English Version

Observations on the EDPB Draft Recommendations Regarding Legal Bases of Mandatory Customer Accounts in B2C E-commerce

1. Questioning the EDPB's Initial Assumptions

The EDPB asserts that the "guest checkout" option would, in principle, constitute the most protective option under Article 25 of GDPR. This assertion is based on several questionable assumptions.

1.1 The guest account is not more secure

On the one hand, the widespread use of online forms and document upload platforms (identity verification, age verification, contractual supporting documents) proposed as an alternative to a mandatory customer account is not intrinsically more secure. **These interfaces constitute high attack surfaces, exposed to phishing, URL spoofing, and social engineering**. The generalization of such practices mechanically increases the likelihood that consumers become accustomed to transmitting sensitive data via one-off links, ultimately weakening their overall security.

On the other hand, **the EDPB's analysis treats weakly secured customer accounts and accounts relying on robust mechanisms** (strong authentication, passkeys, MFA) in an equivalent manner, while acknowledging that the latter are still insufficiently deployed. This approach wrongly neutralizes the potential of the customer account as a vector of enhanced security, both for consumers and for merchants.

1.2 The guest account is not less intrusive

The classification of the "guest" pathway as a less intrusive collection method is not accurate in general terms. The intrusive nature of a collection method must be assessed in light of the quantity, nature, and repetition of the data actually requested. In practice, **the guest pathway may lead to more extensive collection of personal data**: in the absence of a permanent customer space, the merchant must request, for each transaction, the information necessary for the purchase, and may even request additional data to compensate for the absence of structured history (one-off supporting documents, additional confirmations, documents transmitted via dedicated platforms or by email). **This logic multiplies collection points, increases repeated data entry, and results in a greater and more dispersed volume of data**. Conversely, a mandatory customer account designed in a proportionate manner makes it possible to limit collection to strictly necessary data and to avoid redundant collection.

Moreover, **it is incorrect to consider that the guest pathway implies less processing or an absence of data retention**: even without a customer account, the data necessary for the transaction and for the merchant's legal obligations are collected, processed, and retained, often in a fragmented manner. The customer account does not create the processing of personal data but constitutes a method of organizing it; therefore, the guest pathway cannot be presumed to be more protective than a mandatory customer account.

2. The Legitimate Interest of the E-merchant Must Be Assessed in a Global and Systemic Manner

2.1 An overly fragmented analysis of purposes

The EDPB examines in isolation the purposes associated with the customer account (order tracking, after-sales service, loyalty, fraud prevention, simplification of future purchases). **However, these functionalities form a coherent and inseparable whole, enabling the merchant also to comply with its legal** obligations (notably under consumer law, as well as accounting and tax law) **and to offer a reliable and differentiated customer experience.**

It is precisely this functional variety that explains the diversity of models: some actors offer a guest account, others structure their value proposition around a mandatory customer account. This diversity falls within the freedom to conduct a business enshrined in Article 16 of the Charter of Fundamental Rights of the EU.

2.2 Necessity in light of operational efficiency

Many e-commerce websites have architectures functionally built around the customer account (CRM, order management, after-sales service, warranties, regulatory compliance, fraud prevention). In such contexts, **the "guest account" alternative is neither equivalent in cost, nor in effectiveness, nor neutral from a security standpoint**.

The condition of "strict necessity" adopted by the EDPB is interpreted in an excessively abstract manner, without considering real organizational constraints. Yet **the assessment of the necessity criterion requires a case-by-case approach and precisely the consideration of the measures implemented for the protection of personal data**. Economic operators must be left free to organize their IT systems, in compliance with security standards.

2.3 A questionable assessment of consumers' reasonable expectations

The EDPB considers that a consumer engaged in a one-off purchase could not reasonably expect to create a customer account. This approach is debatable:

- the merchant (nor the authorities) cannot, ex ante, know the customer's relational intent;
- the very purpose of the customer account is to create a lasting commercial relationship, which constitutes a recognized legitimate interest.

Making the lawfulness of the processing dependent on a presumed intention of the consumer amounts to imposing a condition that is impossible to satisfy.

3. Recommendations in Contradiction with Regulation and EDPB Doctrine

3.1 Necessary consistency with consumer law

The EDPB's draft recommendations, by almost systematically favoring the guest account option, particularly for one-off purchases (notably sections 3.1.1 and 4), do not take into account obligations under consumer law, which require e-merchants to provide online functionalities

enabling the effective exercise of rights such as termination or withdrawal. In practice, **compliance with these obligations requires a secure personal space enabling reliable identification, traceability of actions, and fair information to the consumer, which are difficult to reconcile with purely transactional and ephemeral mechanisms**.

3.2 Tension with established doctrine on retention and archiving

Furthermore, the EDPB's analysis of the risks linked to prolonged data retention in user accounts (points 8 and 87) calls into question archiving practices implemented by controllers in accordance with the GDPR and the doctrine of supervisory authorities, notably the CNIL. These practices are precisely based on differentiated lifecycle management of data (active databases, intermediate archiving, deletion), including specific rules applicable to inactive accounts, making it possible to reconcile storage limitations with compliance with legal obligations. The compliance projects carried out by organizations in the context of GDPR implementation have required significant investment.

3.3 Increased risk of over-collection of personal data

Paradoxically, the recommendations, by encouraging alternative mechanisms to account creation (one-off verification of status or identity, sections 3.1.4 and 41), are likely to induce additional data collection, sometimes more intrusive, such as identity documents. **Such an approach creates tension with the GDPR principle of data minimization** repeatedly recalled by the EDPB (points 33, 34 and 70), with the consistent doctrine of national authorities, and with cross-cutting instruments such as the DSA, which expressly provides that compliance with obligations concerning the protection of minors online does not require providers of online platforms to process additional personal data.

3.4 Contradiction with doctrine relating to the facilitation of the exercise of rights

Finally, while the EDPB emphasizes that the exercise of rights can, in theory, be ensured without a user account (points 40 to 42), **this position appears to depart from its own doctrine and that of local authorities, which encourage the implementation of dedicated spaces for the management of preferences and rights in order to guarantee their effectiveness online**. The principle of parallelism of forms indeed supports the idea that a person who has provided their data electronically should be able to manage them by the same means, in a secure and autonomous environment, without having to call customer service.

4. Risks Already Covered by the Existing Legal Framework

Several risks identified by the EDPB do not, as such, justify a general and absolute prohibition of mandatory customer accounts:

- the absence of an adequate legal basis for excessive processing is already sanctioned by the GDPR;

- the abusive use of the customer account to force additional consents is likewise prohibited by the principles of purpose limitation, minimization, and fairness.

These risks exist independently of the mandatory or optional nature of the customer account. They concern compliance of practices, not the principle of the account itself.

5. GDPR Compliance of the Mandatory Customer Account Can Be Strengthened Through the Sharing of Best Practices

Rather than a prohibition in principle, an approach based on **best practices** would be more balanced:

- strictly dissociating account creation from any tracking or unnecessary personalization;
- limiting the data required at account creation to what is strictly necessary;
- strengthening security (strong authentication, passkeys, MFA);
- offering simple and effective mechanisms for deleting the account and associated data;
- ensuring enhanced transparency regarding purposes and retention periods;
- avoiding unnecessary repetition of data requests, often induced by the guest pathway.

A properly designed mandatory customer account can fully comply with the principles of minimization, transparency, and data protection by design.

6. Open Questions to the EDPB

• Has the EDPB consulted competition authorities (notably DG COMP) in order to assess the impact of these recommendations on the freedom to conduct a business enshrined in Article 16 of the Charter of Fundamental Rights of the EU and on the diversity of economic models?

• On what objective basis does the difference in assessment between C2C and B2C platforms rest?

• How can the requirement of "less intrusive means" be reconciled with real constraints relating to security, cost, and operational efficiency?

• In what way would the multiplication of one-off forms and platforms be, in practice, less intrusive and more secure than a well-governed and secure customer account?

Conclusion

The EDPB draft recommendation is based on a theoretical and fragmented vision of the customer account, which underestimates both the potential of the customer account as a tool for security, compliance, and differentiation and the economic realities of e-commerce. An *in concreto*, risk-based approach (as prescribed by the GDPR), informed by the sharing of best practices rather than a prohibition in principle, would make it possible to strengthen the compliance of mandatory customer accounts and to reconcile the protection of personal data with the freedom to conduct a business.

Version française

Observations sur le projet de recommandations du CEPD relatif aux bases légales des comptes clients obligatoires en e-commerce BtoC

1. Questionnement des postulats initiaux du CEPD

Le CEPD affirme que le parcours « invité » constituerait, par principe, l'option la plus protectrice au regard de l'article 25 du RGPD. Cette affirmation repose sur plusieurs postulats contestables.

1.1 Le compte invité n'est pas plus sécurisé :

D'une part, le recours massif à des **formulaires en ligne** et à des **plateformes de dépôt de documents** (vérification d'identité, de majorité, justificatifs contractuels) proposé en alternative au compte client obligatoire n'est pas intrinsèquement plus sécurisé. Ces interfaces constituent des **surfaces d'attaque élevées**, exposées au phishing, à la contrefaçon d'URL et à l'ingénierie sociale. La généralisation de ces pratiques accroît mécaniquement la probabilité que les consommateurs s'habituent à transmettre des données sensibles via des liens ponctuels, affaiblissant in fine leur sécurité globale.

D'autre part, l'analyse du CEPD traite de manière équivalente des comptes clients faiblement sécurisés et des comptes reposant sur des mécanismes robustes (authentification forte, passkeys, MFA), tout en reconnaissant que ces derniers sont encore insuffisamment déployés. Cette approche neutralise à tort le potentiel du compte client comme vecteur de sécurité renforcée, tant pour les consommateurs que pour les commerçants.

1.2 Le compte invité n'est pas moins intrusif

La qualification du parcours « invité » comme méthode de collecte moins intrusive ne saurait être retenue de manière générale. Le caractère intrusif d'une méthode de collecte doit s'apprécier au regard de la quantité, de la nature et de la répétition des données effectivement demandées. **En pratique, le parcours invité peut conduire à une collecte plus étendue de données personnelles** : en l'absence d'espace client pérenne, le commerçant est conduit à redemander à chaque transaction les informations nécessaires à l'achat, voire à solliciter des données complémentaires pour pallier l'absence d'historique structuré (justificatifs ponctuels, confirmations supplémentaires, documents transmis via des plateformes dédiées ou par courriel). Cette logique multiplie les points de collecte, accroît la répétition des saisies et conduit à un volume de données plus important et plus dispersé. À l'inverse, un compte client obligatoire conçu de manière sobre permet de limiter la méthode de collecte aux seules données strictement nécessaires et d'éviter les collectes redondantes.

Par ailleurs, il est erroné de considérer que le parcours invité impliquerait un moindre traitement ou une absence de conservation des données : même sans compte client, les données nécessaires à la transaction et aux obligations légales du commerçant sont collectées, traitées et conservées, souvent de manière fragmentée. **Le compte client ne crée donc pas le traitement de données**

personnelles, mais en constitue un mode d'organisation, de sorte que le parcours invité ne saurait être présumé plus protecteur que le compte client obligatoire.

2. L'intérêt légitime du e-commerçant doit être apprécié de manière globale et systémique

2.1. Une analyse trop fragmentée des finalités

Le CEPD examine isolément les finalités associées au compte client (suivi de commande, SAV, fidélisation, prévention de la fraude, simplification des achats futurs). Or, ces fonctionnalités forment un **ensemble cohérent**, indissociable, qui permet au commerçant de répondre également à ses obligations légales (notamment issues du droit de la consommation ou encore du droit comptable et fiscal) et proposer une **expérience client fiable et différenciante**.

C'est précisément cette variété fonctionnelle qui explique la diversité des modèles : certains acteurs proposent un compte invité, d'autres structurent leur proposition de valeur autour d'un compte client obligatoire. Cette diversité relève de la **liberté d'entreprise consacrée par l'article 16 de la Charte de droit fondamentaux de l'UE**.

2.2. La nécessité au regard de l'efficacité opérationnelle

De nombreux sites de e-commerce disposent d'architectures fonctionnellement construites autour du compte client (CRM, gestion des commandes, SAV, garanties, conformité réglementaire, lutte contre la fraude). Dans ces contextes, l'alternative « compte invité » n'est ni équivalente en coût, ni équivalente en efficacité, ni neutre du point de vue de la sécurité.

La condition de « stricte nécessité » retenue par le CEPD est interprétée de manière excessivement abstraite, sans prise en compte des **contraintes organisationnelles réelles**. Or, l'analyse du critère de nécessité suppose une approche au cas par cas et précisément la prise en compte des mesures mises en place pour la protection des données personnelles. Il doit être laissé aux acteurs économiques **la liberté d'organiser leur système IT**, dans le respect des standards de sécurité.

2.3. Une appréciation contestable des attentes raisonnables des consommateurs

Le CEPD estime qu'un consommateur engagé dans un achat ponctuel ne pourrait raisonnablement s'attendre à créer un compte client. Cette approche est discutable :

- le commerçant (non plus que les autorités) ne peut, ex ante, connaître l'intention relationnelle du client,
- l'objectif même du compte client est de **créer une relation commerciale durable**, ce qui constitue un intérêt légitime reconnu.

Faire dépendre la licéité du traitement d'une intention supposée du consommateur revient à poser une condition impossible à satisfaire.

3. Des recommandations en contradiction avec la réglementation et la doctrine du CEPD

3.1 Une nécessaire cohérence avec le droit de la consommation

Les recommandations du CEPD, en privilégiant de manière quasi systématique le recours au compte invité en particulier pour les achats ponctuels (notamment sections 3.1.1 et 4), ne prennent pas en compte les obligations issues du droit de la consommation, qui imposent aux e-commerçants la mise à disposition de fonctionnalités en ligne permettant l'exercice effectif de droits tels que la résiliation[1] ou la rétractation[2]. Or, **le respect de ces obligations suppose, en pratique, un espace personnel sécurisé permettant une identification fiable, une traçabilité des actions et une information loyale du consommateur, difficilement conciliables avec des dispositifs purement transactionnels et éphémères.**

3.2 Une tension avec les doctrines établies en matière de conservation et d'archivage

En outre, l'analyse développée par le CEPD sur les risques liés à la conservation prolongée des données dans des comptes utilisateurs (points 8 et 87) remet en question les pratiques d'archivage mises en œuvre par les responsables de traitement conformément au RGPD et à la doctrine des autorités de contrôle, notamment la CNIL. Ces pratiques reposent précisément sur une gestion différenciée du cycle de vie des données (bases actives, archivage intermédiaire, suppression), incluant des règles spécifiques applicables aux comptes inactifs, permettant de concilier limitation des durées de conservation et respect des obligations légales. Ces chantiers de mise en conformité menés par les organisations dans le cadre de l'application du RGPD ont entrainé de lourds investissements.

3.3 Un risque accru de sur-collecte de données personnelles

Paradoxalement, les recommandations, en encourageant des mécanismes alternatifs à la création de compte (vérifications ponctuelles de statut ou d'identité, sections 3.1.4 et 41), sont susceptibles d'induire une collecte additionnelle de données, parfois plus intrusives, telles que des justificatifs d'identité. Une telle approche entre en tension avec le principe de minimisation du RGPD rappelé à plusieurs reprises par le CEPD (points 33, 34 et 70) et avec la doctrine constante des autorités nationales, ainsi qu'avec des textes transverses comme par exemple, le DSA, qui dispose expressément que le respect des obligations prévues pour la protection des mineurs en ligne n'impose pas aux fournisseurs de plateforme en ligne de traiter des données personnelles supplémentaires[3].

---

[1] Loi n° 2022-1158 du 16 août 2022

[2] La directive 2023/2653 du 22 novembre 2023 relative aux services financiers conclus à distance, laquelle est venue modifier la directive 2011/83/UE sur les droits des consommateurs, par l'introduction d'un nouvel article 11 bis.

[3] Règlement (UE) 2022/2065 (DSA), article 28, §3

3.4 Une contradiction avec la doctrine relative à la facilitation de l'exercice des droits

Enfin, si le CEPD souligne que l'exercice des droits peut, en théorie, être assuré sans compte utilisateur (points 40 à 42), cette position semble s'écarter de sa propre doctrine et celle des autorités locales, qui **encouragent la mise en place d'espaces dédiés de gestion des préférences et des droits afin de garantir leur effectivité en ligne**. Le principe de parallélisme des formes plaide en effet pour qu'une personne ayant fourni ses données par voie électronique puisse les gérer par les mêmes moyens, dans un environnement sécurisé et autonome, sans avoir à appeler un service client.

4. Des risques déjà couverts par le cadre juridique existant

Plusieurs risques identifiés par le CEPD ne justifient pas, en tant que tels, une interdiction générale et absolue du compte client obligatoire :

- l'absence de base légale adéquate pour des traitements excessifs est déjà sanctionnée par le RGPD ;
- l'utilisation abusive du compte client pour contraindre des consentements supplémentaires est également prohibée par les principes de finalité, de minimisation et de loyauté.

Ces risques existent **indépendamment du caractère obligatoire ou facultatif** du compte client. Ils relèvent de la conformité des pratiques, non du principe même du compte.

5. La conformité au RGPD du compte client obligatoire peut être renforcée par un partage de bonnes pratiques

Plutôt qu'une interdiction de principe, une approche fondée sur les **bonnes pratiques** serait plus équilibrée :

- dissocier strictement la création du compte de toute logique de tracking ou de personnalisation non nécessaire,
- limiter les données exigées à la création du compte au strict nécessaire,
- renforcer la sécurité (authentification forte, passkeys, MFA),
- offrir des mécanismes simples et effectifs de suppression du compte et des données associées,
- assurer une transparence renforcée sur les finalités et les durées de conservation,
- éviter la répétition inutile des demandes de données, souvent induite par le parcours invité.

Un compte client obligatoire correctement conçu peut pleinement satisfaire aux principes de **minimisation, transparence et protection dès la conception**.

6. Questions ouvertes à destination du CEPD

- Le CEPD a-t-il consulté les autorités de concurrence (notamment la DG COMP) afin d'évaluer l'impact de ces recommandations sur la liberté d'entreprendre consacrée à

l'article 16 de la Charte de droit fondamentaux de l'UE et la diversité des modèles économiques ?

- Sur quel fondement objectif repose la différence d'appréciation entre plateformes CtoC et BtoC ?
- Comment concilier l'exigence de « moyens moins intrusifs » avec les contraintes réelles de sécurité, de coût et d'efficacité opérationnelle ?
- En quoi la multiplication de formulaires et de plateformes ponctuelles serait-elle, en pratique, moins intrusive et plus sécurisée qu'un compte client bien gouverné et sécurisé ?

Conclusion

Le projet de recommandation du CEPD repose sur une vision théorique et fragmentée du compte client, qui sous-estime à la fois le potentiel du compte client comme outil de sécurité, de conformité et de différenciation et les réalités économiques du e-commerce. Une approche *in concreto*, par les risques (telle que prescrite par le RGPD), éclairée par un partage des bonnes pratiques plutôt qu'une interdiction de principe, permettrait de renforcer la conformité du compte client obligatoire et de concilier protection des données personnelles et liberté d'entreprise.