Comments on the EDPB recommendations 2/2025 *on the legal basis for requiring the creation of user accounts on e-commerce websites*

1. Introduction

Thuiswinkel.org is the Dutch trade association for the e-commerce sector. Our members represent approximately 75% of all consumer spending in the Netherlands. Our constituency consists of companies that offer products and services to consumers through digital channels. These companies vary significantly in nature, scale and business model and together represent the full breadth of e-commerce activities.

Through this position paper, we welcome the opportunity to respond to the recommendations of the European Data Protection Board (EDPB) regarding the mandatory use of user accounts on e-commerce websites. We support the objective of ensuring a high level of data protection. However, we believe that certain aspects of the recommendations leave insufficient room for legitimate differences in services and business models.

Our core concerns relate in particular to the limited space the recommendations leave for freedom of enterprise, the diversity of e-commerce services, and the reality that an account can form part of the agreed service. In addition, we question the proportionality and effectiveness of a general preference for guest checkout, particularly in light of data protection, fraud prevention and consumer rights.

2. Freedom of Enterprise

Thuiswinkel.org emphasises that every entrepreneur has the freedom and the right to determine the conditions under which they are willing to offer their products and/or services to consumers, provided those conditions are non-discriminatory and in line with general civil law, consumer legislation and, where applicable, platform regulation, including the Digital Services Act (DSA). This freedom of enterprise is safeguarded by Article 16 of the Charter of Fundamental Rights of the European Union.

This freedom does not only concern the possibility of requiring an account as a condition, but also the freedom to shape the service itself. Entrepreneurs must be able to decide whether they offer a purely transactional webshop or a service focused on personalisation, inspiration, convenience and an ongoing customer environment. This also includes the freedom to define the subject matter of the agreement: what exactly is delivered to the consumer and under which conditions.

Conversely, consumers are free to purchase a product or service from a given provider under the conditions set by that provider. Just as consumers weigh factors such as price, delivery time and withdrawal period when making a purchase decision, they can also take into account whether or not the creation of an account is required. Considering these non-exhaustive factors may lead a consumer either to proceed with the purchase or to refrain from doing so.

The proposed obligation for entrepreneurs to offer a guest checkout option as a counterbalance to requiring an account interferes with the freedom of the entrepreneur to offer products and services under their chosen conditions. Data protection rules are intended to regulate the processing of personal data, not to redesign business models. It is important that the interpretation of the GDPR remains balanced with other fundamental rights, including the freedom to conduct a business.

3. Proportionality

With regard to the concerns raised by the EDPB in paragraphs 7 to 11, Thuiswinkel.org considers that these concerns cannot be directly linked to the requirement to create an account in order to make a purchase. As the EDPB itself notes, risks such as data loss due to malware, insecure passwords and security breaches are inherent to the use of any online account. In our view, the existence of such risks cannot in itself serve as a starting point for a general obligation to offer guest checkout. Entrepreneurs are already responsible for implementing appropriate technical and organisational measures to ensure that personal data are processed in a manner that guarantees appropriate security (Article 5(1)(f) GDPR).

The concerns raised by the EDPB in paragraphs 13 and 14 can be addressed by ensuring that, when creating an account, the collection of personal data is closely aligned with Article 5(1)(a) and Article 6(1)(a) GDPR. Where consent is required, it must be obtained in accordance with Article 6(1)(a) GDPR. Where processing is based on the performance of a contract or on a legitimate interest, this must be clearly and demonstrably substantiated pursuant to Article 6(1)(b) or (f) GDPR.

Furthermore, any potential negative consequences of non-compliance rest with the entrepreneur. It is for national supervisory authorities to assess, on a case-by-case basis, whether the GDPR has been complied with and, where appropriate, to take further action. A general recommendation that effectively amounts to a standard obligation to offer guest checkout fits less well with such case-by-case assessment and with the diversity of services in e-commerce practice.

Practice also shows that requiring an account does not necessarily result in more data processing. A guest model may lead to additional repetition, additional checks and additional linkages, for example because customers must repeatedly identify themselves or because additional verification is required for payments and fraud prevention.

4. The Use of Accounts in E-commerce Practice

Customer accounts are a common and functional instrument in e-commerce practice for structuring service provision and communication towards consumers. Requiring the creation of an account contributes to an optimised customer experience and streamlined communication. It also enables customers to exercise their consumer rights easily and efficiently, such as the right of withdrawal, submitting complaints regarding product conformity and contacting customer service. The use of such accounts also ensures that consumer reviews published by entrepreneurs originate from customers who have actually purchased or used the product, in line with Directive 2019/2161.

Naturally, entrepreneurs remain at all times obliged to ensure that the collection and processing of personal data comply with the GDPR, irrespective of whether a guest checkout or a mandatory account is used. At the same time, accounts enable customers to exercise their rights under the GDPR, including Articles 15 to 18 GDPR. Furthermore, accounts enable entrepreneurs to verify the identity of the person exercising those rights. The use of a guest checkout will still result in the collection and processing of personal data of the customer.

It is important to note that many modern e-commerce services go beyond a single purchase. Retail services are often ongoing: inspiration, preferences, order history, returns across multiple sellers, warranty and customer service over a longer period of time. The execution of the agreement between consumer and provider therefore does not end at checkout but continues afterwards. In that context, an account may constitute a logical and sometimes necessary component of the agreed service.

For the customer, an account primarily functions as the key to their personal environment, including order history, invoices, returns and service cases. The underlying order data must in any event be stored in a structured manner in order to perform the contract and comply with statutory obligations. The account does not create that data; it makes it accessible and manageable for the customer. Even in the case of a guest checkout, a technical account or transactional record is created, albeit without a durable login credential for the customer. Additionally, modern authentication methods such as password reset, passwordless login and social login mean that requiring an account does not necessarily create a barrier for consumers. In practice, it is often the fastest route to completing a purchase, as customers do not have to repeatedly enter the same information.

Below is a non-exhaustive overview illustrating the value of customer accounts for webshops and, in particular, online platforms.

Ordering Without an Account Does Not Necessarily Lead to Less Data Processing

Offering a guest checkout may create the impression that fewer personal data are processed, whereas in practice this is often not the case. Even without an account, the entrepreneur must process personal data such as name, address, order details and invoice information in order to perform the contract. In addition, tax legislation requires invoices and underlying documentation to be retained for seven years. The absence of an account does not change these statutory retention obligations.

Guest checkout may therefore create a false sense of reduced processing: it may appear as if less data are processed or stored, while the same data remain necessary and legally required. This may even undermine consumer expectations regarding what happens to their personal data. At the same time, offering a full guest-checkout solution alongside account-based processes entails significant operational costs. These investments do not lead to a demonstrable reduction in personal data processing nor to a concrete improvement in privacy protection. From the perspective of proportionality and effectiveness, there is therefore no fair balance between the costs incurred by the entrepreneur and the alleged privacy benefit for the customer.

In addition, a guest model may in practice lead to more processing, as the same individual must repeatedly enter data and undergo verification during subsequent interactions.

An Account Enables Structured Data Minimisation and Purpose Limitation

A customer account enables the entrepreneur to process personal data in a structured, purpose-bound and proportionate manner. Without a customer account, there is a greater risk of fragmented storage or duplication of data, which may increase the risk of errors and unnecessary processing. Data minimisation must be assessed in relation to the specific purpose pursued. It is not intended to redefine the purpose or the service itself, but to ensure that processing remains appropriate in light of what is offered and agreed.

An Account Supports Service Provision, Transparency and Consumer Control

Many core consumer functionalities and corresponding obligations for entrepreneurs are linked to a customer account. This concerns not only the efficient provision of services but also transparency, legal certainty and continuity for the consumer. Examples include:

- Tracking orders
- Access to invoices and proof of purchase
- Returns and warranty requests
- Subscription management
- Customer service and complaint handling

An account also enhances transparency and control for the consumer over their personal data. Contrary to the assumption that an account would restrict privacy, an account may in fact support it. Through an account, customers have insight into their personal data and order history, can easily correct or update information and centrally manage privacy and communication preferences. Requests under the GDPR, such as access, objection and erasure, can also be handled in an efficient and secure manner.

Consumers also increasingly expect continuity and efficiency in their interactions. A well-designed customer account offers a transparent and structured means of providing such service. In practice, privacy and security risks more often arise from opaque data processing environments than from visible, customer-facing account structures.

For platforms and marketplaces, the coordination of processes across multiple sellers adds an additional dimension. A central customer environment makes communication, return handling and warranty support more structured and manageable for the consumer. When carefully and transparently designed, an account can strengthen both the quality of service and the effective exercise of consumer rights, without automatically linking marketing or tracking to the use of the account.

Fraud Prevention

The use of a customer account and the associated processing of personal data is essential for ensuring fraud prevention and payment security. For online platforms, the entrepreneur is subject to a statutory duty of care to take appropriate measures to prevent and limit misuse and fraud. This duty arises, inter alia, from general civil law, consumer protection rules and, where applicable, specific platform regulation including the Digital Services Act (DSA).

The DSA requires online platforms to identify and mitigate systemic risks, including misuse and fraudulent activities, by means of appropriate and proportionate measures. In that context, fraud prevention is not optional but a necessary component of responsible platform governance. Without a customer account, the continuity and contextual linkage necessary to effectively fulfil this duty of care may be lacking. This may lead to the deployment of heavier or more intrusive measures, such as extensive device- or behavioural-based analysis. Such measures may have a greater impact on customers' privacy than proportionate and transparent account-based fraud prevention.

For providers subject to stricter obligations, such as very large online platforms, this consideration applies even more strongly.

Legal and Safety Obligations Are Difficult to Execute Without an Account

Entrepreneurs offering products or services to consumers, including online platforms, are subject to various legal obligations. They must inform customers in a timely and effective manner in the event of product recalls related to safety risks. They may be required to apply age verification for age-restricted products and must be able to respond adequately to supervisory authorities and other competent bodies.

A customer account can serve as an important instrument in the careful and timely execution of these obligations. A stable and authenticated customer environment makes it possible to communicate in a targeted manner, trace purchases and identify affected customers more quickly. This enhances enforceability and reduces the risk that legal obligations are not fulfilled in a timely or complete manner. Without a structural link between customer and purchase, execution may become more complex in practice, potentially affecting the speed and effectiveness of compliance.

5. Different Business Models

Attention must also be given to the diverse business models in e-commerce practice, which extend beyond traditional webshops and online platforms. For example, several members of Thuiswinkel.org sell audiobooks and e-books outside of a subscription model.

After purchase, the customer may download the audiobook as a set of mp3 files via their account on the website. Such a set is offered as a ZIP file containing as many mp3 files as there are chapters in the audiobook.

In response to the argument that a mandatory account would not be necessary because download links could be sent by email, it should be noted that managing downloads via an account serves to prevent, or at least limit, the unauthorised forwarding of links in a proportionate and effective manner. In addition, a mandatory account prevents situations in which customers no longer have access to an email containing download links. Through the account, purchased audiobooks and corresponding download links remain accessible and can be downloaded again at any time.

Furthermore, most customers no longer download ZIP files but use a free mobile application. This app connects to the webshop and, after identification through login, recognises which purchases the customer has made. The specific app provides a digital bookshelf containing all audiobooks ever purchased by the customer. This functionality can only be realised if the customer can identify themselves, for which a mandatory account provides a simple, efficient and proportionate solution.

This practical example demonstrates that even in the case of a la carte sales, the account component may form part of the core of the service. Delivery does not end at payment but consists of continued access, the possibility to re-download purchases and usage via an app. A mandatory account also prevents download links from being easily forwarded and thereby supports a legitimate interest of the provider and of rights holders.

6. Conclusion

Thuiswinkel.org supports the objective of a high level of data protection and preventing unnecessary data processing. At the same time, we observe that the EDPB recommendations in certain respects take insufficient account of the freedom to conduct a business and the reality that many e-commerce services encompass more than a single purchase.

An account can in many cases be a legitimate and proportionate part of the service, for example for ongoing service provision, platform functionality, fraud prevention, product safety, warranty and the efficient exercise of rights. Many businesses in practice already choose to offer guest checkout. However, that choice should best remain with the entrepreneur, depending on the chosen business model and the design of the service. A generic obligation to always offer guest checkout goes further than necessary. Consumers retain the freedom to choose from which provider they purchase and under which conditions.

A generic preference for offering guest checkout may also lead to higher costs and, in practice, even more data processing due to repeated entry and verification.

Rather than structurally prioritising guest checkout, it would be more proportionate to focus on ensuring that account-based models are transparent, understandable and manageable for customers. Where an account

clearly indicates which data are processed for which purpose and allows customers to control their preferences, it can function as a tool for the customer rather than as a risk to privacy or security.

We therefore call for an approach that leaves room for different business models, with the assessment focusing on whether the processing of personal data is necessary within the chosen purpose and the chosen service, and on how transparency and security are ensured.