



European Commission's Digital Omnibus (Digital Package on Simplification) Position paper

Alliance Digitale

Summary

Alliance Digitale welcomes the Commission's initiative to streamline the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD) frameworks. This proposal is a vital step towards strengthening the Digital Single Market by addressing **long-standing regulatory fragmentation and disproportionate compliance burdens that have hindered the European digital ecosystem's competitiveness**.

We believe **several measures significantly improve the business environment, bringing more harmonization and legal certainty**. This is notably the **codification of the SRB v. EDPS** case law on the definition of personal data (Article 3(1) of the proposal amending Article 4 of the GDPR), the possibility to use the **legitimate interest legal basis for AI systems** (Article 3(15) creating Article 88c), and the **power given to the Commission to adopt common templates or lists of processing subject to DPIA** (Article 3(9) amending Article 35).

However, **we also have deep concerns regarding certain proposals affecting the ePD framework**, especially the **centralized cookie management mechanism** (Article 3(15) creating Article 88b) which could significantly damage the EU digital economy but also undermine proportionality, competition, and technological neutrality.

Other areas where we see risks and recommend improvements are:

- **Split regime resulting from the partial integration of Article 5(3) of ePD into the GDPR** (Article 3(15) creating Article 88a): this provision would create a fragmented consent regime, fail to address user's consent fatigue and lead to uncertain application and enforcement by relevant authorities;
- **Six-month ban on re-requesting consent without taking into consideration evolving processing purposes or technological improvements** (Article 3(15) creating Article 88a(4)): this requirement fundamentally alters consent lifecycle management, and would in practice contradict data minimisation principles.

Last but not least, **simplifying the GDPR and the ePD would only produce results if the implementation itself is also simplified**. We also respectfully share some recommendations in this area in the last section.

About Alliance Digitale:

The Digital Marketing and Data Association - Alliance Digitale is dedicated to **representing all professions and professionals linked to data and digital marketing in France**, with the aim of promoting their development and defending their interests. Alliance Digitale's mission is to represent the views of all its **300 members**, regardless of their size or position in the value chain – media and consulting agencies, publishers and sales houses, logistics providers, data providers, tech solution providers (adtech, martech), and brands. Our trade body is the **French representative of three emblematic international digital marketing and data networks: IAB, FEDMA and GDMA.**

1. Welcoming the Commission's initiative to improve legal clarity, simplification and innovation in the GDPR

General remarks: We appreciate the Commission's recognition that **legal uncertainty and fragmented interpretation of GDPR concepts have created disproportionate compliance burdens**, especially for data-driven sectors such as advertising. By addressing long-standing ambiguities and aligning the GDPR more closely with technological realities, **the proposal represents an important step towards a more workable and innovation-friendly data protection framework for our sector**, and the digital sector at large which relies on advertising as part of its business-model.

1.1. On codifying the SRB v. EDPS case law (Article 3(1) of the proposal amending Article 4 of the GDPR)

The Commission's proposal positively incorporates the Court of Justice of the European Union's case law *EDPS v Single Resolution Board* (case T-557/20) on pseudonymized data, clarifying that information is not personal data for an entity if it lacks the means that are reasonably likely to be used for re-identification.

We strongly welcome this clarification: information should not be considered personal data for a specific entity in all cases. It provides the legal certainty necessary to foster a **proportionate, risk-based approach to data protection, ensuring that obligations are not triggered by purely theoretical identification risks.** This clarification is particularly important for complex advertising value chains where multiple actors process mainly pseudonymized data, for different purposes and with different technical and legal capabilities. The risk posed by the data processing activities varies greatly across the supply chain from one actor to the other and from one processing operation to the other. This clarification would enable controllers to better delineate (1) processing involving personal data and clearly subject to the GDPR from (2) processing that involve data that cannot be reasonably and legally linked to an individual and that are outside of the scope of the GDPR. As a result, controllers would

better allocate their compliance resources to protect personal data where it is the most relevant, while enabling time and money for data-driven R&D.

In addition, **we support the Commission's intention to rely on a Commission implementing act**, applicable to both **pseudonymisation and anonymisation**, supported by a clear and practical **toolbox**. Such an approach would:

- provide binding and harmonised guidance across Member States,
- reduce reliance on non-binding and sometimes inconsistent EDPB guidance, and
- offer legal certainty for businesses operating cross-border.

To incentivize the adoption of innovative technical safeguards, Article 41a should explicitly recognize **Privacy Enhancing Technologies (PETs)** as part of the "state of the art" assessment. In addition, **contractual safeguards** should also be explicitly accepted as valid guarantees against re-identification risk.

Alliance Digitale's proposals:

1. **Extend the scope of the proposed pseudonymisation implementing act to anonymisation:** addressing both within the same act will be key to avoid divergent interpretation for a same use case, while helping to clarify the rules and roles for entities accessing data that is personal or has undergone pseudonymization.
2. **Recognize privacy-enhancing technologies as 'state-of-the-art' pseudonymisation techniques:** Article 41a assessment due to be conducted by the Commission should be an opportunity to incentivize their development.
3. **Clarify the perspective for assessing identifiability:** to bring additional clarity, we urge the co-legislators to clarify that **identifiability should be assessed from the entity's perspective, considering objective factors** like costs, technological resources, time for identification, and applied processing safeguards.

1.2. On introducing legitimate interest as a legal basis for AI systems (Article 3(15) creating an Article 88c)

We warmly welcome the introduction of Article 88c, which establishes an **explicit and dedicated legal basis—legitimate interest—for the development, testing, and deployment of AI systems**. This is a highly positive and long-awaited development for the advertising industry, as it would **bring certainty with regard to recourse to legitimate interest by AI systems developed or used by our members** (e.g. for supporting personalized advertising, audience segmentation, content relevance, and performance measurement).

Crucially, the explicit reference to legitimate interest:

- reflects existing GDPR principles (e.g. Opinion 1/2024 of the EDPB¹),
- allows for appropriate balancing of interests, and
- avoids forcing AI-related development and operation into unsuitable legal bases.

We do however disagree with current limitations to this provision. Firstly, providing an unconditional right to object to the data subject creates legal contradiction with the objective of facilitating model training and not requiring prior consent. It also raises concerns regarding the feasibility assessment. Article 21(1) of the GDPR establishes a conditional right to object, which allows controllers to demonstrate "compelling legitimate grounds" (e.g. fraud prevention, security) that can override the data subject's objection. By granting an unconditional right to object to data subjects, this also potentially creates a security loophole where malicious actors (e.g. fraudsters) could opt-out of detection systems simply by objecting.

Secondly, the balancing test only takes into account the controller's interest whereas GDPR also considers third parties', as confirmed by CJEU case law. Without any change, this proposal would significantly limit the benefits of Article 88c for foundational model developers but also companies fine-tuning AI models with their own datasets.

Thirdly, as AI is more and more included at the core of products, allowing an AI opt-out would be equivalent to an opt-out of the vendor rather than to an AI-powered feature, since the vendor may not be able to deactivate only this feature.

And finally, should this opt-out possibility be at browser level in a spirit similar to proposed Article 88b (see below Section 2.1 for further comment on this), it would increase the risk to see high volumes of opt-outs with strong impact along the digital advertising and marketing value chain.

Alliance Digitale's proposals:

4. **In line with current GDPR provisions, ensure the right to object for data subjects to AI model training remains conditional:** delete the word "unconditional" and stick to the current wording of Article 21(1) of the GDPR to avoid legal contradiction and creating security loopholes.
5. **Allow third parties' interests to be taken into account for the legitimate interest balancing test:** this is in line with balancing test provided for by Article 6.1(f) of the GDPR, and consistent with CJEU case law.
6. **Address the potential for other EU or national laws to override the GDPR-level affirmation of legitimate interest** as a lawful basis by "explicitly requiring consent": ensuring that such overrides are harmonised and clearly defined will promote legal

¹ "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR", EDPB.europa.eu, 2024. URL: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_fr

certainty and consistent application of this provision across all EU Member States and sectors.

1.3. On the power given to the Commission to adopt common templates or lists of processing subject to DPIA (Article 3(9) amending Article 35)

We also welcome very positively this power given to the Commission. Currently, Article 35 of the GDPR allows national supervisory authorities to establish their own lists of processing operations requiring a Data Protection Impact Assessment (DPIA). **This has resulted in 27 divergent national lists based on different taxonomies, creating huge complexity and a significant lack of legal certainty for organizations involved in cross-border processing.** We therefore support the proposal to replace these fragmented national lists with a single, unified EU-level list of high-risk activities, which will streamline compliance and harmonize the interpretation of "high risk" across the Union.

However, while standardization is a positive step toward reducing costs for pan-European companies, we identify a **significant risk that the new list could become a "super-list" if it merely combines all existing national requirements.** Such an approach would create a far more onerous burden than it currently exists. To avoid this, we recommend that co-legislators mandate the EDPB to ensure the harmonized list reflects the **existing consensus** of national authorities rather than introducing new, expansive obligations.

Furthermore, the current proposal fails to clarify how these new lists will apply to existing products and services. Since Article 35 requires a DPIA to be conducted "prior to processing," it is logically impossible to apply this requirement to operations that have been running safely and compliantly for years. With no further clarification on this, businesses face a legal limbo and the risk of **retroactive non-compliance** for established services.

Alliance Digitale's proposals:

7. **Reflect consensus, not expansion:** the harmonized list should reflect the existing agreement among supervisory authorities rather than being an expansive list to maintain proportionality.
8. **Prevent retroactivity:** the text should explicitly state that new DPIA requirements apply only to **new processing operations**. Existing processing, already compliant under current national guidance, should be exempt from retroactive assessments.

2. Taking a cautious approach on ePrivacy Directive-related proposed evolutions

General remarks: While we support the Commission's objective of simplification and legal clarity, we **urge caution with regard to the ePrivacy Directive-related amendments introduced through the Digital Omnibus**.

Several of the proposed changes to cookie and tracking technologies rules indeed risk:

- introducing **new layers of complexity**,
- imposing **disproportionate compliance burdens**, particularly on smaller actors,
- reducing **effective user choice**, and
- exacerbating **competitive and structural imbalances** in the digital advertising ecosystem,
- while delivering **no additional protection for individuals** beyond the existing GDPR and ePD frameworks.

2.1 On introducing a centralized cookie management mechanism (Article 88b)

Under Article 88b, the Commission introduces a new mechanism that will require centralisation of consent management in browsers or through other technical means. This proposal represents a new regulatory requirement, rather than a mere simplification exercise. It extends beyond the stated objectives of the Digital Omnibus, which are to simplify and streamline EU laws. If adopted as currently proposed, **this mechanism risks exacerbating structural imbalances and creating significant gatekeeping risks within the digital ecosystem**.

Our concerns lie in the **(i) economic consequences of such disproportionate technical and operational burdens, (ii) failure to address consent fatigue and risk of creating user confusion, (iii) potential anti-competitive effects, and (iv) marginalization of already-existing decentralized and industry-led solutions such as the Transparency and Consent Framework (TCF)**.

(i) Economic consequences of such disproportionate technical and operational burdens:

The obligation for website operators and advertising actors to interpret and comply with automated signals emitted at browser level would introduce substantial new technical constraints, requiring deep adaptations of existing tracking, consent and monetization infrastructures. **These changes would be complex, costly, and difficult to harmonize**. By enabling default refusal at system level, this approach also risks significantly **lowering acceptance rates** for advertising-related tracking, independently of the context, quality of information, or safeguards applied by individual service providers. Such a structural shift would have a direct and negative impact on advertising-based business models, particularly for publishers and smaller market players, directing investments to environments deemed more efficient such as walled gardens. As consent is required from

users for more than just cookies, data processing would still require contextual consent that a centralized cookie mechanism would not handle – no matter how exemptions could be shaped and for which types of websites.

Finally, the implementation of such a mechanism would affect all website providers, and would necessarily depend on the active cooperation of browser developers to define and deploy technical standards—raising **concerns around feasibility, governance, and equal participation in the standard-setting process**.

(ii) Failure to address consent fatigue and risk of “consent confusion”: crucially, mandating centralized refusal mechanisms does not meaningfully address the root causes of consent fatigue, but could create “consent confusion”. Indeed, users may:

- express preferences at system level without understanding their downstream effects, such as receiving a downgraded version of the service or having to pay for previously free services,
- be unable to easily revise or contextualize their choices, and
- face inconsistent outcomes across services and devices.

(iii) Potential anti-competitive effects and a lack of a level playing field, particularly for smaller market participants: the centralization of consent signaling at browser or operating system level raises serious competition concerns. By concentrating the power to define and implement technical standards in the hands of a limited number of dominant actors, Article 88b risks distorting the level playing field to the detriment of smaller publishers, advertisers and intermediaries. The proposal introduces significant gatekeeping risks and conflicts with the pro-competition objectives of the Digital Markets Act (DMA). By concentrating consent capture within browsers, operating systems, or a limited number of consent management platforms, Article 88b would effectively create “consent gatekeepers”, thereby amplifying the market power of these intermediaries.

In the absence of robust governance and interoperability safeguards, the proposed mechanism could accelerate market concentration and undermine competition, innovation and media pluralism across the digital advertising ecosystem.

(iv) Marginalization of already-existing decentralized, industry-led solutions such as the TCF: Article 88b risks undermining well-established, decentralised consent-management frameworks, such as the Transparency and Consent Framework.

It has been developed to:

- reflect GDPR principles;
- enable granular user choice; and
- ensure accountability across complex multi-actor ecosystems.

By privileging centrally imposed browser-level signals, **the proposal sidelines market-driven and interoperable solutions that already provide meaningful user control and regulatory oversight, discouraging further innovation in privacy-enhancing consent tools.**

Alliance Digitale's proposal:

9. **Deleting the centralized cookie management mechanism (Article 88b):** mandating centralized browser signals fails to practically solve user fatigue and instead creates "consent confusion" while functionally banning the ad-supported web, including privacy-safe contextual ads models.

2.2. On partially integrating Article 5(3) of the ePrivacy Directive into the GDPR (Article 88a)

The Commission's proposal partially integrates Article 5(3) of the ePD into the GDPR, **creating differing consent requirements for tracking technologies based on whether data is personal or non-personal.**

With the SRB case law codification mentioned earlier, some uses of tracking technologies would be recognized as non-personal data to some entities' of the advertising value chain, but not to others – resulting in a **fragmented consent regime.**

Such a split regime especially with a Regulation subject to a one-stop shop enforcement model and a Directive non-evenly transposed across the Member States would reduce legal certainty, complicate compliance (especially for smaller actors), and confuse users and regulators due to inconsistent consent standards for similar uses of terminal equipment, without clear gains for user protection.

Alliance Digitale's proposal:

For a single, coherent framework, we strongly recommend co-legislators to:

10. **Fully integrate Article 5(3) of the ePrivacy Directive into the GDPR:** all rules governing access to and use of terminal equipment be fully integrated into the GDPR, ensuring consistent interpretation and enforcement, and a more user-understandable regime.

2.3. On exempting low privacy risk activities from consent (Article 88a)

Adding to audience measurement which is mentioned in Article 88a(3) as one of the four exemptions to consent, we recommend recalibrating the framework to permit other low-risk activities to be pursued on the legal basis—an approach being considered at the moment in the United Kingdom.

In line with the EDPB-EDPS Joint Opinion², **contextual advertising** should be incentivized through not requiring user's consent for being able to count who saw an ad or clicked on it (ie impression and click pixels essential for billing purposes) – opting out of personalized advertising has a direct impact on how much publishers can sell their ad inventories, but not being able to gather such simple metrics is jeopardizing at large their capacity to sell them at all. For those who consented to personalization, modulating exposure through **frequency capping** to an ad is key to avoid high commercial pressure, and is also a legal obligation for minors as per Article 28 of the Digital Services Act guidelines.

Fraud prevention, security, product maintenance as well as **software updates** are also not secondary to the user experience, but essential to the functioning of a safe and sustainable digital ecosystem. Given the value they add for users, they should also be exempted.

Other low-risk data processing activities that are essential for companies while presenting little privacy challenges that would also benefit from an exemption are **aggregated analytics**, as well as **personalisation based on first-party data** (ie directly collected by a company from its own users and customers on its channels).

Such additions to the exemption list would reduce friction for users, restore the significance of consent for high-risk processing, and create positive incentives for privacy innovation. As an example, it would help incentivizing the development and use of PETs by allowing the processing of those under the legitimate interest basis.

Alliance Digitale's proposal:

11. **Exempting from consent transparent, low- privacy risk activities such** as the use of cookies or similar technologies for: (i) **contextual advertising**; (ii) **frequency capping**; (iii) **fraud prevention**; (iv) **security**; (v) **product maintenance**; (vi) **software updates**; (vii) **aggregated analytics**; and (viii) **personalisation based on first-party data**.

2.4. On creating a six-month ban for re-requesting consent (Article 88a(4))

Article 88a(4) introduces a mandatory six-month ban on re-requesting consent for the same purpose after a user's refusal. While intended to address consent fatigue, **this requirement fundamentally alters consent lifecycle management** by treating refusal as a long-lasting default state, applicable to both access to terminal equipment and subsequent consent-based processing.

² « EDPB-EDPS Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) », *EDPB.europa.eu*, 11 February 2026. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-2026-proposal_en

It removes the **flexibility necessary to reflect evolving processing purposes, technological improvements, enhanced transparency, or changes in partners**. In practice, this rigid approach **disproportionately impacts advertising models reliant on cookies in the open web**, creating structural asymmetries with other digital ecosystems not subject to comparable constraints such as large online platforms, connected TV, etc. Cookies remain widely used across the open web, and such asymmetry with other channels appear as disproportionate.

Lastly, such a proposal **conflicts with the principle of data minimisation**. It would require to reliably identify a same person across different devices, browsers or networks, as well as authenticated and non- authenticated environments – which is technically challenging, if not impossible. It would require the storing of information on refusal to consent for a long time. This creates conflicts and deception with users' expectations and raises risks for controllers.

Alliance Digitale's proposal:

12. **Deleting Article 88a(4):** evolving processing purposes, technological improvements, enhanced transparency, and changes in partners cannot technically and reliably be reflected, while creating asymmetry between digital channels.

3. Reducing implementation fragmentation and ensuring European-level accountability

General remarks: In line with President Von der Leyen's emphasis on innovation and competitiveness in the State of the Union's speech addressed in September 2025 **we recommend taking the opportunity of the Digital Omnibus to assess every legal means to nourish this agenda.**

The risk-based approach which was one of the key principles of the GDPR has been challenged by national data protection authorities as well as the EDPB since the implementation of this regulation. **The Digital Omnibus must be the vehicle for streamlining enforcement and ensuring European-level accountability.**

Indeed, **simplifying the GDPR and the ePD would only produce results if the implementation is also simplified.** Otherwise, the Digital Omnibus would be a missed opportunity for Europe's competitiveness and innovation agenda, with no clear benefits for users. Enforcement of EU digital rules, particularly the ePD and the GDPR, differs greatly from one Member State to another. This has created significant fragmentation and complicated compliance for businesses operating across the single market. The situation is exacerbated when national authorities responsible for other regulations (e.g. telecom, consumer or competition law, etc.) also oversee privacy-related topics under the ePD, leading to inconsistent interpretations of core concepts and legal principles. For instance in France, the CNIL's dual competence over both GDPR and e-Privacy matters, combined with its public communication practices in enforcement procedures, can generate regulatory instability and reputational risks for market actors.

On advisory exchanges between companies and data protection authorities, ensuring their confidentiality would also be essential to foster legal certainty and regulatory coherence. A Simplification Draft Bill, which is being finalized in France, has provisions on such matters which could be reflected across Member States and at the European level, between companies and the EDPB.

Adding to that, **the EDPB mandate should be transformed so as to make its decisions more transparent**, hence making it a more accountable European authority.

Furthermore, a return to a risk-based regulatory approach is necessary to avoid over-cautious practices that impede legitimate data processing, including international data transfers and the use of non-sensitive inferred data.

Alliance Digitale's proposals:

13. **Mandate a statutory duty for inter-regulatory consultation:** this would require national authorities to consult when issues fall under multiple regulations, ensuring

consistent enforcement and guidance.

14. **Establish a formalized inter-authority forum for digital regulation:** a structured forum would facilitate information sharing and align legal interpretations to prevent national divergence on key principles.
15. **Develop joint guidance through mandatory public consultation:** authorities should collaboratively develop shared guidelines on key areas of overlap, ensuring the resulting rules are practical and workable.
16. **Reinforce European oversight:** strengthen the EDPB to act as a genuinely independent European authority, ensuring harmonized enforcement and preventing divergent national interpretations.
17. **Enhance procedural safeguards:** require the anonymization of actors targeted by DPAs injunctions to prevent reputational harm, strengthen the advisory role of Data Protection Authorities while ensuring that exchanged documents are treated as trade secrets by default.