Response to the EDPB on the draft Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites - February 2026

Google welcomes the opportunity to provide feedback to the European Data Protection Board (**EPDB**) on its draft *Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites*, as adopted on 3 December 2025 (the **Recommendations**). We summarise our key observations on the Recommendation below, which we would be grateful for the EDPB to consider.

Introductory remarks

Google builds products that are private by design,[1] which ensure efficient processing and a secure online environment. We therefore welcome the EDPB seeking to ensure that e-commerce users are also provided with privacy-protective options.

Ensuring the most appropriate privacy-protection option requires considering the nature, scope, and context of processing (as per Article 25 GDPR). As a result, and as the EDPB recognises, there may be instances where it is appropriate and proportionate to require the creation of a user account on an e-commerce website.

This will be on a case-by-case basis, reflecting the circumstances applicable to the e-commerce transaction, provider, or website. For example, the risk of fraud and abuse, the nature of the service or product provided, and the nature of the relationship with the data subject.

Google encourages the EDPB to recognise the importance of context to ensure that the final Recommendations do not disproportionately limit controllers from discharging other obligations under GDPR, in particular under Articles 25 and 32 GDPR.

Key observations

1. **Ensuring clear and consistent scope**

   The Recommendations do not apply to online software applications services (such as app stores or equivalent digital services), online search engines services, and audio-visual media services. This is a reasonable approach. It acknowledges the

[1] Google, Privacy Practices, https://safety.google/intl/en-IE_ALL/safety/privacy-practices/

different nature and context of digital services and goods (including software, digital applications and products purchased online) in comparison to physical goods.

Digital services and goods are delivered to, used by, and owned by (or licensed to) end-users differently. The nature of these digital services and goods also means that the relationship between provider and data subject often does not conclude on delivery. To facilitate the ongoing delivery and maintenance of digital products and services (such as those delivered via an app store and equivalent services), the provider may require a verified online user account with a particular service or product user. This can be integral for licensing purposes, digital service obligations (such as efficient and more privacy-conscious compliance with mandatory age assurance requirements), and to ensure continued and cross-device access (preventing loss of access or rights if the underlying device is lost or if the user accesses the service/product via multiple devices like a phone, laptop, and tablet).

Google encourages the EDPB to ensure that this distinction - between physical goods and digital services, products, and goods (including online software applications, such as app stores and equivalent services) - is clear and consistently applied in the final Recommendation.

2. Context is important; a case-by-case assessment is necessary

The EDPB confirms that the purposes (in which an e-commerce provider can require an account) are non-exhaustive. Google encourages the EDPB to recognise more explicitly that a case-by-case approach is necessary.

Whether it is appropriate to require an account to conduct an e-commerce transaction will be context dependent. For example, considering the nature of the service or good (such as a need to interface with an existing account), the context, relationship, and reasonable expectations between the provider and data subject, and the relevant risks related to security, fraud, and abuse (which vary across different types of e-commerce websites).

It is therefore important to recognise that (considering the nature, scope, and context of processing, and the risks of varying likelihood and severity), controllers may in fact consider that an online user account is necessary in accordance with Article 25 GDPR. This position - that mandatory accounts can be reasonable and proportionate, subject to the data minimisation principle - was also confirmed by the Higher Regional Court of Hamburg (**Hamburg Decision**).[2]

[2] See Higher Regional Court of Hamburg (*Hanseatisches Oberlandesgericht Hamburg*), judgement dated 27 February 2025, case no. 5 U 30/24 [ECLI:DE:OLGHH:2025:0227.5U30.24.00], para 66(cc).

3. **Recognising the freedom to conduct a business**

The GDPR is a principles-based Regulation and controllers can in practice discharge the same obligation via different means. As a result, regulatory guidance should also be principles-based. Restrictive guidelines that envisage a uniform approach (without reference to relevant context or circumstances) risk indicating that there is only one way to conduct e-commerce, to discharge orders, and to manage customer relationships. This would disproportionately restrict the freedom to conduct business (as enshrined in the Charter of Fundamental Rights and recognised in Recital 4 GDPR).

For example, the Recommendation appears to assume that (other than in very limited circumstances) data subjects must be able to access and purchase items from e-commerce websites without making an account, irrespective of the provider's terms and conditions or business model. This does not recognise or consider the data subject's agency (including their choice whether or not to use a particular e-commerce website), the data subject's reasonable expectations in accessing an e-commerce website, and the freedoms afforded to a provider in how to build and manage a business (including how to offer discounts and manage purchase, delivery, and customer support). As the Hamburg Decision notes (paragraph 61), making an order on a specific e-commerce platform is "voluntary" and every consumer is free to purchase goods from another online retailer.

4. **Recognising end-user benefits**

The Recommendation recognises certain (but not all) benefits of mandatory user account creation. For example, to simplify the process and provide efficiency for the data subject (especially if the data subject will have an ongoing relationship with the provider) - this helps ensure a seamless and integrated user experience (particularly with questions on use and returns). The Recommendation also notes the purposes of fraud prevention, both to help protect data subjects from fraudulent activities and to ensure that the data subjects do not misuse the service.

However, notwithstanding this, the EDPB concludes that the processing involved in mandatory account creation does "*not seem necessary for fraud detection and prevention*". The EDPB bases this conclusion on the assertions made in Section 2 "General Remarks"; principally that the creation of a user account, and collection of personal data itself "*might lead to fraudulent activities*" (in the event the e-commerce provider experiences a personal data breach).

However, this risk is not unique to the creation of user accounts (voluntary or otherwise). As a result, the Recommendation risks misunderstanding and underestimating the extent of fraud targeted towards consumers and online platforms

and the significant benefits provided to both consumers and providers as a result of account-linked fraud prevention techniques.

For example, guest accounts can be exploited by malicious actors to conduct automated attacks to test whether stolen credit cards are active and can be used for larger fraudulent purchases. Where no account is required, malicious actors can conduct rapid, high-volume, and automated checks without barriers. In contrast, mandatory accounts require email verification and provide useful account history and account-associated signals that are essential for security analysis. As a result, accounts create friction for attackers, making their automated attacks more complex and difficult, which allow e-commerce providers to more easily identify and restrict suspicious accounts (for example, accounts that frequently change payment methods and make numerous, successive small purchase attempts). Mandatory accounts therefore allow for holistic risk analysis, enabling systems to better detect coordinated attacks and to distinguish fraud from legitimate customer behaviour, including to identify where new accounts are created using the same device and demonstrate suspicious behaviour. This benefits consumers, financial institutions, and e-commerce website providers.

Google therefore encourages the EDPB to reassess its position, which has been asserted without any verifiable evidence. The effective detection and prevention of fraud and abuse requires multi-layered defence mechanisms, including account-based protections. Fraudsters are constantly evolving and using more sophisticated and harder-to-prevent methods to conduct scaled online payment fraud. An account construct enables certain types of online providers (like app stores and equivalent businesses) to effectively combat these attacks. Account-linked fraud prevention on e-commerce websites is therefore an important risk mitigant for both providers and data subjects. Adopting an unreasonably limited interpretation of the balancing exercise (in relation to fraud and abuse) could significantly and unintentionally harm legitimate and proportionate fraud prevention activities implemented by providers across the digital ecosystem.

It is important for the Recommendations to recognise the significance of fraud and abuse prevention as a factor (within the context of the e-commerce service) when considering necessity across the various Article 6 conditions, particularly for the legitimate interests balancing test.

5. Ensuring the Recommendations are based on tangible and relevant risks

The EDPB appears to base the Recommendations on four risks (identified in Section 2 "General Remarks"). Specifically that the mandatory creation of online user accounts: (1) "*may* encourage" the systematic identification of data subjects, which "*may*" result in

greater amounts of data being collected; (2) *may* involve the retention of personal data longer than strictly necessary for purchase and delivery, and such data *may* be vulnerable to unauthorised access or use, or the data subjects *may* re-use a password for the account; (3) *may* "*make it easier*" for controllers to track users; and (4) "*may*" encourage the disclosure of more personal data than necessary for purchase and delivery.

These risks are not unique to account creation (mandatory or voluntary); they are equally applicable to guest check-out. The risks are also based on the EDPB's assumptions on how controllers approach their broader GDPR principles, such as storage limitation, purpose limitation, data minimisation, lawfulness, and transparency, and an incorrect assertion that the processing of personal data (by an e-commerce provider) in the context of an order from a guest differs substantively from processing relating to an account holder.

The Recommendations do not recognise that requiring online user accounts can also constitute - and be combined with - data protection by design measures, support compliance with the data protection principles, and can help strengthen user privacy expectations and trust, in particular in relation to security and preventing fraud.

As a result, the Recommendations do not in fact address the causes of the risks identified (e.g. storage limitation). Instead, the Recommendations consider an activity (online account creation) which is not only distinct from those risks, but which can help mitigate broader risks affecting both providers and data subjects depending on context (such as fraud and abuse - see our comments above).

We therefore encourage the EDPB to ensure that - as per the Helsinki Statement[3] - the final Recommendation is practical and risk-based, and is not based on assumptions on (non-)compliance.

[3] EDPB, The Helsinki Statement on enhanced clarity, support and engagement: A fundamental rights approach to innovation and competitiveness, adopted on 2 July 2025, www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf.