



Attorneys at Law
External Data Protection Officers

Title **Position Paper**

Public consultation on Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites, Version 1.0

Date Bonn, 11. February 2026

Authors Jenny Strauß, LL.M. (Information Technology Law)
Attorney at Law

Benedikt Schönbrunn, LL.M. (Information Technology Law)
Certified Specialist Lawyer (Information Technology Law)

Isabel Boymanns
Attorney at Law

Scheja & Partners GmbH & Co. KG
Adenauerallee 136 · 53113 Bonn · Germany
T +49 228 227 26-0 · F +49 228 227 26-26

www.scheja-partners.de

We welcome the initiative of the EDPB to provide controllers with recommendations on the processing of personal data with regard to user accounts on e-commerce websites.

In our opinion, the EDPB takes an overly strict view of accounts on e-commerce websites in some of the examples.

We would therefore welcome it if the EDPB took our position paper as an opportunity to take a differentiated view and, using specific and practical examples, show the limits according to which, in the EDPB's opinion, an user account can be legally created even without a guest mode. In particular, it would be helpful if the EDPB were to consider the possibility of a contract specifically covering the creation of a user account and the provision of certain account functions.

In our position paper, we focus on data processing within the scope of the GDPR and on some – in our view – practice-relevant aspects to be highlighted. The structure of our paper follows the recommendations and supplements them with our corresponding comments.

We consent to the publication of our statement.

2 General remarks

The risks and problems described in paragraphs 8, 11, 12, 13, and 14 share a common structural feature: the mandatory creation of a user account is implicitly understood as the starting point or trigger for a multitude of further data processing operations that are potentially prohibited or risky. This line of argument suggests that the creation of an account alone is the cause of the data protection issues described.

However, such a simplification is not convincing. The risks mentioned mainly concern subsequent or additional processing operations based on independent design and implementation decisions by the controller. The consequences described in the aforementioned paragraphs appear less as arguments against the legitimacy of account creation and more as general references to data protection obligations that must be complied with.

In detail:

Paragraph 8 correctly points out that the creation of user accounts may involve the long-term storage of personal data, which may give rise to risks with regard to data security and the principle of storage limitation. However, the risks mentioned, in particular the continued existence of inactive or “orphaned” user accounts and an increased vulnerability to unauthorised access, are not compelling or unavoidable consequences of account creation as such.

Rather, they are aspects of the proper design and management of user accounts, which fall within the responsibility of the e-merchant and can be addressed by appropriate technical and organisational measures. These include, in particular, clearly defined deletion concepts for inactive accounts, automated deletion periods, and appropriate security measures – which would have to exist for active accounts anyway. If such measures are consistently implemented, both the principle of storage limitation and the requirements for data security can be taken into account.

Paragraph 11 describes a number of abuse and security risks that may arise in connection with the use of user accounts, in particular when insecure authentication methods are used or passwords are reused. These risks are undeniable. However, the argument raises questions regarding the underlying standard applied to the data subject.

Insofar as the recommendations are based on the fact that users often reuse passwords, this is behavior that is usage-related and therefore beyond the immediate control of the controller. Although the controller can contribute to risk minimisation through appropriate technical and organisational measures (e.g., minimum requirements for password strength, two-factor authentication, alternative authentication methods), they cannot prevent users from using passwords that have already been used elsewhere.

Reusing passwords constitutes inattentive or security-ignorant user behaviour. It is questionable whether the underlying standard applied to the data subject should be based on such behaviour. Neither the GDPR nor the relevant case law suggest that the assessment of data protection risks should always be based on the most careless user imaginable. Rather, EU law in comparable contexts, particularly in consumer law, works with the concept of the average consumer, who is considered to be “reasonably well-informed and reasonably observant and circumspect” (e.g. CJEU, judgment of July 16, 1998, Case C-210/96, Gut Springenheide and Tusky, para. 31). Even if this concept has not been explicitly transferred to data protection law, there is much to suggest that the typological consideration of user behaviour should be based on an average, reasonable user and not on a standard that assumes a serious lack of knowledge of basic security risks.

The other risks mentioned in paragraph 11, such as compromised email accounts, represent general “digital” risks that are also not specifically caused by the obligation to create a user account. In this respect, too, these are less arguments against the legitimacy of user accounts than aspects that must be taken into account in their design and security.

Paragraph 12 refers, among other things, to the fact that logged-in user environments can make it easier for controllers to analyse usage and purchasing behaviour for commercial purposes, in particular commercial targeting.

However, these risks do not relate to the creation or existence of a user account as such, but to subsequent processing operations that must be assessed independently and that can be based on an appropriate legal basis.

The fact that user accounts can technically facilitate such processing is not in itself sufficient to raise data protection concerns regarding the obligation to create an account, as long as the respective processing operations are reviewed separately.

Paragraphs 13 and 14 point out that there is a risk that controllers may use so-called ‘deceptive designs’ to collect more personal data than is necessary for the specific ordering and delivery process, to obtain a “last-minute consent” in the order process for purposes other than managing the order or by promoting account confirmation in order confirmation emails.

These statements also do not concern account creation as such, but appear as examples of possible legal violations that should be avoided. They do not constitute an independent argument against the legitimacy of the mandatory creation of a user account. The decisive factor is whether the controller designs the account creation and the associated processing operations in such a way that they comply with the requirements of the GDPR. A controller who acts in compliance with data protection regulations can, for example, mark additional information as voluntary, refrain from any form of misleading presentation and ensure that there is a legal basis for data processing. The mere possibility of abusive or inadmissible implementation cannot in itself be sufficient to classify a user account as problematic under data protection law.

3.1 Performance of a contract under Article 6(1)(b) GDPR

We understand the EDPB's statement in paragraph 18 and footnote 13 to mean that the creation of a user account for accessing goods and services or purchasing them does not constitute a sufficiently specific purpose. The creation of such a customer account is therefore not an end purpose in itself. Rather, it is a processing step that serves another purpose.

The same applies, for example, to the collection of customer data entered in an online order form for the purpose of placing an order. The collection of data is not the specific purpose. It serves the purpose of entering into a contract with the customer. The conclusion of the contract serves the purpose of generating sales.

In parallel with this goal, an e-merchant may also want to increase its profits. To this end, it may pursue the purpose of offering its customers special opportunities when using its e-commerce website, which makes the sales experience as attractive as possible and thereby increase the number of contracts

concluded and the total revenue. An e-merchant can provide such functions by registering and providing an (online) user account.

In the examples in section 3.1 of its recommendations, the EDPB assumes contracts for the sale, purchase, and brokerage of goods and services. The creation and operation of a user account shall not be necessary for the fulfilment of such contracts.

In our opinion, this does not consider the possibility that the e-merchant may additionally conclude its own user agreement for the setup and provision of a user account for customers. The subject matter of the user agreement would then be the registration and access to the functions in the customer account that go beyond the mere purchase, sale, and brokerage of goods/services and enhance contract handling or new purchases.

In practice, many e-commerce websites allow users to register for a customer account without having to order anything at the same time. The actual order can be placed later. In practice, common functions of a customer account include wish lists for individual goods, pinboards for compiling various goods, communication with other e-commerce users, or personal order histories. Access to these functions is a service that is provided independently of a contract for goods, services, or brokerage and can therefore also be agreed upon. This is to be viewed separately from processing for the purpose of preparing and carrying out advertising (e.g., personalized suggestions, tracking across multiple online services, etc.).

In this respect, it is possible for a customer to enter into a user agreement on an e-commerce website for a user account with functions beyond the purchase process and then subsequently enter into a contract for the purchase, sale, or brokerage of goods and services.

The CJEU has ruled on the subject matter of a necessity test pursuant to Article 6 (1)(b) GDPR in the case of a contract involving several services to be provided independently of each other. Accordingly, the applicability of Article 6(1)(b) GDPR must be assessed separately for each service in a contract (CJEU, judgment of July 4, 2023, Case C-252/21, *Meta v. Bundeskartellamt*, para. 100).

Following these considerations, the at least two contracts—one for the user account and one for goods and services—must also be examined separately. Processing is only necessary for the performance of a contract if it is objectively indispensable to achieve a purpose that is an essential part of the contractual performance intended for the data subject. As quoted by the EDPB in paragraph 20 “the controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur” (CJEU, judgment of July 4, 2023, Case C-252/21, *Meta v. Bundeskartellamt*, para. 98). The subject matter of the user agreement is the creation of a user account and access to its functions. The subject matter of the agreements on goods and services is the delivery or provision of the service in return for payment.

In this respect, it would be helpful to have an assessment by the EDPB as to whether processing for the creation and operation of a user account with functions that are intended to enhance the purchase transaction and to simplify new purchases can be assessed as necessary for the performance of a corresponding user agreement in accordance with Article 6(1)(b) GDPR, irrespective of a subscription in receiving goods or services regularly (cf. next paragraph).

3.1.2 Subscriptions

The examples given in paragraphs 26, 28 and 29 are intended to illustrate the conditions under which the mandatory creation of a user account can be considered necessary for the performance of a contract within the meaning of Article 6(1)(b) GDPR or not. However, taken as a whole, these examples raise questions regarding the consistency of the underlying criteria for differentiation.

In **paragraph 26 Example 2**, it is stated that the creation of a user account in a subscription-based business model can be considered necessary for the performance of the contract within the meaning of Article 6(1)(b) GDPR, as the account is used for “follow their packages, communicate with the e-merchant or make changes to the delivery conditions”.

At the same time, this example raises questions of demarcation, as the functions mentioned – in particular shipment tracking, communication with the retailer or changes to delivery terms – are **not specific to subscription relationships**. Comparable needs may also arise in one-off sales contracts, for example in the event of delivery delays, delivery problems or subsequent adjustments to the delivery address.

This lack of clarity is particularly evident in conjunction with the later statements in paragraphs 39 and 40. These emphasize that after-sales services may be provided without the requirement to create an online user account. The mentioned after-sales services should be implemented, for example, through secure online forms, contacting customer service, or by providing the customer with a specific hyperlink via email that allows the controller to automatically respond to queries. The question here is why these after-sales services should be assessed differently from the services mentioned in paragraph 26. Shipment tracking, communication with the retailer, or changes to delivery terms can also be implemented using the measures mentioned in paragraph 40 (e.g., contacting customer service).

Against this background, it remains unclear which **specific distinguishing criterion** should be decisive for assuming the necessity of a user account. Without such clarification, there is a risk that functionally comparable scenarios will be assessed differently, even though they are subject to the same standards under data protection law.

3.1.3 Access to exclusive offer

Paragraph 28 states that access to exclusive offers can only be considered necessary for the performance of the contract within the meaning of Article 6(1)(b) GDPR if the offer actually is not open for everyone. If exclusive offers are accessible to all interested parties simply by creating a user account, the EDPB denies the necessity of creating an account and does not classify the model as a ‘closed community’.

However, this argument raises fundamental questions about freedom of contract and the definition of the business model. The assumption that an offer loses its exclusivity as soon as there are no further access requirements other than the creation of a user account does not appear compelling. Even a business model that links access to certain services or price advantages to prior registration can be deliberately designed to be exclusive, even if this registration is open to everyone in principle. In this case, exclusivity does not lie in personal characteristics or barriers to access, but in the contractual structure of the offer.

Furthermore, it remains unclear what practical consequences are to result from the classification described above. If the creation of a user account in such constellations is not considered necessary within the meaning of Article 6(1)(b) GDPR, the question arises as to the legal basis on which the account should be created instead. Recourse to consent pursuant to Article 6(1)(a) GDPR appears problematic, as account creation in this model is a prerequisite for access to the offer and thus the voluntary nature of the consent may be called into question.

Paragraph 28 leaves open how to assess situations in which a e-merchant deliberately opens its web shop or certain areas of its offering exclusively to registered users without providing for any further access criteria. In such cases, the contract is concluded precisely on the condition that a user account

exists. The blanket rejection of the necessity of creating an account in these cases contradicts permissible business models and also the freedom of contract of the parties.

Paragraph 29 Example 4 states that the creation of a user account for participation in an online event with early access to selected products can be considered necessary for the performance of a contract within the meaning of Article 6(1)(b) GDPR, provided that participation is limited to loyal customers with a long-term business relationship. This classification raises several questions of demarcation.

It should be noted that the online event described is a one-off or time-limited offer. This circumstance alone does not automatically necessitate the creation of a user account. Access to such an event could also be achieved through other, less intrusive mechanisms, such as individual access codes, time-limited links or comparable access criteria. Therefore, it remains unclear why the creation of a user account is considered objectively necessary.

It is also unclear which contract should be decisive here, legitimizing the creation of a user account as necessary data processing. **In paragraph 30**, the EDPB states that it must be a contract whose main subject matter is registration within the community.

It would be helpful if the EDPB clarified whether this could be a previously concluded contract for goods and services – that also stipulates registration to a community – , or a new contract for registration for the event.

3.3 Legitimate interest under Article 6(1)(f) GDPR

The arguments put forward in **paragraphs 54, 55, 59, 64 and 67** regarding Article 6(1)(f) GDPR are based largely on the criterion of the ‘reasonable expectations’ of the data subjects. Overall, it is apparent that the criterion of ‘reasonable expectations’ is not applied consistently throughout the aforementioned paragraphs. Without a clearer definition of the underlying standard, there is a risk that predictability will be used as a flexible argument without providing sufficiently predictable criteria for practice.

First of all, it seems questionable whether the predictability of account creation can actually be determined in the manner suggested in paragraphs 54 and 55 in particular. The assumption that individuals do not regularly expect to create a user account for one-off purchases is only partially consistent with current market practices in e-commerce. Rather, a significant proportion of users are likely to be familiar with the fact that access to certain functions or even the completion of a purchase may be linked to registration. Against this background, the criterion of predictability proves to be **vague and highly context-dependent**, without it being clear what standard is used as a basis for this.

This is also evident when comparing paragraphs 54 and 55. While paragraph 54 denies the predictability of account creation for open offers, paragraph 55 affirms it for offers with special access requirements (e.g. recommendations by other members). This differentiation is not immediately convincing. Even in such cases, alternative access concepts are conceivable, such as time-limited access codes or online forms (see e.g. para. 33), without necessarily requiring a permanent user account. The predictability of account creation is thus linked to the form of the offer, without it being clear why this form alone should be decisive.

Similar demarcation problems arise in paragraph 59. There, it is stated that although the option to change orders after payment has been received as user-friendly, a user account is not necessary for this, as alternative solutions are conceivable. This argument conflicts with other passages in the recommendations, in which comparable functions – such as changing delivery details or communicating

with the retailer – are used as examples for the necessity of a user account depending on the relationship between customer and e-merchant (see e.g. para. 26). The mere existence of alternative technical solutions is sometimes considered decisive here, sometimes not, without it being clear when this criterion should be decisive.

Finally, paragraph 64 makes it clear that personalised content and customer loyalty cannot be expected without further ado and generally require an active decision on the part of the data subject. However, this is not directed against the existence of a user account as such, but against certain subsequent processing, such as tracking. Here, too, it is clear that the predictability of individual processing operations cannot automatically be transferred to the predictability of account creation as a whole.

The same applies to the considerations in paragraph 67 on storage limitation. The assumption that data subjects do not expect their data to be stored for longer than is necessary for the performance of the contract at the time of purchase, only contributes to the assessment of account creation if this storage takes place without transparency or contrary to clear information. If the creation of the account is communicated openly and it is apparent to the data subject during the ordering process that a user account is being created, this does not constitute covert or surprising processing, but rather a conscious decision within the purchase process to create a account.

3.3.3 Fraud prevention

Insofar as **paragraph 74** requires a balancing of interests to be carried out within the framework of the legitimate interest pursuant to Article 6(1)(f) GDPR on the premise that mandatory account creation per se interferes with the rights and freedoms of the data subjects, this assumption is too narrow and remains general. It does not sufficiently take into account that authenticated user interaction regularly creates a higher barrier to identity theft, abuse, and unauthorized use. The creation of a user account can – especially if the authentication and security mechanisms are appropriately designed – help to prevent fraud, unauthorized access, or multiple use. Thus, the creation of an account does not necessarily infringe on fundamental rights, but can, on the contrary, serve to protect the data subjects themselves. Therefore, any security and prevention aspects in favour of the data subjects must be taken into account in the balancing of interests.

The assumption in **paragraph 75** that the balancing of interests in connection with mandatory account creation regularly works to the detriment of the controller does not appear to be compelling or required by EU law. Such a generalised prediction runs the risk of effectively undermining the open balancing mechanism of Article 6(1)(f) GDPR.

Instead of a blanket assumption of a regularly negative outcome of the balancing of interests, it seems more appropriate to recognize positive outcomes of the balancing of interests where the account requirement contributes to risk minimization, for example in the case of services with an increased potential for abuse, sensitive communication or transaction processes, or offers where the integrity of the user identity itself is a central protected interest. In such cases, the balancing of interests may be in favour of the controller without disproportionately affecting the rights and freedoms of the data subjects.

4.1 Data processing operations enabled by offering a choice

The EDPB's comments in section 4 lack clear criteria for distinguishing between the legality of voluntary user accounts and their individual functions. Although the wording suggests that consent is not the only

possible legal basis, it remains unclear how this can be applied in practice if individual account functions are assumed to have their own purposes and different legal bases, even though they are part of the same user account. It also remains unclear how an offered guest mode affects the previously expressed doubts about the necessity assessment under Article 6(1)(b) and (f) GDPR.

These open questions will be examined in more detail below:

Paragraph 80 states that certain purposes must first be defined for both guest mode and voluntary user accounts in order to determine their legality. Examples include the execution of the purchase contract on the basis of Article 6 (1)(b) GDPR and marketing processing on the basis of consent pursuant to Article 6 (1)(a) GDPR. However, these statements relate to subsequent processing and leave open the question of how the processing operations for the creation and operation of a voluntary user account as such are to be classified legally.

Paragraph 81 specifies that **each individual function** of the account is to be understood as an additional service and requires an independent examination of its legal basis depending on the purpose of the function. The wording in paragraph 81 “*where such a service is based on the data subject's consent*” suggests that the EDPB **does not assume that all account functions must necessarily be based on consent**. Rather, it seems to be recognized that, depending on the purpose, different legal bases may be considered for each function. The obligation to clearly separate the purchase process is explicitly emphasized only for services based on consent, but not across the board for all components of a voluntary user account.

In practice, this may mean that individual functions of a user account are based on a legitimate interest pursuant to Article 6 (1)(f) GDPR or on the performance of a contract pursuant to Article 6 (1)(b) GDPR, while consent pursuant to Article 6 (1)(a) GDPR is required for other functions. Against this background, there is a considerable practical challenge in how controllers can design consents and contractual provisions for individual functions in a uniform user account in such a way that they are transparent, differentiated, and permissible under EU law. These practical considerations make it necessary to clearly differentiate between functions requiring consent and those not requiring consent within a user account and to present this distinction in a way that is comprehensible to the data subjects.

In this respect, clarification by the EDPB would be welcome as to the criteria for distinguishing between account functions that require consent and those that do not. This includes an explanation of the extent to which, in the opinion of the EDPB, Article 6(1)(b) or (f) can be considered as alternative legal bases for the creation and operation of the voluntary user account and its functions. It would also be welcome to see what controllers should bear in mind when designing a user account with functions based on different legal bases in a data protection-friendly manner. It would be particularly interesting to see the EDPB discuss whether functions that serve to enhance orders or order management can be assigned to one purpose (e.g. Provision of functions for enhancing the purchasing process as the subject matter of a contract). This would reduce the number of purposes and legal bases and thus the complexity of the arrangements for justifying processing in connection with the provision of functions.

Furthermore, the explanations in section 4 do not clarify the extent to which the offer of a guest mode influences the legal assessment of the voluntary user account. Section 3 explains why a mandatory account generally results in a negative outcome of the necessity tests within the framework of an assessment pursuant to Article 6 (1)(b) or (f) GDPR. With regard to contract performance as a possible legal basis, Section 4 does not mention any separate contract for the voluntary user account. This would leave only contracts for goods and services. As explained by the EDPB in its examples under Section 3, the voluntary user account is still not necessary for the performance of these contracts. This is even more true if it is possible to order in guest mode as an alternative. This raises the question of which

contract should be considered from the EDPB's perspective when assessing the necessity of functions within a voluntary user account.

In this respect, clarification would be helpful as to how guest mode (positively) affects the necessity tests pursuant to Article 6(1)(b) and (f) GDPR. This includes clarifying which contract should be decisive for assessing the applicability of Article 6(1)(b) GDPR – the contract for the goods or services or a contract for the provision of the voluntary user account and its functions.

4.2 Giving the user a choice: data protection by default and by design

Paragraph 84 describes that users can be informed that a purchase as a guest only enables the fulfilment of the sales contract, while the creation of a user account can offer an 'improved service', for example through facilitated subsequent purchases, loyalty programs, special offers. This is presented as permissible information about different scopes of services.

However, this argument raises questions with regard to the voluntary nature of account creation. The comparison of a purely functional guest purchase with an 'improved' service for registered users does not merely represent neutral information, but can also be understood as targeted steering of the decision. In particular, the qualitative assessment as 'improved service' implies an added value that is suitable to motivate the user to create an account.

Against this background, the question arises as to what extent such a presentation is still compatible with the requirement of voluntariness, especially if the account creation is to be based on consent. Does emphasising an 'improved' service here not in fact create pressure that can impair the user's freedom of choice, especially if the guest purchase is deliberately limited to a minimum of functions?

It is also striking that paragraph 84 apparently regards such influence as unproblematic, while in paragraph 81 high demands are placed on voluntariness and the avoidance of disadvantages for non-registered users. This different assessment suggests that the EDPB does not formulate clear criteria between permissible information and unauthorised influence. A more precise demarcation would be helpful to enable controllers to design such information on functions of a voluntary user account in a legally compliant manner.