combined sale of hardware and digital subscription services

The Recommendations primarily distinguish between:

- one-time purchases of goods
- and subscription-based services.

However, they do not adequately address a highly relevant business model for the digital economy. The combined sale of hardware together with digital services that are subscribed to at the time of purchase (e.g. security services, cloud services, maintenance, insurance, or software services).

It should be clarified that:

- such constellations fall under the reasoning applicable to subscription services pursuant to Section 3.1.2 of the Recommendations;
- the contract from the outset includes ongoing and recurring obligations, which typically require authentication, configuration and management by the user;
- in these cases, the user account is an integral component of contract performance, rather than a mere convenience feature.

Bitkom therefore encourages the EDPB to explicitly address this hybrid model in the Recommendations to ensure legal certainty.

VII. Timing of account creation and customer expectations for high-value products

The analysis under Section 3.3.1 («Management of subsequent changes to the order») does not sufficiently reflect customer expectations in the context of high-value and complex products, particularly where such products are combined with subscription-based digital services.

In these cases, customers legitimately expect:

- comprehensive possibilities to modify, configure or influence the product and associated services;
- up to the latest possible point prior to handover or activation;
- through a secure and centralised interface.

For such offerings, the user account is functionally necessary to enable contractual changes, service configuration and the activation of subscribed services. Consequently, the necessity test under Article 6(1)(b) GDPR should be assessed from the moment of contract conclusion, and not only from the moment of first use or delivery of the hardware.

VIII. Marketplaces: clear distinction between buyer and seller side

In the context of online marketplaces, it is essential to clearly distinguish between the buyer side and the seller side.

On the buyer side (B2C and C2C), voluntary guest mode can be a valuable instrument to promote user choice and user trust.

On the seller side, however, mandatory user accounts and reliable identification remain indispensable, particularly to ensure compliance with:

- know-your-customer (KYC) obligations;
- DAC7 reporting requirements;
- due diligence obligations under the Digital Services Act (DSA);
- and other regulatory and safety-related requirements.

The Recommendations should avoid any ambiguity that could be interpreted as questioning the necessity of mandatory seller accounts, as this would undermine security, compliance and trust in marketplace ecosystems.

IX. Available legal bases for user accounts

1. Performance of a contract (Article 6 Abs. 1 lit. b GDPR)

User accounts may themselves constitute part of the contractual service, particularly for:

- platform-based and marketplace models,
- integrated digital ecosystems,
- offerings involving regulated products or services,
- holistic service bundles accessed through a single interface.

An isolated assessment of individual products or services does not adequately reflect these business models. Furthermore, restrictions to companies' decision-making on their business models and how they design their online business would violate their freedom to conduct business (Art. 16 of the Charter of Fundamental Rights of the European Union).

2. Compliance with legal obligations (Article 6 Abs. 1 lit. c GDPR)

The Recommendations do not sufficiently consider legal obligations that may require authenticated access or traceability, such as:

- age verification requirements;
- product safety and recall obligations;
- regulatory transparency obligations (e.g. under the Digital Markets Act).

3. Legitimate interests (Article 6 Abs. 1 lit. f GDPR)

Many e-commerce platforms rely on User accounts to ensure:

- a consistent customer experience;
- effective customer support and self-service solutions;
- efficient interaction with third-party sellers on marketplaces.

Bitkom encourages the EDPB to consider that processing of personal data can be considered necessary for pursuing legitimate interests where these cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects.

Guest mode is not an equally effective alternative for achieving these legitimate interests and may lead to fragmented user journeys and reduced transparency for consumers.

X. Data subject rights

User accounts can facilitate the exercise of data subject rights in a more data-protection-friendly manner than guest mode by:

- reducing the need for additional identity verification data;
- enabling secure remote access to personal data (as encouraged by Recital 63 GDPR);
- lowering the risk of misuse or errors.

A mandatory guest-mode approach may therefore, in certain cases, run counter to the principle of data protection by design and by default under Article 25 GDPR.

XI. Conclusion and recommendations

Bitkom encourages the EDPB to further refine the Recommendations by:

1. Explicitly recognising hybrid and holistic business models, including combined hardware-and-service offerings;
2. Avoiding any implication that guest mode should be mandatory, while allowing businesses to decide freely whether and how to offer guest mode in line with their contractual setup and user expectations;
3. Adopting a technology-neutral and evidence-based approach to security and fraud prevention;
4. Acknowledging that personal data can be processed in line with GDPR requirements in the context of user accounts;
5. Clarifying the scope of application, in particular for platforms and marketplaces and the distinction between buyer and seller sides;
6. Ensuring appropriate consideration of contractual freedom and the freedom to conduct a business under Article 16 of the Charter of Fundamental Rights of the European Union alongside data protection objectives.
7. Publish the analysis the EDPB refers to provide clarity and transparency and allow stakeholders to fully understand the evidentiary basis for the proposal.

A high level of data protection and a competitive, innovative digital economy are mutually reinforcing goals. Achieving both requires guidance that is balanced, proportionate and reflective of real-world digital services and business models.

Bitkom represents more than 2,300 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact person

Isabelle Stroot | Head of Data Protection Law & Policy

P +49 30 27576-228 | i.stroot@bitkom.org

Responsible Bitkom Committee

WG Data Privacy

Copyright

Bitkom 2026

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.