Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites

Version 1.0

Adopted on 03 December 2025

Executive summary

On e-commerce websites, users are frequently required to create an online account before being able to access offers or purchase goods and services. Controllers generally justify the imposition of account creation for several reasons, such as to perform a sale, enable the subscription to services, grant access to exclusive offers to their users or facilitate the operational management of orders.

While controllers in the e-commerce sector may have a commercial interest to require users to set up an account, the EDPB notes that such account creation may also expose data subjects to additional risks to their rights and freedoms.

In this document, the EDPB provides recommendations to the controllers operating in the e-commerce sector on the conditions under which they may lawfully require their users to create an account under Articles 5(1)(a) and 6 GDPR. In particular, these recommendations set out examples of situations in which mandatory creation of an account may or may not be necessary for the performance of a contract (Article 6(1)(b) GDPR), for compliance with a legal obligation to which the controller is subject (Article 6(1)(c) GDPR), or for the purpose of a legitimate interest pursued by the controller or a third party (Article 6(1)(f)) GDPR).

Following the analysis of various use cases, the EDPB finds that imposing the creation of an online user account can be justified only for a very limited - though non-exhaustive - set of purposes, such as offering a subscription service or providing access to exclusive offers. However, in several other use cases assessed in these recommendations, the imposition of the creation of an account on e-commerce websites does not comply with the conditions for lawful processing under Article 6(1)(b), (c), or (f) GDPR.

In these latter cases, the EDPB concludes that offering users the option to either set up an account or continue browsing and purchasing as a guest appears to be the most efficient way for personal data to be processed on e-commerce websites. The EDPB notes that this "guest" mode is, in principle, the most privacy-protective option to enable purchases, in line with the obligation of data protection by design and by default under Article 25 GDPR.

Table of Contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Has adopted the following Recommendations:

1 Introduction

1 Many websites require users to create an online account, either to access offers or make purchases. As this practice is particularly widespread in the e-commerce sector, these recommendations aim to clarify the conditions under which controllers may lawfully require their users to create an account for the purchase of goods and services online, and to guarantee a homogeneous protection of data subjects' rights, as required by the GDPR.

2 For the purpose of these recommendations, an "online user account" is a personal online space assigned to a user, or several users using different profiles, and accessible by an authentication mechanism using an identifier and a password[2]. For the sake of clarity, this definition does not include personal online spaces which are temporarily accessible with temporary access tokens and do not require a password. Online user accounts are usually proposed by e-commerce companies to users before browsing a website or making a purchase. The creation of an online user account requires the user to provide information that will be used as a unique identifier (such as an e-mail address).

3 These recommendations are relevant for e-commerce websites[3], including e-commerce platforms acting as intermediaries between professional merchants and consumers, such as online marketplaces. Online platform services which connect individuals with each other in a non-professional capacity for the purpose of selling products or providing services, social media services, including social media marketplaces, online search engines services, online software applications services, audio-visual media services and online news websites are excluded from these recommendations.

4 The scope of these recommendations comprises the data-protection-related aspects of the relationship between e-merchants and consumers, in particular as regards the creation of online user accounts, to the extent that the relevant processing activities fall under the territorial scope of application of the GDPR4. For the purpose of these recommendations, an

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[2] For sake of clarity, this definition includes personal online spaces requiring a multifactor authentication.

[3] Reference to "e-commerce websites" in these recommendations includes e-commerce websites, web applications and mobile applications.

[4] Article 3 GDPR, as construed in Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, adopted on 7 January 2020.

"e-merchant" refers to a person or entity that buys, sells or brokers products or services for profit on an e-commerce website.

5 These recommendations are without prejudice to any MS or EU law requiring the mandatory creation of accounts for products and services subject to specific regulations, (e.g. alcohol, gambling or pharmaceuticals).

2 General remarks

6 When requiring the creation of an online user account to access offers or to make purchases, data subjects may be exposed to additional risks to their rights and freedoms.

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, including purchases or accessing content. This may result in a greater amount of data being collected and processed regarding the data subject, including data collected directly from the data subject and data produced or inferred by the controller.

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. The storage of such data has two possible consequences:

- The first consequence is that, unless data subjects ask for the erasure of their data pursuant to Article 17 GDPR, users' personal data tend to be stored by the controller even if their accounts have not been used for a long time or will never be used again. Such practice would not be in line with the principle of storage limitation under Article 5(1)(e) GDPR.
- 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[5].

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. Moreover, users may expect to receive a link from a controller with whom they have an account, and may be more prone to clicking on a deceptive link that appears to have been sent by that controller. Therefore, using one-time links sent via email or SMS as an alternative to account creation would not introduce additional security risks for data subjects. In all cases, the EDPB recalls that it is the responsibility of the controller to take the appropriate technical and organisational measures to mitigate these risks[6].

10 In addition, the process of creating an account in itself does not prevent malicious bots operated by scalpers from abusing the purchase function to acquire a large proportion of a

[5] The longer personal data are stored in an active database, the greater the risk of a data breach either at the website's owner or at one of its data processors. There is also a greater chance the data could be misused – intentionally or by mistake – by the website owner, one of its processors or one of the persons involved in the processing. In contrast, storing data in an archive for taxation and accounting purposes only reduces this risk, especially since this storage usually only concerns part of the data from the customer account.

[6] Article 32 GDPR and Recital 83.

certain category of goods for the sake of reselling them at an inflated value. Rather, it is the associated measures, such as CAPTCHA tests, that might thwart these bots and such measures could be implemented in the absence of an account. Moreover, bots are also able to create accounts and place orders when logged in.

11 Stolen personal data may be misused to the detriment of data subjects, such as by taking over their identity, placing fraudulent orders in their name, and phishing. Secure authentication methods, such as passkeys[7], are rarely offered. Moreover, users required to open an account often use a password that has already been used for other accounts. This increases the risk that unauthorised users gain access to the account and potentially exploit it for fraudulent activities, which could be attributed to the original account holder. Attackers could also gain access to all personal data stored within the account. In addition, "password reset" functions[8] may not sufficiently protect against scammers who gained access to a data subject's email account to take over all of their online user accounts, even if the person uses different passwords. Single sign-on login methods through other platform accounts may cause additional security risks for consumers. If attackers gain access to this one account, they can potentially access all other connected services as well.

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. The personal data provided by users - such as name and contact details - are often "persistent" and can be used as unique identifiers. The collected data creates a unique fingerprint using a hash function. This fingerprint allows e-merchants to link multiple online user accounts and understand their browsing and purchasing behaviour.

13 Lastly, within the account creation process, e-merchants may prompt data subjects to disclose more personal information than strictly required[9] for purchasing and delivering goods, often through the use of deceptive designs[10], especially when the creation of online user account is requested between the shopping cart validation and the payment. At this moment, controllers could obtain a "last-minute consent" for purposes other than managing the order, in particular

[7] A form of password-less authentication based on cryptographic key pairs. Instead of re-entering their credentials for each individual resource, users can use their securely stored private key to perform the authentication.

[8] The most common version of such a password reset function is to send an email with a link that the user clicks on to set a new password for her or his account. Alternatively, other approaches involve sending a temporary password or, more concerning from a data protection and security standpoint, simply providing access to the account without requiring the creation of a new password or even transmitting the password in plaintext.

[9] While some data can be necessary for the billing or the shipping – such as the name or address of the client - other types of personal data should, however, not be required for the creation of the online user account itself. See Guidelines 4/2019 on Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020 (hereafter 'Guidelines 4/2019 on Data Protection by Design and by Default'), para. 70.

[10] Deceptive designs are defined as: *"[…] interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions in regards of their personal data."* See: Guidelines 3/2022 on deceptive designs in social media platform interfaces: how to recognize and avoid them, version 2.0, adopted on 14 February 2023, para. 3.

by formulating consent requests in a deceptive way. This may constitute a breach of several GDPR provisions, including Article 5(1)(a) and, when applicable, Article 6(1)(a) GDPR[11].

14 Deceptive designs can also be implemented post-purchase. For example, some websites present the user's profile as "incomplete" to encourage the customer to fill in additional personal data, such as gender or birth date, or encourage customers to create an account by clicking a button in the email confirming the order[12].

15 The risks described above are inherent to the use of any online account. However, these risks are all the more detrimental to data subjects when there is no other option for them to access the offers or to make purchases without creating an account.

3 Legal bases for imposing the creation of online user accounts under Article 6 GDPR

16 When requiring the creation of an account for users to access offers or to make purchases on e-commerce websites, controllers often invoke the legal bases of performance of a contract (Article 6(1)(b) GDPR), legal obligation (Article 6(1)(c) of the GDPR), or legitimate interest (Article 6(1)(f) GDPR).

17 These recommendations focus exclusively on the mandatory creation of accounts for accessing offers or making a purchase. Therefore, the user cannot freely consent to the processing of their data for such purpose, and the legal basis of consent (Article 6(1)(a) GDPR) is not addressed in Section 3. However, the legal basis of consent is addressed in Section 4 of the recommendations.

18 In the following subsections, the EDPB analyses the three aforementioned legal bases in the context of the most common processing purposes invoked by controllers for imposing the creation of online accounts. With regard to the purpose of the processing, it should be noted that creating an account for the user to access online sales or service offers or to make a purchase, whether on a mandatory or voluntary basis, does not constitute a specific purpose under Article 5(1)(b) GDPR[13].

[11] In light of Articles 4(11) and 7 GDPR.

[12] This means that an account has already been created in the technical background. By choosing a password the user confirms this account.

[13] As mentioned in Guidelines 2/2019 on the processing of personal data under Article 6(1) Point (b) of the GDPR, in the context of the provision of online services to data subjects, version 2.0, adopted on 8 October 2019 (hereafter 'EDPB Guidelines 2/2019 on Article 6(1)(b) GDPR'), para. 18, the identification of the appropriate lawful basis is tied to the principles of fairness and purpose limitation. It will be difficult for controllers to comply with these principles if they have not first clearly identified the purposes of the processing, or if processing of personal data goes beyond what is necessary for the specified purposes. See also EDPB Binding Decision 4/2022, para. 107; EDPB Binding Decision 5/2022, para. 101.

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

19 To determine whether performance of a contract, pursuant to Article 6(1)(b) GDPR, is appropriate for a specific processing operation, the controller must assess whether such processing is "necessary for the performance of a contract to which the data subject is a party"[14].

20 Article 6(1)(b) GDPR "must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller"[15]. In this regard, the controller must be able to demonstrate "how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur"[16]. The controller must also ensure that there is no workable, less intrusive processing of personal data to perform the contract[17].

21 In the below subsections, the EDPB assesses examples of purposes for which Article 6(1)(b) GDPR may or may not be invoked as a legal basis for requiring the creation of an account.

3.1.1 Performing a one-time sale

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 option provided by some e-merchants to make purchases in guest mode supports this observation.

> **Example 1:** Company A sells a wide range of clothing and accessories for women, men and children. Individuals need to create an account if they want to purchase items on the website. In this case, Company A cannot impose the creation of an account because the personal data necessary for the execution of the sales contract can be collected without requiring an account. For instance, Company A can provide a guest mode option, in which the order can be facilitated rather than imposing the creation of an account.

23 Therefore, controllers should not rely on Article 6(1)(b) GDPR to impose the creation of an account for the purpose of performing a one-time sale of good or service, because the necessity test required by this legal basis is unlikely to be met.

3.1.2 Subscriptions

24 Some e-commerce websites offer data subjects the possibility to subscribe to a service over a given or indeterminate period of time. In these recommendations, subscription refers to an arrangement by which one party commits to paying a specified sum in order to receive a good or service provided regularly. It involves either an upfront payment or a regular payment. A

[14] Guidelines 2/2019 on the processing of personal data under Article 6(1) Point (b) of the GDPR.

[15] Guidelines 2/2019 on the processing of personal data under Article 6(1) Point (b) of the GDPR, para.28.

[16] Guidelines 2/2019 on the processing of personal data under Article 6(1) Point (b) GDPR, para. 30. Similarly, see CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt,* (ECLI:EU:C:2023:537), para. 98.

[17] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt*, (ECLI:EU:C:2023:537), para. 99.

subscription can be valid for a specific or indeterminate period, including after a sale is concluded.

25 In this case, controllers requiring users to create an online user account might have an interest that users are entering a long-term contractual relationship with the controller requiring a frequent identification of the data subject.

The use of the account would allow the customers to use certain features of the services, such as:

- accessing the content of the subscribed service;
- regularly following their packages or activity throughout the subscription to the service;
- securely and easily communicating with the e-merchant; and
- checking or changing the status of the subscribed offer or service.

26 In the context of subscriptions, the processing involved in the creation and management of a compulsory account may be based on Article 6(1)(b) GDPR provided that such an account is strictly necessary for data subjects to access the services to which they have subscribed. In such cases, the performance of the contract should require recurrent authenticated interactions throughout the duration of the contract. Controllers may only rely on this legal basis for the duration of the contractual relationship. Furthermore, there should be an actual and valid contract for the subscribed service. In particular, controllers should be able to demonstrate that the data subject agreed to enter into a long-term contractual relationship and had a corresponding intention to be contractually bound.

Example 2: Company B provides a subscription service for receiving cosmetic products at home on a monthly basis. Individuals need to create an account if they want to subscribe to the service. They can use the account to follow their packages, communicate with the e-merchant or make changes to the delivery conditions. In this case, the creation of the account may be considered as necessary for the performance of the subscription contract within the meaning of Article 6(1)(b) GDPR.

3.1.3 Access to exclusive offers

27 Some controllers require the creation of an online user account in order to access exclusive offers. In that case, controllers must assess whether the creation of an online user account is necessary for the customer to access a closed community of members who can benefit from privileged access to certain offers of the controller.

28 Whether access to exclusive offers can be considered an essential part necessary for the performance of a contract will depend on the nature of the service provided, the reasonable expectations of the data subjects and whether the contract can be considered to be 'performed' without the provision of exclusive offers. In particular, when such offers are actually accessible to all data subjects through the mere creation of an account, the mandatory creation of an account (and the associated processing of personal data) does not appear to be *necessary* for the performance of a contract.

Example 3: An online retailer offers membership discounts that are available to individuals only upon the creation of an account. Membership does not require meeting any specific eligibility criteria other than the provision of personal data. In this case, the arrangement does not constitute a "closed

community," and therefore the creation of an account cannot be regarded as necessary for the performance of a contract within the meaning of Article 6(1)(b) GDPR.

29 By contrast, practices such as co-opting, referral, access by invitation or by selection of members only or via a membership in a cooperative (for instance, by verifying a professional status during the registration and throughout the relationship) could constitute a criterion to limit access to the service and thereby create a community of members[18].

Example 4: A retailer hosts an online event reserved to loyal customers. Only customers who have a long-term commercial relationship with the controller may receive an invitation to participate in the event. The invitation provides access to a restricted platform offering an early access to a range of selected products. In this case, the creation of an account may be considered as necessary for the performance of the contract between the retailer and the eligible customer, within the meaning of Article 6(1)(b) GDPR.

30 Therefore, the processing involved in the creation and management of an online user account may be necessary under Article 6(1)(b) GDPR in cases where access to offers or services is reserved to a selected community of members with specific proven characteristics and involves a long-term commercial relationship with the controller, in a way that registration within this community becomes the main subject-matter of the contract. By contrast, when the processing involved in the creation and management of an online account is not linked to the data subject's membership of a specific community with specific proven characteristics, the legal basis of Article 6(1)(b) GDPR does not seem appropriate.

3.1.4 Conditional purchasing

31 Some websites only allow the purchase of goods or services (or special discounts) to users with a specific status or characteristic (e.g. student status). To be eligible, the data subjects must create an account and provide proof of a special status or characteristic at the time of purchase. As opposed to the use case developed in Section 3.1.3 ("Access to exclusive offers"), controllers do not require the creation of an account to access offers, but to make the purchase. Furthermore, the data subject's ability to make a purchase does not depend on their relationship with the controller, but rather on a status or characteristic inherent to them.

32 In this context, the controller might seek to demonstrate the necessity to create an online account by arguing:

- The need to verify that the users meet the condition(s) required to validate the shopping cart at each of their purchases;
- The need to effectively identify a returning customer;
- The need to facilitate the management of the commercial relationship with the user: the account would grant the client access to a private space allowing the communication of contractual documents (e.g. a student card) in a secure and confidential manner.

[18] Such practices would need to comply with the rules on non-discrimination of recipients of online services, such as Article 20 of Directive of 12 December 2006 on services in the internal market, as per the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

33 However, in order to satisfy the necessity test, the controller has to demonstrate that there are no less intrusive means of carrying out the needed verifications. In this regard, it should be noted that controllers could check the user's status or characteristics by other means. They could, for instance, make available a secure online form allowing a collection of data to verify the status of a user, the online purchase, and the upload of the supporting documents concerned. The information collected could then be deleted as soon as it is no longer necessary.

> **Example 5:** Company C sells professional-grade medical and laboratory equipment that can be purchased only by licensed doctors or certified laboratories. To verify eligibility, the company makes available a secure online form through which users can provide the necessary information and upload supporting documents, such as a copy of their professional licence or institutional certification. The verification takes place during the purchase process, without requiring the creation of a permanent user account. The data collected through the form are used solely to confirm the buyer's professional status and are deleted as soon as they are no longer necessary for this purpose.

34 This approach allows the controller to fulfil its obligation to restrict sales to eligible professionals while ensuring that the processing of personal data remains limited and proportionate, in line with the principles of data minimisation and storage limitation.

35 Therefore, controllers should not rely on Article 6(1)(b) GDPR to justify the requirement to create an account for the purpose of the one-time verification of a user's status in situations of conditional purchasing. This is because, in such circumstances, less intrusive and equally effective alternative solutions exist to verify whether a user meets certain conditions for the purchasing of good or services, and the "necessity" test required by this legal basis is unlikely to be met.

Contract for receiving personalised shopping recommendations in the context of a purchase

36 Some controllers argue that, in addition to the purchase contract concluded between the controller and the data subject through the e-commerce website, another contract is concluded with the data subject to receive personalised shopping recommendations. In practice, before the data subject validates the purchase, they would create an account which implies that they agree to a contract to receive personalised shopping advice. Such advice would include, for instance, product suggestions generated by a recommendation system based on profiling. Some controllers argue that the creation of an account would be necessary, at the time of the purchase, in order to provide personalised recommendations in line with, for example, data subject's preferences, clothing sizes, interests, gender identity and former purchases.

However, to the extent that controllers invoke Article 6(1)(b) GDPR, the burden of proof for the existence of a contract with the respective content lies with the controller. Such demonstration would require, in particular, that the data subject has agreed to the conclusion of a contract and it is for the controller to demonstrate that these terms and conditions are validly included in the contract and relate to its main subject-matter.

37 In addition, contracts and contractual terms should meet the requirements of contract law and - in the case of consumer contracts - consumer protection law, where applicable, so that

processing based on these clauses can be considered lawful and in accordance with the principle of good faith[19].

38 For example, if the customer is required to create an account when they have already placed goods in the shopping cart and proceeded to the checkout, and are about to confirm the transaction, it seems unlikely that the controller will be able to demonstrate that the data subject is aware and agrees to any contract beyond the mere purchase of that good or service. In this case, data subjects would probably not expect the conclusion of a contract for receiving personalised shopping recommendations and the conditions of Article 6(1)(b) GDPR to justify the imposition of the creation of an account would unlikely be met.

After-sales services and exercise of rights

39 After-sales services from the e-merchant can include exchanges and returns, ability to lodge a complaint in case of dissatisfaction or benefiting from a contractual guarantee.

40 These services may be provided without the requirement to create an online user account, in particular by allowing data subjects to use secure online forms or contact the customer service. These services can be provided, for instance, by providing the customer with a specific hyperlink via email that allows the controller to automatically respond to queries related to the specific order in their customer relationship management system.

41 In addition, the creation of an account is unlikely to be necessary to identify users and respond to their exercise of consumer rights (such as withdrawal right or statutory warranties), or their rights under the GDPR, given that the controller may identify the person using other means of communication known to belong to the data subject, such as an e-mail address or a phone number. Moreover, the fulfilment of obligations of the controller (e-merchant) under consumer protection law should not depend on whether the data subject has provided the controller with their personal data by means of a mandatory online user account. Controllers must comply with their obligations under the GDPR and consumer protection and contract law regardless of the existence of an online user account. If the controller has reasonable doubts concerning the identity of the person making a request under the GDPR, it may request the provision of additional information necessary to confirm the identity of the data subject[20]. Moreover, pursuant to Article 11 GDPR, a controller should not maintain the identification of the person for the sole purpose of complying with data subjects' rights if the purpose for which the personal data are processed does not or no longer requires the identification of a data subject.

42 Therefore, controllers should not rely on Article 6(1)(b) GDPR to justify the requirement to create an account for the purposes of providing after-sales services, or enabling the management of consumer rights or of rights under the GDPR, because the "necessity" test required by this legal basis is unlikely to be met.

[19] See Guidelines 2/2019 for the processing of personal data pursuant to Article 6(1)(b) GDPR, para. 9.

[20] Article 12(6) GDPR. See also Guidelines 01/2022 on data subject rights - Right of access, version 2.1, Adopted on 28 March 2023, Section 3.2, 3.3 and 3.4.

3.2 Compliance with a legal obligation under Article 6(1)(c) GDPR

43 Legal obligations referred to in this section do not include legal requirements to assign mandatory online user accounts for offering regulated products and services, which are excluded from the scope of these recommendations.

44 To rely on Article 6(1)(c) GDPR, controllers should ascertain the extent to which their existing legal obligations require them to carry out processing activities related to the mandatory creation of online user accounts. Such legal obligations should be clear and precise, and their application should be foreseeable to persons subject to it[21]. Furthermore, processing that relies on Article 6(1)(c) GDPR must be proportionate to the legitimate objective pursued, meaning that there must be no other less intrusive means which, at the same time, would be as effective to pursue the objective[22].

45 Some legal provisions might require controllers to process and store personal data of their customers to demonstrate the fulfilment of contractual or tax and accounting obligations. Processing operations for tax and accounting legal obligations are usually restricted to specific documents such as invoices. They usually do not require the storage of personal data which has been used to create those documents. Such data processing and data storage may be achieved without requiring the user to create an account and without prejudice of the user's ability to exercise their rights under the GDPR.

46 Both identification and, where applicable, authentication of the users making a request to exercise an individual right under GDPR (such as an access right pursuant to Article 15 of the GDPR), and later the provision of access to that user, are possible without requiring the creation of online user accounts. The legal basis under Article 6(1)(c) GDPR includes the criteria of necessity, which goes beyond pure usefulness. In any case, the controller must assess the necessity of such processing, taking into account Article 11(1) GDPR[23].

47 In the circumstances described above, controllers should not rely on Article 6(1)(c) GDPR in order to justify the requirement to create an account for the purpose of the necessity to comply with a legal obligation because the 'necessity' test under this legal basis is unlikely to be met.

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

48 Article 6(1)(f) GDPR provides that a data processing may be lawful if "it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the data subject prevail".

[21] Recital 41 GDPR. This complements the requirements of Article 7 and 8 of the Charter, as interpreted by the CJEU, according to which any interference must be provided for by law which is clear, precise and foreseeable.

[22] CJEU, judgment of 9 November 2023, Case C-319/22, *Gesamtverband Autoteile-Handel eV v Scania CV AB*, (ECLI:EU:C:2023:837), para. 52 to 62.

[23] Article 11(1) GDPR states that "[*if*] *the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation*".

49 As developed in the EDPB Guidelines on legitimate interest[24], controllers relying on Article 6(1)(f) GDPR need to fulfil three cumulative conditions:

i. The pursuit of a *legitimate interest* by the controller or by a third party.
ii. There must be a need to process personal data for the purposes of the legitimate interest(s) pursued (*the necessity test*).
iii. The interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over the legitimate interest(s) of the controller or of a third party (*the balancing test*).

50 As underlined in the jurisdiction of the CJEU and in the EDPB guidelines on the processing of personal data under Article 6(1)(f) GDPR: "in the absence of a definition of the concept of legitimate interest in the GDPR, a wide range of interests is, in principle, capable of being regarded as legitimate"[25]. An interest may be considered as "legitimate" and be relevant under Article 6(1)(f) GDPR if the cumulative criteria are met.[26] Some of the most typical purposes pursued by controllers in the context of requiring data subjects to create an online account could be legitimate interests.

51 With regard to the second criterion, processing may only be deemed necessary if the legitimate interest in processing the data cannot reasonably be achieved equally effectively by other means which interfere less with the fundamental rights and freedoms of the data subjects, in particular the rights to respect for private life and to the protection of personal data.[27] The processing must therefore be "strictly necessary" in order to achieve the legitimate interest.[28] In many cases, this criterion will not be met, as outlined in conjunction with the discussion of Article 6(1)(b) GDPR.[29]

[24] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, version 1.0, adopted on 8 October 2024, pending public consultation (hereafter 'Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR').

[25] CJEU, judgment of 7 December 2023, Case C-26/22 and C-64/22, *SCHUFA (discharge of residual debt)* (ECLI:EU:C:2023:958), para. 76; CJEU, judgment of 12 September 2024, Case C-17/22 and C-18/22*, HTB Neunte Immobilien Portfolio*, para. 55; CJEU, judgment of 4 October 2024, Case C-621/22*, Koninklijke Nederlandse Lawn Tennisbond*, (ECLI:EU:C:2024:858), para. 38; CJEU, judgment of 9 January 2025, Case C-394/23, *Mousse*, (ECLI:EU:C:2025:2), para. 46; Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 16.

[26] See Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 17.

[27] CJEU, judgment of 7 December 2023, CaseC-26/22 and C-64/22, *SCHUFA (discharge of residual debt),* (ECLI:EU:C:2023:958) para. 77; CJEU, judgment of 4 July 2023, C-252/21, *Meta v. Bundeskartellamt*, (ECLI:EU:C:2023:537), para. 108; CJEU, judgment of 12 September 2024, Case C-17/22 and C-18/22, *HTB Neunte Immobilien Portfolio* (ECLI:EU:C:2024:738), para. 51; CJEU, judgment of 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:858), para. 42.

[28] CJEU, judgment of 7 December 2023, Case C-26/22 and C-64/22, SCHUFA (discharge of residual debt), (ECLI:EU:C:2023:958), para. 88, 91; CJEU, judgment of 12 September 2024, Case C-17/22 and C-18/22, *HTB Neunte Immobilien Portfolio*, (ECLI:EU:C:2024:738), para. 76; CJEU, judgment of 4 October 2024, Case C-446/21, *Schrems (data made public),* (ECLI:EU:C:2024:834), para. 59; CJEU, 4 October 2024, Case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, (ECLI:EU:C:2024:858), para. 57; CJEU, judgment of 9 January 2025, Case C-394/23, *Mousse*, (ECLI:EU:C:2025:2), para. 48, 55, 63, 64, 67, guiding principle 1.

[29] See Section 3.1.

52 The third condition entails the balancing of the opposing rights and interests at issue which depends on the specific circumstances of the particular case[30]. the controller must weigh its legitimate interest(s) or those of a third party and the "interests or fundamental rights and freedoms of data subjects". This "balancing exercise" between the fundamental rights, freedoms and interests at stake must be performed for each processing to be based on legitimate interest as a legal basis[31], and must be done before carrying out the relevant processing operation(s).

53 In order to perform the balancing test, the controller must identify and describe:

i. The data subjects' interests, fundamental rights and freedoms.
ii. The impact of the processing on data subjects.
iii. The reasonable expectations of the data subject.
iv. The final balancing of opposing rights and interests.

54 The reasonable expectations may vary. Contextual elements such as the proximity of the relationship between the controller and the data subjects, the place and context of the data collection, the nature and characteristics of the service or good offered or applicable legal requirements in the relevant context can be considered in the assessment of the reasonable expectations of individuals. The fact that certain types of personal data are commonly processed in a given sector does not necessarily mean that data subjects can reasonably expect such situation[32].

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 long-term relationship with the e-merchant beyond this purchase. In this case, the processing involved in a required account creation may not be expected.

Example 7: An individual has placed an item in a virtual shopping cart, proceeded to the check-out and is about to confirm the transaction. The website then requires the consumer to create an account. In this case the individual is already engaged in a process which started without having to create an account, and is therefore less likely to expect to then have to create an account than when the obligation appears at the beginning of the process.

55 On the other hand, the processing involved in the required creation of an account may reasonably be expected by data subjects where accessing the offers or making a purchase is subject to special conditions, such as getting a referral from another member, as, in that case, it is obvious that the service is not open to the public but only to a restricted audience.

56 In order to conduct this analysis, the EDPB has identified purposes that controllers might invoke in order to justify the mandatory creation of an account, and for which they might seek to rely on the legitimate interest legal basis.

[30] See CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 110.
[31] CJEU, judgment of 4 May 2017, Case C-13/16, *Rīgas satiksme* (ECLI:EU:C:2017:336), para. 28.
[32] CJEU, judgment of 4 July 2023, Case C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), para. 117

3.3.1 Facilitating the operational management of an order

Tracking of the order

57 Although the creation of an online user account enables data subjects to track the status of their orders or the orders' delivery, this purpose can be achieved by less intrusive means at the disposal of the controller to allow data subjects to carry out such tasks. In particular, relevant information about the status of the orders may be sent via email (for instance, a tracking number and a hyperlink where data subjects may obtain information[33]). Furthermore, customers cannot reasonably expect their personal data to be processed for the purpose of tracking their order for a period far longer than the actual delivery time.

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 be met.

Management of subsequent changes to the order

59 In some cases, the controller wishes to offer data subjects the possibility to edit their order before it is dispatched. Although being able to easily modify the order after payment may benefit the user, an online user account is not strictly necessary in that context since the modification could be offered in an alternative way, either online or by phone or email to the customer service. Customers could for instance be provided with a webpage to request a time-limited and one-use link to be sent to them, provided that their contact details can be associated with a recent order, or such a link could be included in the order confirmation[34]. In addition, customers cannot reasonably expect their personal data to be processed for the purpose of making subsequent changes to their order for a period longer than until dispatch of their order.

60 Therefore, controllers should not rely on Article 6(1)(f) GDPR to justify the requirement to create an account for the purposes of managing subsequent changes to an order. This is because the "necessity" and "balancing" tests required for the application of this legal basis are unlikely be met.

3.3.2 Services offered after or in parallel to the execution of the order

61 Some controllers argue that there is a need to impose the creation of an online user account for the continuation of the commercial relationship after or in parallel to the performance of the sales contract, as well as to provide services offered together with or after the purchase.

[33] In this context, controllers may require users to submit additional elements, such as ZIP code or name.

[34] See footnote 33.

Building customer loyalty

62 E-merchants may have a legitimate interest in offering online user accounts to develop customer loyalty, especially by personalising content, offering discounts or other exclusive benefits, or by sending commercial messages to customers who decide to create those accounts.

63 However, in many instances, processing activities in order to build customer loyalty, such as tracking the user's activity, require the data subjects' consent under Article 6(1)(a) GDPR and under Article 5(3) of the ePrivacy Directive[35].In addition, requiring data subjects to create an account does not seem strictly necessary to build a customer database for customer loyalty-related purposes, since there may be other means which are equally effective and less restrictive of the data subjects' rights and freedoms to pursue such purposes[36]. For example, a one-time collection of data (in particular an e-mail address) in the context of a guest mode or the creation of a voluntary online user account would also enable the pursuit of that purpose.

64 Although the creation of an account allows controllers to propose personalised content, which is a way of building customer loyalty, controllers should not assume the data subjects wish to be offered personalised content, especially before any purchase. Personalised content should result from an active choice of the data subject, such as agreeing to their activity being tracked or subscribing to a loyalty programme involving personalised content.

65 In general, requiring the data subjects to create an account is not necessary in order for controllers to propose loyalty initiatives. In addition, customers cannot reasonably expect such mandatory account creation for the purpose of building customer loyalty. 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 purpose of building customer loyalty. This is because the "necessity" and "balancing" tests required for the application of this legal basis are unlikely to be met.

Facilitating subsequent orders

66 Among the arguments in favour of imposing the creation of an online user account, e-merchants might invoke the facilitation of subsequent transactions. Although this is a legitimate interest, the legal basis of legitimate interest pursuant to Article 6(1)(f) GDPR also requires the *need* to process personal data for the purposes of the legitimate interest pursued. It is questionable that the processing involved in the required creation of an online user account is necessary to facilitate future purchases. In fact, whether another purchase is ultimately completed depends on the consumer's decision[37].

67 Furthermore, it appears that at the time of purchase, while providing personal data for the fulfilment of the contract to be concluded in that moment, the data subjects may not reasonably expect their personal data to be retained longer than what is necessary to fulfil the contract,

[35] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47.

[36] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 29..

[37] See, by analogy, Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions, adopted on 19 May 2021, (hereafter 'EDPB Recommendations 02/2021 on the legal basis for the storage of credit card data'), para. 8.

i.e. to deliver the goods or perform the services that they are buying[38]. Consequently, the fundamental rights and freedoms of the data subject are likely to take precedence over the controller's interest in this specific context.

68 Therefore, even if the interest of facilitating subsequent orders can be considered legitimate, controllers should not rely on Article 6(1)(f) GDPR to justify the requirement to create an account for the purpose of facilitating subsequent orders, because the "necessity" and "balancing" tests are unlikely to be met.

3.3.3 Fraud prevention

69 It might be argued that imposing the creation of an online user account is necessary because it helps controllers to detect and prevent fraud. Such fraud could consist of, for instance, using the data subject's stolen credentials to access their data, place fraudulent orders in their name, modify the delivery address of a purchased good, or taking over the data subject's identity in order to exploit it for fraudulent activities. Potential arguments include the fact that:

- The data stored in the online user account would reveal typical behaviour or other relevant information that could be used to assess further actions, in particular to prevent sending orders where there is fraudulent activity. This way, for instance, fraudulent actions by bots using leaked login credentials could be detected.
- Changes to the delivery address or the e-mail address of the account shortly before an order is placed could also indicate fraud, as could the use of the account from a device not previously linked to the account.
- Software updates – that change a device's digital fingerprint – may be seen as indicators of fraud.

70 Data processing in the field of fraud prevention may find its legal basis in Article 6(1)(f) GDPR[39]. However, this does not mean that it is automatically possible to rely on Article 6(1)(f) GDPR as a legal basis to engage in any processing of personal data for the purpose of fraud prevention[40]. In order to lawfully rely on Article 6(1)(f) GDPR, the envisaged processing needs to be based on an interest that is legitimate and fulfil both the necessity and balancing tests. In particular, the processing of personal data must be "strictly necessary for the purposes of preventing fraud"[41], which should be examined in conjunction with the "data minimisation" principle enshrined in Article 5(1)(c) GDPR[42].

71 An e- merchant may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment). Moreover, the customers, as well as other third parties, also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur[43].

[38] See, by analogy, Recommendations 02/2021 on the legal basis for the storage of credit card data, para. 9. However, in the case discussed in Recommendations 02/2021, a long-term relationship involving an online user account is already assumed whereas in the present case, the question is whether the data subject may be required to enter into such long-term relationship.

[39] Recital 47 GDPR.

[40] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 100.

[41] Recital 47 GDPR.

[42] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 104

[43] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 103.

72 Although fraud detection and prevention may be a legitimate interest, the processing involved in a required account creation does not seem necessary for fraud detection and prevention.

73 Regarding necessity under Article 6(1)(f) GDPR, many e-commerce websites do not require the creation of an account, and a purchase and usage history is actually not available when a customer account is used for the first time. In addition, the relevance of the anti-fraud measures allowed when imposing the creation of an account is questionable as changes in the delivery address usually happen right before an order is placed, users often use different devices, and software updates, which are necessary for security purposes, lead to different browser fingerprints and may be misinterpreted as an indicator of fraud. Finally, as developed in Section 2 "General remarks" of these recommendations, requiring the creation of an account might lead to fraudulent activities to the detriment of data subjects. Therefore, the necessity test is unlikely to be met.

74 Even if imposing the creation of an account would be considered necessary in order to prevent fraud, the controller would have to check if such processing meets the conditions of the balancing test. The controller should verify that the interests or fundamental freedoms and rights of the concerned data subjects do not take precedence over its legitimate interest to detect and prevent fraud. When performing the balancing test, controllers should be specific about what type of fraud they are trying to prevent, and what data they really need to process in order to prevent that type of fraud. The fraud the controller is trying to prevent should be of substantial importance, otherwise, the balancing of interests will most likely turn out in favour of the data subject, and the controller will not be able to rely on Article 6(1)(f) GDPR in this respect[44].

75 Therefore, controllers should not rely on Article 6(1)(f) GDPR to justify the requirement to create an account for the purposes of fraud prevention, because the "necessity" test required for the application of this legal basis is unlikely to be met.

4 Setting up an alternative to mandatory online user accounts

76 As developed in Section 3 of these recommendations, processing of personal data involved when imposing the creation of an online user account can be justified only for a very limited – though non-exhaustive – set of purposes, such as offering a subscription service or providing access to exclusive offers. Otherwise, requiring the creation of online accounts should be considered to be unlawful, as it would violate Article 6(1) GDPR.

77 In most cases analysed in these recommendations, the processing involved in imposing the creation of an online user account is not necessary in order to achieve various processing purposes that might be invoked by controllers.

78 Therefore, with the exception of cases in which the legal bases of the contract or legitimate interest may validly apply, it appears that the different advantages of creating an online user account should result from an active choice of the data subject.

[44] Guidelines 1/2024 on the processing of personal data under Article 6(1)(f) GDPR, para. 105.

4.1 Data processing operations enabled by offering a choice

79 In order to allow users to keep control of their data, they should be offered the possibility to access offers and make a purchase without creating an account. For instance, users can be offered a choice between creating an account or proceeding to the purchase as a guest. The "guest mode" option allows the user to complete an order without creating an account or signing in, by simply filling in a form. Users do not need to authenticate themselves using an identifier and a password in order to complete a purchase. As opposed to online user accounts, the guest mode option does not provide the user with a personal digital environment. Offering this option to the user does not require a specific data processing activity from the controller.

80 The principle of lawfulness requires the data controller to be able to demonstrate that the processing is necessary for the intended processing purpose. In this respect, neither the guest mode option nor the voluntary account creation constitute purposes in themselves. Therefore, even in the framework of the guest mode option or voluntary account creation, the controller should determine the purposes of processing and identify corresponding legal bases. For instance, for execution of the sales contract, the controller may validly rely on the legal basis of the performance of a contract under Article 6(1)(b) GDPR, whereas for collecting data for marketing purposes, the controller may rely on the legal basis of consent under Article 6(1)(a) GDPR[45], provided that all data processed are necessary. The controller may also collect or process personal data for other purposes such as for direct marketing, provided that such processing complies with the specific requirements of Article 13 ePrivacy Directive.[46] In case of further processing, the requirements for the compatibility of the purposes in accordance with Article 5(1)(b) and Article 6(4) GDPR must be taken into account.

81 In the context of a voluntary account creation, the controller may also offer additional services such as order history, facilitated subsequent purchases, or personalised offers or loyalty programmes, relying on the appropriate legal basis depending on the purpose at stake. Where such a service is based on the data subject's consent, the offer should be clearly separated from the core purchase process so that customers who choose not to register are not disadvantaged[47]. Controllers should provide clear information, specifying the purposes of processing, retention periods, and available rights, including the right to withdraw consent (Article 7(3) GDPR) and the right to erasure (Article 17(1)(b) GDPR). Moreover, the data subject must be able to withdraw the consent via the same interface as the consent was obtained[48]. Data controllers should not silently switch the lawful ground from consent to another legal basis if the consent is being withdrawn, as every change in the data processing should be notified to the data subject[49].

[45] Provided that the consent is obtained in accordance with Article 7 and Article 4(11) of the GDPR.

[46] Subject to the outcome of CJEU case C-654/23 (ECLI:EU:C:2025:213) with regard to the applicability of the GDPR to processing within the meaning of Article 13(2) ePrivacy Directive.

[47] Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, adopted on 4 May 2020 (hereafter 'Guidelines 05/2020 on consent under Regulation 2016/679'), para. 13.

[48] Guidelines 05/2020 on consent under Regulation 2016/679, para. 114.

[49] Guidelines 05/2020 on consent under Regulation 2016/679, para. 120.

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

82 Giving the user a choice between creating an account or purchasing as a guest is more compatible with the obligations of data protection by default and by design contained in Article 25 GDPR. In accordance with this article, controllers must design and create products and services that ensure the effective implementation of data protection principles such as lawfulness, transparency, data minimisation and the integrity and confidentiality of personal data, when they plan the processing of personal data and continually throughout the processing lifecycle[50]. The guest mode is a relevant way for controllers to comply with these principles.

83 First of all, the principle of transparency entails that data subjects must be adequately informed in order to assess beforehand the extent and implications of the processing, and avoid unexpected steps regarding the processing of their personal data. Giving users the choice of making online purchases by creating an account or with the guest mode option encourages the data controller to provide in-depth information on both procedures, particularly with regard to their respective purposes.

84 For example, the user may be informed that buying as a guest only enables the sales contract to be fulfilled, e.g., the goods to be delivered to the right address and the payment to be executed. On the other hand, the data controller may indicate to the customer that the creation of an account enables an improved service, including for example facilitated subsequent purchases, loyalty programmes, special offers, etc.

85 In this respect, the guest mode option enables the data controller to collect data from users in a fair manner. Given the greater transparency that the creation of an account or making a purchase as a temporary guest implies in comparison with an imposed account creation, consumers are better able to determine the extent and consequences of the processing when choosing to create an account.

86 In addition, it appears that the guest mode option would be more compatible with the data minimisation principle (Article 5(1)(c) GDPR), as opposed to the required creation of an online user account which requires the processing of user credentials and often has a significant risk of collecting more data than necessary for the performance of the sales agreement, as explained in the introduction of these recommendations.

87 The repeated purchase via a guest mode option would not lead to more data being processed nor result in data being stored several times, provided that controllers comply with the principle of purpose limitation set out in Article 5(1)(b) GDPR. In particular, processing operations for tax and accounting purposes, which are usually required by Member States' law, do not require the storage of personal data which have been used to create the respective documents such as invoices. They require certain documents to be stored separately, with restricted access and the documents and the data used to create these documents to be deleted from the main customer relationship management system. Therefore, if controllers strictly comply with their obligations, there will be no duplication of personal data: every invoice should be retained, regardless of whether it stems from a guest purchase or from regular buyers with an online user account. In case of a purchase via a guest account, no data should be stored in

[50] Guidelines 4/2019 on Article 25 of the GDPR (Data Protection by Design and by Default).

the general customer relationship management system, unless justified by a relevant purpose – such as retaining certain data for warranty purposes – and in accordance with a valid legal basis.

5 Conclusion

88 Except in very limited situations, such as when offering a subscription service, requiring users to create an account to access offers or to make a purchase would not normally meet the conditions for lawfulness set out in the GDPR, because the processing activities involved in the account creation are unlikely to be necessary in order to achieve the considered purposes. The conditions for relying on the legal basis of a legal obligation, the performance of a contract or a legitimate interest would rarely be fulfilled, as most of the time, such processing activity associated with the creation of an account would be unnecessary in order to achieve the underlying processing purposes. The purposes could generally be achieved by using less intrusive means than the requirement to create an account.

89 Offering the possibility to the user to either create an account or continue browsing and purchasing as a guest appears to be the most efficient way to collect personal data lawfully. It also contributes to a more secure online environment, more aligned with the principles of transparency, data minimisation and the obligation of data protection by default and by design.

For the European Data Protection Board

The Chair

(Anu Talus)