CHAMBER OF DIGITAL ECONOMY

Position of Chamber of Digital Economy on
Recommendations 2/2025
on the legal basis for requiring
the creation of user accounts
on e-commerce websites
Version 1.0
Adopted on 3 December 2025

The consequences and arguments presented in the "Commentary" column regarding the EDPB recommendations on the mandatory creation of accounts can be summarized in the following points:

1. **Restriction of freedom of business activity and the principle of proportionality**: The imposition of an obligation to offer a "guest checkout" option is perceived as a restriction of contractual freedom and the freedom to conduct a business, which does not satisfy the proportionality test and should be regulated at the legislative level, rather than through guidelines. The GDPR does not contain any provision imposing an obligation on controllers to offer a "guest" option. Moreover, the EU legislator has not decided to introduce such an obligation in any of the recent regulations concerning electronic commerce, in particular the Digital Services Act, nor in the course of the reform of consumer law carried out by Directive (EU) 2019/2161 of the European Parliament and of the Council.

   The EDPB guidelines effectively create new legal obligations, which go beyond their interpretative powers. Furthermore, such action constitutes an interference with the freedom to conduct a business protected by the Charter of Fundamental Rights of the European Union, as it interferes with the freedom to decide on the adopted business model. Measures of this kind may only be introduced by way of legislation. The EDPB guidelines disregard not only the Charter of Fundamental Rights of the European Union, but also the very objective of the GDPR, as emphasised in Recital 4 thereof.

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

The EDPB indicates that the requirement to create user accounts may be justified only in relation to a "very limited, though non-exhaustive set of purposes." The use of the term "non-exhaustive" while simultaneously recommending restrictions on business practices leads to legal uncertainty.

2. **Legal bases for the creation of online user account**

Within the freedom to conduct a business, an entrepreneur may offer a consumer the conclusion of a separate agreement for the creation and maintenance of an online user account in an e-store or on an online platform. Such an agreement, distinct from the distance sales contract, is valid under national civil law and entails specific obligations on the part of the entrepreneur, including enabling access and providing account-related functionalities.

The performance of an account agreement necessarily requires the processing of personal data; therefore, where such an agreement has been validly concluded, Article 6(1)(b) GDPR constitutes the appropriate legal basis for the processing of personal data for its performance. The GDPR does not empower the EDPB to question the admissibility or validity of account agreements as such, nor do Articles 5(1)(a) or 6(1)(b) GDPR provide grounds to undermine the principle of freedom of contract or to impose an obligation to offer purchases in a "guest" mode.

The choice of whether to base a service model on user accounts remains an element of the entrepreneur's autonomous business decision, which may be restricted only by law and in compliance with the principle of proportionality.

3. **Doubts regarding security and data retention:**

   a. Impossibility of achieving greater security by introducing the guest option: Purchases without an account do not lead to a shorter data retention period, as the longest storage duration is often enforced by law (e.g., tax purposes: 6 years, DAC7: 5 years, VAT e-commerce: 10 years).

   b. Account provides a higher level of security: The account infrastructure compels better protection (detection of suspicious logins/activity, informing about leaks), which "guest" purchases do not offer. The "guest" model leaves the user "on their own" and may be more susceptible to phishing attacks.

c. Post-purchase management: Suggestion of use of "hyperlinks" (in the case of guest purchases) is highly susceptible to hacker attacks, does not allow for user verification, and prevents the platform from controlling data security to the same extent as an account.

d. For platforms operating in regulated sectors, including online trading platforms, an account-based model enables effective compliance with security requirements arising from other EU legal frameworks, such as DORA and NIS2. In a “guest” model, administrators are unable to reliably verify user identity or implement strong authentication mechanisms, including two-factor authentication. An account-based model, in turn, significantly facilitates the detection, analysis, and monitoring of security incidents and breaches.

4. **Risk of economic regression and ignoring customer convenience**:

e. Convenience as a market standard: Treating convenience (e.g., easy shipment tracking) as "unnecessary" for contract performance leads to "economic regression," as these features have become a market standard expected by customers.

f. Order tracking and communication: Customers expect convenient order tracking through an account. Relying on suggested email notifications is outdated, generates costs/traffic, and limits the ability to change the delivery address/date.

5. **Limitations on business models and market fragmentation**:

g. Denying the ability to limit access to exclusive offers or services (e.g., loyalty programs, insurance) only to account users is seen as a misunderstanding of how business works and prevents the offering of a full service package.

h. Granting local data protection officers the authority to assess and decide on business models would cause huge fragmentation of approaches across Europe.

i. Implementing both the “with account” and “without account” models simultaneously entails the costs of duplicate infrastructure (development and maintenance of two paths, security testing of two paths, additional responsibilities for customer service employees). This affects customers (price increases) and promotes larger entities that can cope with such costs, and may eliminate smaller ones.

6. Impossibility of applying to complex marketplaces: The guidelines focus on "per process" recommendations and offer no suggestions for how complex platforms and marketplaces, where the entire service is a package of connected functionalities, should operate. Consequently, this may lead to a "chilling effect" and hinder the

development of e-commerce services.	
EDPB - recommendation on mandatory creation of accounts	Commentary
General remarks	According to Article 16 of the Charter of Fundamental Rights of the European Union, business activity is a fully recognized freedom protected by the Charter. According to Article 52 of the Charter, any limitations of protected freedoms shall be provided for by “law” and respect the essence of those rights and freedoms, subject to the principle of proportionality. By “law” in this context cannot mean “Guidelines” because of the hierarchy of legal acts; in other words, simple guidelines cannot shape the freedoms from the Charter, and the intervention on the legislative level is the minimum. Moreover, guidelines which impose a factual obligation to provide for "guest" options (additionally in very blurred and unclear situations) do not meet the proportionality test and limit contractual freedom. They create a wide and unclear field for interpretation, and give data protection offices the “unwritten” and in fact highly discretionary authority to assess and decide in which cases the entrepreneurs should apply the “guest” option. The recommendations also disregard Recital 4 of the GDPR, which clearly states that the right to the protection of personal data is not an absolute right and must be considered in relation to its social function and balanced against other fundamental rights in accordance with the principle of proportionality. That recital further confirms that the GDPR does not undermine, inter alia, the freedom to conduct a business as

	enshrined in the Charter. The recommendations fail to take this recital into account, even though they lead to serious interference with the freedom to conduct a business, as they effectively determine which business model an entrepreneur should implement, leaving no room for an autonomous decision that takes into account the conditions relevant to the specific economic activity. Moreover, when registering an account, many platforms have limited the amount of data required (email and password) to a minimum. At the same time, in many online stores, customers provide significantly more data when making purchases as a guest.
Legal bases for imposing the creation of online user accounts under Article 6 GDPR	Within the scope of decision-making freedom resulting from the freedom to conduct a business, an entrepreneur may offer a consumer the conclusion of an agreement for the creation of an account in an online store or on an online platform. Such an agreement provides, inter alia, for the entrepreneur's obligations to enable logging in and to ensure access to the functionalities forming part of the account. This agreement is separate from the distance sales contract. An agreement for maintaining a user account is valid, as it is based on the declarations of intent of both parties. The performance of an account maintenance agreement necessarily requires the processing of the consumer's personal data; therefore, where a valid agreement for maintaining an account in an online store or on a platform has been concluded, the legal basis for the processing of personal data for the purposes of performing that agreement is Article 6(1)(b) GDPR. The EDPB does not analyse this circumstance, focusing instead on specific individual situations. In order to conclude that Article 6(1)(b)

	GDPR cannot apply, it would be necessary to challenge the admissibility of concluding an agreement for maintaining a user account as such. The GDPR does not confer such competence on the EDPB, as it does not regulate the validity or effectiveness of contracts. These matters are governed by national civil law of Member States. Neither Article 5(1)(a) GDPR nor Article 6(1)(b) GDPR constitute provisions that allow for undermining the principle of freedom of contract. No conclusion can be drawn from them as to the inadmissibility of concluding an agreement for maintaining a user account in an online store or on an online platform. Nor do they provide a legal basis for imposing an obligation to offer purchases in a guest mode without concluding an account maintenance agreement. This remains an element of the entrepreneur's autonomous business decision, grounded in the freedom to conduct a business. That freedom may be restricted only by law and in compliance with the principle of proportionality.
(7) Firstly, requiring the creation of online user accounts may encourage the development of logged-in environments where data subjects are systematically identified in order to complete actions,	Account creation is accompanied by better data security connected with multi-layered security measures protecting the account. The creation of the account is accompanied by greater convenience, which should not be treated as a threat or a fact which has negative consequences, or should be treated as "bad". Economic progress is strictly connected with the constant improvement of services or products, including e.g. user convenience. Taking into account users'convenience it is worth mentioning that they often log in via social media or other online platforms (Google, Facebook, AppleID), which significantly speeds up the registration/login process and is popular with users, especially younger generations. Shopping as a

	guest does not offer such possibilities.
(8) Secondly, while online accounts can simplify purchases, they also entail the retention of personal data on an active database for a period of time longer than what is strictly necessary for the purchase and delivery of the order.	This is a big simplification because purchase data are stored for various purposes, and quite often the longest duration of storage is forced by the provisions of law e.g.: - tax purposes 6 years - DAC7 purposes 5 years - VAT e-commerce- 10 years It is not the creation of an account that affects longer data processing, but various legal requirements and needs, which cannot be limited to “purchase and delivery”.
(8), second bullet) The second consequence is that the personal data stored in an active database for a longer period than what is necessary are more vulnerable to unauthorised access or other security risks, as unmanaged accounts or “orphaned accounts” are more exposed to attackers	Longer retention results from various purposes (see above), and such purposes (e.g., legal obligations) are applicable both for “account” purchases and “guest” purchases. So, having no account will not change it. The fact is that an organized infrastructure of the account-based environment forces better protection because security is often a crucial factor of commercial attractiveness of the platform. The fact is that “guest” purchases also require the creation of internal management infrastructure, e.g., for tax accountability. This infrastructure is not visible to users, but it exists and is obvious, so the assumption **that if we impose restrictions on creation of accounts, we will achieve shorter retention periods is false.**

(9) The risk of receiving a deceptive link by malicious actors seeking to spread malware or ask for sensitive information exists both in cases where the data subject has created an account or not.	Attacks based on deceptive links or similar techniques are based on human misperception (human mistake). There is no possibility to create safety on the max. 100% level, but in case of accounts e.g.: - we are able to detect suspicious login - we are able to detect suspicious activity on the account/ payment - we are obliged to track newest vector attracts and implement remedies - we are able to scan and detect data leaks and inform users All these examples of actions would not be possible for “guest” purchases. Moreover “guest” purchases can also be used as a vector of attacks (phishing + fake link to fake website), but in this case it is the user who is basically left alone and in fact everything depends on his/her awareness.
(12)Thirdly, logged-in environments also make it easier for the controller to log browsing history and track the browsing habits of users in order to improve possible commercial targeting, especially by combining personal data collected in different purchasing channels. Without a proper legal basis, this would result in a breach of the GDPR.	Non logged users can also be tracked easily, so there is no cause-effect relation.
(20) The controller must also ensure that there	This logic leads to doubtful conclusions, e.g., the controller should

is no workable, less intrusive processing of personal data to perform the contract	always have a cash payment option (cash on delivery), because cash is basically always “workable” and electronic payment is “more intrusive” because it always requires more data than a cash payment. But does it mean that e-commerce should by default have a cash option? No. The “necessity” should be interpreted very closely to Recital 2 of the GDPR and the assumption that the GDPR should support progress. Article 6(1)(b) cannot be reduced to objective necessity, because such a logic will always lean towards economic regression. This is due to the fact that many improvements and, generally speaking, progress in the field of e-commerce activity are in fact more “enhancements” than objectively necessary features. But these “enhancements” become a market standard, which is expected by the customers who always choose more convenient options than the really necessary ones.
(22) As regards the one-time sale of a good or service, the personal data necessary for the execution of the sales contract and the management of the order can be collected without requiring the creation of an online user account.	The one-time sale problem is not a problem of privacy, but a problem of the business model. There are models where one-time sale is desired, because the sale model is focused on client loyalty, which cannot be considered a violation of anyone’s right; it is just a business idea. There are mixed models where both account and guest purchases are welcome, and it is also a business decision. It is not clear why the choice of the customer, who can decide whether to buy as a guest from platform A or to create the account on platform B, should be additionally supported by a legal obligation. It also affects the freedom of business activity without real cause, because all risks described in “2 General remarks” are not specific to the account model and also occur in the “guest” model.

	Any limitation of business activity, including the imposing of strict expectations, should have a justification and be proportionate. We do not observe the problem of limited options for the customers, so they are not in fact forced to create accounts due to the lack of alternatives. Both big and medium/small players apply various models, so if anyone wants to buy something as a “guest,” it is very easy to find a good offer.
3.1.3 Access to exclusive offers	This is a big misunderstanding of how the business works. 1) Basically it is not possible to create, offer, or adjust any incentives without the account structure. In order to show a good offer, the platform should have the possibility to communicate. Without the account, it is generally very limited because clients usually do not subscribe to marketing emails. In the case of the account, there are some options to display offers and additional service in the account. 2) Without the account, the client cannot manage the services/offers. Clients like and expect to have easy access to management panels, to enable/disable options, etc. 3) Many platforms offer a full scope of additional features (e.g., delivery tracking and management, insurance, special programmes, discount systems, withdrawal from the agreement is much simpler etc.) and they often go as a full package, which cannot have a legal basis other than letter “b.” 4) The officer should not have the authority to decide whether offer A shall be available for guest purchases and offer B can be limited to the account models. It is not only a clear breach from the fundamental rights perspective, but also a clear recipe for huge fragmentation of approaches along the whole of Europe. Each country and each nation has its own specific shopping habits,

	and giving the local Data Protection Officers the authority to assess and decide on the business models would cause more problems.
3.1.4 Conditional purchasing	This is a big misunderstanding of how the business works. All situations where special conditions must be met usually require an account. The example of a student is a very good illustration of how many important aspects are not mentioned in the justification, including the proposal “a secure online form allowing a collection of data to verify the status of a user.” 1. The most secure options are “own” options, which are known by the controller. The idea of an online form may be good for the collection of e-mails for a webinar, but not for student status verification where often more data are necessary. What is the difference between the creation of a secure account and the creation of a “secure form”? 2. One-time verification is useless because it must be repeated. Clients do not like repetitive verification, and it discourages them from engagement. 3. Each verification is a moment when something can happen (fault, mistake, or even attack); that is why the best option is to do it as rarely as possible. In the case of repetitive verification, the threat will also be repetitive. 4. After verification of the student status, these data must be stored until the status expires. Why shouldn't the controller store it within the account when, in the case of guest verification, the status must be stored anyway?

	5. The account supports the collection and processing of data in one “place,” when “guest” options support more scattered forms, which are not safer. There is also a third option: that the controller should offer a "guest" option, but in the backend must store the whole bunch of data on the user, which would not be visible, as is the case with the existence of an account. The case of “student” is only an example, but very illustrative, showing that the “guest verification” is not a solution and, moreover, it is connected with more serious security issues.
After-sales services and exercise of rights	In the current state, as things stand on the market, and taking into consideration customers' expectations, the proposal, where we should use "hyperlinks," does not solve any issues and creates additional complexity. 1. The account allows you to manage purchases freely. It is definitely a more convenient option because clients can see purchases on the dashboard. 2. In order to manage purchases, the client has to log in to the store = additional security. 3. The use of separated “hyperlinks” for the guest purchase requires the creation of a network/infrastructure very similar to the account, especially when the same user repeats purchases. Eventually, we’ll have a situation where a similar amount of data is stored and processed both in case of “account” and in case of “guest.” The difference lies only in the fact that the account allows the user for management, and guest requires “hyperlink logic.”

	4. “Hyperlink” logic is very susceptible to hacker attacks, so it has no positive impact on security. 5. In the case of “clicking” the link, we cannot always be sure that the right person contacts us, especially in times where a constant log-in session on popular e-mail providers is a standard. 6. In case of the “clicking the link” logic, e-commerce platforms will have no options other than to execute the demand, including GDPR demands. In case of the account, platforms have options such as detection of suspicious traffic, detection of account breach, or data leak, etc. In the case of the “link,” it would not be possible. However, the e-commerce business is very prone to losing trust, so in the long term, they prefer to have more control over data security, rather than saying that the user is irresponsible for their own security. 7. Again, the convenience connected with the account cannot be treated as “unnecessary” for the contract performance. Such a logic raises further questions, e.g., is the “guest” purchase also a “necessary” option, because a phone order with cash on delivery options would be even less intrusive? We need to assess necessity in close connection with the current market state and current habits of users.
(54) Example 6: An individual wishes to buy an item on a retailer’s website. The individual is only interested in purchasing the item and has no intention to develop a longterm relationship	The individual should have the option to find alternative suppliers, so it is more a question of fair and balanced competition. The model of business activity which would rely on individual wishes assessed by the data protection organs - that's an impossible demand.

with the e-merchant beyond this purchase. In this case, the processing involved in a required account creation may not be expected.	
(58) Therefore, provided that the pursuit of a legitimate interest by the controller or by a third party has been complied with, controllers should not rely on Article 6(1)(f) GDPR to justify the requirement to create an account for the purposes of tracking an order. This is because the “necessity” and “balancing” tests required for the application of this legal basis are unlikely to be met.	Customers reasonably expect that the tracking will be easy and convenient. They do not want to contact the platform to ask where the parcel is. Relying on email notification takes us back to the 2000s. Individuals already receive hundreds of mails, and they are overwhelmed. In case of users who are very active, e.g., 30 purchases a month, this is equal to approx. 100 e-mail notifications per user, which means cost and traffic. In case of “e-mail” notification, the possibility to change delivery address, to change delivery date, etc., is rather not possible; this is very easy from the account perspective.
The problem of cumulative purposes in complex platforms and marketplaces.	Guidelines give recommendations “per” process but give no suggestions as to how complex platforms (marketplaces) act when the whole service consists of a package of connected functionalities, benefits, or options, which are often treated as a must in the current market circumstances, constant competition pressure, and it is also treated as a more attractive option for customers. In this situation, offering advanced services whose legal basis is uncertain, diversified, and which, according to the guide, cannot be safely offered as “performance of a contract,” may result in the so-called chilling effect and, in the long term, will hamper the development of e-commerce services. Moreover, in the case of mobile applications, creating an account in order to make purchases is standard practice and, in our opinion, meets market/customer expectations.

	What works in a regular e-store will not work in a multi-service platform.
4.2. data protection by default and by design	The recommendations indicate that the “guest” model is more compliant with Article 25 of the GDPR (privacy by design and by default). Meanwhile, Article 25 of the GDPR in conjunction with Article 5(1)(f) of the GDPR requires the implementation of measures to ensure, among other things, the integrity and confidentiality of data - the account model provides better opportunities to achieve this goal through multi-factor authentication, monitoring of suspicious activity, and access control. The “guest” model can lead to data fragmentation—the same personal data stored in different systems for each transaction. The account model forces data consolidation, which implements the principle of minimization.