Response to EDPB Recommendations 2/2025 on the Legal Basis for Requiring the Creation of User Accounts on E-Commerce Websites

Milos Novovic, PhD

Associate Professor of Law

BI Norwegian Business School[1]

milos.novovic@bi.no

I. Executive summary

The EDPB has chosen to tackle a mechanism which many data subjects experience as frustrating, and which, indeed, most would agree brings little direct benefit to the consumers. And yet, Recommendations suffer from three defects – methodological, doctrinal, and consequential – each independently warranting fundamental revision.

The methodological defect is one which strikes first: the Recommendations regulate the *means* of processing rather than its *purposes*. Lawfulness under Article 6 GDPR is assessed by reference to the purposes for which data are processed as its primary relation. "Requiring the creation of user accounts" is not a purpose; it is a mechanism through which multiple purposes are pursued. Evaluating a mechanism's lawfulness in abstract introduces a category error that allows any design pattern to be preemptively prohibited on the basis of risks generically associated with its use, irrespective of the controller's specific purposes and safeguards. The EDPB acknowledges this, but the Recommendations consistently slide between evaluating lawfulness of purposes and necessity of means with no clear dividing line.

The doctrinal defect: the legal analysis under Articles 6(1)(b), (c), and (f) is internally incoherent. Under Article 6(1)(b), the distinction between subscriptions (permitted) and one-time sales (prohibited) tracks commercial structure rather than any data protection principle.

[1] All views are personal and do not represent the views of my employer.

Under Article 6(1)(f), the three-part legitimate interest test is collapsed into a single inquiry – whether any less intrusive alternative is conceivable – and the effectiveness limb the CJEU treats as indispensable is systematically omitted. The way in which legitimate interest analysis is treated is outright worrisome.

The consequential defect: the Recommendations are incompatible with the soft opt-in for direct marketing under Article 13(2) of the ePrivacy Directive. The CJEU confirmed in *Inteligo Media* (C-654/23) that Article 13(2) constitutes a self-standing regime displacing GDPR Article 6(1) entirely, and that the concept of "sale" is broad. The Recommendations acknowledge the judgment only in a hedging footnote. Their storage-limitation analysis – holding that post-fulfilment retention fails the balancing test – would require deletion of the contact details Article 13(2) authorises controllers to retain. Their channelling of marketing toward GDPR consent replaces the legislature's permitted opt-out regime with an opt-in regime.

None of this denies that mandatory account creation raises legitimate data protection concerns. It does. But the EDPB should not address them through guidance that assesses the lawfulness of a mechanism as such, applies a necessity test the CJEU does not recognise, and produces conclusions that conflict with the ePrivacy Directive.

The most appropriate course is withdrawal and reconsideration. Failing that, significant revision is needed in scoping, definitions, risk assessment, legitimate interest balancing, and integration of CJEU case law.

II. The foundational problem: purposes and means

Article 6(1) conditions lawfulness on the existence of a legal basis for the *purpose* for which data are processed. The entire lawfulness framework operates at the level of purposes, not mechanisms. The Recommendations acknowledge this – paragraph 18 states that creating an account "does not constitute a specific purpose under Article 5(1)(b)" – and then proceed to evaluate the lawfulness of account creation as such, treating it as a unitary operation assessable in abstract.

A natural response is that the GDPR does engage with processing means in Articles 25, 32, 35, and 22. That is indeed true – but these operate downstream of the lawfulness determination.

Article 25 governs the implementation of processing that already has a legal basis; it does not authorise the EDPB to determine, in abstract, that a design pattern lacks a legal basis under Article 6.

The precedent this sets is dangerous. If a mechanism's lawfulness can be assessed in abstract by identifying a less intrusive alternative, the method constrains nothing. CRM databases aggregate data beyond individual transactions; paper filing is less intrusive. Customer support chatbots collect interaction data; call centres exist. Credit card payments transmit financial data; cash on delivery is possible. Each analysis replicates, each reaches a prohibitive conclusion.

A framework that can justify anything justifies nothing.

Furthermore, Recommendations rest on the assumption that mandatory accounts expose data subjects to materially greater risk than alternatives. The genuine additional processing attributable to the account consists of a credential and a persistent identifier enabling cross-session linking. This creates a real risk differential – but the GDPR addresses it through Articles 25 and 32, not Article 6. Treating infrastructure risk as a reason to deny a legal basis collapses two distinct obligations, allowing every security or design concern to become a lawfulness objection. And the conflation runs in both directions: every concern the Recommendations raise about data stored in accounts applies equally to data collected via guest checkout. If a controller retains guest-checkout data beyond what is necessary, it violates storage limitation – with or without an account. The obligations attach to the *data*, not the container.

The Recommendations also fail to examine how accounts serve data protection principles.

Authenticated access to a persistent profile allows data subjects to keep delivery and billing information current, supporting accuracy under Article 5(1)(d). It provides direct visibility into what data the controller holds, supporting transparency under Article 5(1)(a). It facilitates access rights under Article 15 – a point the EDPB's own paragraph 41 concedes but does not explain why this benefit is insufficient to affect the analysis. Accounts support data portability under Article 20 and the controller's ability to comply with breach notification under Articles 33–34, where identifying affected individuals is straightforward with account records and difficult with minimal-retention guest sessions.

Beyond doctrine, the approach raises systemic concerns. If supervisory authorities can prohibit design practices through soft-law instruments evaluating mechanisms in abstract, different authorities will inevitably prohibit different things – structurally incompatible with the consistency mechanism the GDPR establishes. Non-EU controllers will continue to require mandatory accounts, leaving supervisory authorities to choose between pursuing cross-border enforcement of a soft-law position and declining to act.

III. Scope and definitions

The GDPR is technology-neutral and sector-agnostic. Issuing sector-specific guidance requires using sector-specific concepts – and therefore either adopting definitions from other EU law instruments or devising autonomous ones. The Recommendations do neither cleanly.

"E-merchant" is defined as a person that buys, sells, or brokers products or services "for profit." EU law already has the concept of "trader," defined functionally under the Unfair Commercial Practices and Consumer Rights Directives – and its scope does not depend on profit. "E-commerce website" maps onto no established legal category; "information society services" and "intermediary service" are defined under the E-Commerce and Technical Standards Directives and clarified by extensive CJEU case law. Because the Recommendations' terms do not correspond to these, supervisory authorities face an unenviable choice: treat them as autonomous GDPR concepts or read them as importing concepts the EDPB has no competence to interpret.

Inteligo Media illustrates the tension. The CJEU held that a free service qualifies as a "sale" for Article 13(2) purposes where indirectly remunerated (paras. 55–57). The Recommendations' "for profit" definition is narrower than the CJEU's concept of "sale." Controllers offering freemium or ad-supported services may fall within the CJEU's definition while arguably falling outside the Recommendations'.

The inclusions and exclusions are also internally incoherent. "E-commerce websites" include mobile applications (footnote 3) but exclude "online software applications services" (paragraph 3). A food delivery application is paradigmatically both – a user browses offerings, places an order, pays, and receives delivery. So is a ride-hailing app. So is a telehealth platform. The text provides no criterion for resolving the overlap.

The scope confusion extends to deceptive design. The EDPB is entitled to address interface design where it directly affects GDPR lawfulness – Article 5(1)(a) fairness, validity of consent under Articles 4(11) and 7, and data protection by design under Article 25 all provide hooks. But the Recommendations invoke deceptive design as a risk inherent to account creation (paragraphs 13–14) without delineating the boundary between design choices relevant to the GDPR and those governed by the DSA and consumer protection law.

> ***Recommendation:*** *The EDPB should align definitions with established EU law – "trader," "consumer," "information society service" – as the current terms create unnecessary ambiguity and misalign with the CJEU's interpretation of cognate concepts. The EDPB should state whether scope of the terms, if autonomous, is determined by commercial function or service category, redraft exclusions accordingly, and clarify the boundary between GDPR-relevant design obligations and those governed by the DSA.*

IV. The risk analysis

Section 2 catalogues risks inherent to online accounts: excessive data collection (paragraph 7), unnecessary retention (paragraph 8), breach vulnerability (paragraph 8), cross-channel tracking (paragraph 12), and deceptive design (paragraphs 13–14). Each is conduct the GDPR already prohibits through data minimisation, storage limitation, security obligations, purpose limitation, and consent requirements.

The section does not distinguish between risks that are structural features of accounts and risks arising from non-compliance with existing law. The former could inform a balancing test; the latter cannot, because non-compliance is not a property of the mechanism.

The GDPR treats lawfulness (Article 6) and security (Article 32) as independent obligations. Treating security risk as a reason to deny a legal basis collapses them, converting any operational risk into a lawfulness objection.

The point is crucial. If the EDPB concludes that processing entails high risk because the controller *may violate the GDPR* by failing to secure data, declining to erase it, or sharing it

illegally – what processing survives? Some controllers may violate the GDPR – hence the risks to the data subjects are increased in all processing?

The security analysis is self-defeating on its own terms. *Certainly* the EDPB does not mean to suggest that *asking data subjects to create passwords* is actually *contributing* to security risks?

Paragraph 9 concedes that phishing risk "exists both in cases where the data subject has created an account or not" and recalls the controller's Article 32 obligations – conceding, within its own text, that the risk differential is manageable through security measures. This concession is not carried through to the legal analysis. Paragraph 11 notes that "secure authentication methods, such as passkeys, are rarely offered." This is an argument for requiring better authentication, not for prohibiting accounts.

> ***Recommendation:*** *The EDPB should remove Section 2 in its current form or restructure it as a balanced analysis, because in its present state it catalogues compliance failures as if they were inherent properties of the mechanism and omits the data-protection-enabling functions of accounts entirely.*

V. Performance of a contract – Article 6(1)(b)

The Recommendations conclude that controllers should not rely on Article 6(1)(b) to impose account creation for one-time sales, because the necessary data "can be collected without requiring the creation of an online user account" (paragraph 22). The existence of guest checkout is offered as proof. This confuses the necessity of the *data* with the necessity of the *mechanism*. The necessity test under Article 6(1)(b) asks whether the *processing* is necessary for contract performance – not whether a particular technical implementation is the only conceivable way to collect relevant data. A controller collecting name, address, and payment details through an account processes the same data, for the same purpose, as one using guest checkout. The data is either objectively necessary for the contract or it is not. The interface does not change the answer.

Paragraph 38 argues that data subjects "would probably not expect" a contract for personalised recommendations when account creation is required at checkout. Read charitably, this may be making an evidentiary point: proving contract formation in that context

is a genuine challenge. But the paragraph slides from evidentiary difficulty into a normative assertion about what data subjects "would probably not expect" – importing a subjective awareness test into Article 6(1)(b). The CJEU has never recognised reasonable expectations as a criterion under this provision. Whether a contract exists is a question of objective formation – governed by national contract law and consumer protection directives – not of one party's subjective anticipation. A consumer presented with terms in plain and intelligible language is bound by them where objective formation requirements are met. The EDPB is, in substance, interpreting rules of contract formation – a domain outside its institutional competence. The GDPR itself defers to "Member State law relating to the general contract law situation such as contractual validity, formation or effect."

The Recommendations permit mandatory accounts for subscriptions (paragraph 26) but prohibit them for one-time sales (paragraph 23), citing "recurrent authenticated interactions." What data protection principle does this distinction track? None. It tracks a commercial classification – recurring versus one-off payment – that the GDPR does not employ. Many subscriptions require no post-signup interaction: an auto-renewing insurance policy, an annual domain registration, or a recurring charitable donation may never require the user to log in after initial setup. Conversely, many one-time purchases involve substantial post-sale engagement: warranty claims, firmware updates, product registration. A consumer who buys a connected appliance may interact with the seller more frequently, and over a longer period, than one who subscribes to a monthly cosmetics box. The processing is not qualitatively different. Both require identification and payment data; both may involve post-transaction communication; both store data for the relevant duration.

The treatment of "exclusive offers" is circular. Mandatory accounts are permitted only where access is "reserved to a selected community of members with specific proven characteristics" (paragraph 30). A retailer's membership programme restricts access to members who create accounts – but the Recommendations deny this counts because "anyone can join." The account *is* the membership. The Recommendations define away the possibility: accounts are necessary only for memberships, but memberships count only if access is restricted by criteria *other than* the account itself. No ordinary loyalty programme can satisfy this test by definition. The examples confirm it: Example 3 (membership discounts available to anyone who registers)

is prohibited; Example 4 (invitation-only event for loyal customers) is permitted. The processing is identical. The only variable is how many people may join. But Article 6(1)(b) conditions lawfulness on whether processing is necessary for contract performance, not on how many people are party to similar contracts.

This is not data protection analysis. It is regulation of commercial practices.

The analysis also overlooks *Inteligo Media*: under the CJEU's broad reading of "sale," the free account creation in Example 3 – granting access to discounts indirectly funded through subsequent purchases – would itself trigger the soft opt-in under Article 13(2), entitling the controller to market by email on an opt-out basis regardless of the Article 6(1)(b) analysis.

> ***Recommendations:*** *The EDPB should reframe the one-time sales analysis to address the necessity of the data processed, not the mechanism, because the current framing conflates two distinct inquiries. Reasonable-expectations reasoning should be removed from Article 6(1)(b), because contract formation is governed by national law and not by the EDPB's intuitions about what consumers "probably" anticipate. If the subscription exception is retained, it should be anchored in a data-protection-relevant criterion rather than a commercial label. The open/closed community distinction should be removed, because it tracks commercial selectivity rather than any data protection principle. Finally, the EDPB should acknowledge that lawfulness of the account mechanism under the GDPR does not determine marketing rights under Article 13(2).*

VI. Legitimate interest – Article 6(1)(f)

The three-part test under Article 6(1)(f) – legitimate interest, necessity, and balancing – exists because proportionality requires weighing. Processing that is somewhat intrusive may be lawful if the interest is sufficiently strong and safeguards are in place. The Recommendations eliminate this structure. Every use-case analysis (order tracking, modifications, loyalty, subsequent orders, fraud prevention) terminates at the necessity stage. The balancing test is never reached.

This is not a three-part test.

It is a one-part test wearing a three-part structure.

The problem is not sequential disposal as such – if processing genuinely fails necessity, the analysis can stop. The problem is that the necessity test applied is malformed.

The CJEU's canonical formulation – in *Meta v. Bundeskartellamt* (para. 108), *SCHUFA* (para. 77), *HTB Neunte* (paras. 51, 59, 61), *KNLTB* (paras. 42, 53), *Mousse/SNCF Connect* (para. 48), *Latvijas* (para. 110), and *Asociația* (para. 47) – asks whether the legitimate interest "cannot reasonably be achieved *just as effectively* by other means less restrictive of the data subject's rights." The alternative must be both less intrusive *and* equally effective. When applying this test, the CJEU consistently engages with effectiveness on the facts. In *Asociația* (para. 49), prior security measures had "proved to be *insufficient*," justifying more intrusive surveillance precisely because the alternative failed. In *Rīgas satiksme* (para. 30), a first name alone "does not make it possible to identify that person with sufficient precision." In *SNCF Connect* (para. 55), title data was unnecessary because name alone achieves personalisation equally well – a straightforward case of practical equivalence. Even the most restrictive formulation, in *Schecke* (para. 86), requires that less intrusive measures "*still contribute effectively* to the objectives."

A third formulation – "strictly necessary" – appears in general principles and dispositifs. But the CJEU never uses it alone when comparing means; it is always accompanied by the comparative test. *SNCF Connect* (para. 48) makes this explicit: strict necessity is the *conclusion* following when no equally effective, less intrusive alternative exists, not an independent test bypassing the effectiveness inquiry. Cases where the CJEU applies "strictly necessary" as a seemingly freestanding standard – *SCHUFA* (paras. 88, 91), *Schrems* (para. 59) – involve contexts where heightened scrutiny is doctrinally warranted: automated decision-making under Article 22, international transfers and the adequacy standard. The Recommendations import this heightened standard into ordinary Article 6(1)(f) analysis without acknowledging the distinction.

The Recommendations acknowledge the comparative formulation at paragraph 51, then transition via "therefore" to "strictly necessary," treating them as interchangeable. In every subsequent analysis, only "strictly necessary" is applied and the effectiveness limb dropped. Their own footnote 27 cites *Meta v. Bundeskartellamt* (para. 108), *SCHUFA* (para. 77), *HTB Neunte* (para. 51), and *KNLTB* (para. 42) – each containing the full comparative formulation.

The Recommendations cite the authorities that state the correct test, then systematically decline to apply its effectiveness limb.

The consequences are visible in every use case. For order tracking (paragraph 57), email is identified as an alternative – without examining whether retrieving a tracking link from an old email is as effective as an account dashboard for multiple concurrent orders. For order modifications (paragraph 59), phone calls are proposed – without asking whether a call to a customer service line is as effective as an authenticated real-time editing interface. For fraud prevention (paragraph 73), the fact that some businesses forgo account-based detection is cited – but the fact that some businesses forgo a measure does not demonstrate that their alternative methods detect fraud just as effectively.

A distinction must also be drawn between the type of alternative at issue in the case law and the type at issue here. In *SNCF Connect*, the Court assessed whether a single data field – the customer's title – was necessary when name alone achieves personalisation equally well. Dropping one superfluous element from an otherwise unchanged system is categorically different from replacing an integrated account infrastructure with a patchwork of ad hoc mechanisms – email links, phone calls, one-use forms – whose effectiveness varies by use case and whose combined security profile may be worse than the system they replace.

Once again, if the EDPB's logic carries on – how are credit cards lawful as such?

> ***Recommendation:*** *The EDPB must apply the necessity test as the CJEU formulates it, because the current approach omits the effectiveness limb the Court treats as indispensable. For each alternative identified as less intrusive, the Recommendations should assess whether it achieves the controller's legitimate interest with equal effectiveness. Where it does not, the alternative does not defeat necessity. The EDPB should acknowledge that "strictly necessary" is the conclusion following the comparative analysis, not a standalone threshold bypassing it.*