The Digital Omnibus (COM(2025) 837 final) offers a real opportunity to tackle "cookie fatigue," and we strongly support this objective. However, Article 3.15 introducing new GDPR provisions (Articles 88a and 88b) - is unlikely to achieve that goal.

Specifically, it:
(i) Establishes two overlapping and inconsistent regimes governing access to user devices.
(ii) Requires a centralised, browser-level consent mechanism that is technically outdated, legally inconsistent, and unlikely to deliver the meaningful user empowerment it intends.

Key Recommendations

- Fully align the use of all data with Art. 6 GDPR legal bases, including legitimate interest, and avoids parallel regimes (GDPR vs. ePrivacy Directive).
- Delete Article 88b (Article 3.15). As browser-level consent mechanisms risk creating new digital gatekeepers and deepening legal complexity.
- Introduce a clear legal distinction between operational data uses for example analytics, fraud prevention, security (art. 88a) and commercial personalisation uses (meaningful, service-level consent).
- Revise the proposed stricter consent rules, including envisaged six month blocking period for a new request for consent following a refusal.

1. Why Article 88b falls short

It introduces invasive and inadequate solutions without solving the problem of consent fatigue

Cookie banners have led to widespread consent fatigue because of their sheer frequency and inconsistent format. Moving these requests to the browser level might not reduce their volume or improve user choice. Instead, the proposed blanket approach risks adding another layer of complexity and undermining the GDPR's consent standard. It will be challenging – if not nearly impossible - to deliver a valid "yes" that meets EU requirements through such a mechanism. In practice. Article 88b would not comply with the GDPR consent standard, which requires the consent to be freely given, specific and informed. What's needed is a structural reduction in consent requests by clearly distinguishing when consent is actually required.

It entrenches dominant players and undermines fair competition

Centralised, browser-level consent shifts control to a few major players, limiting genuine user choice and distorting competition. With most users relying on a handful of browsers, this approach effectively hands gatekeepers influence over Europe's consent framework - reinforcing their position and disadvantaging competitors. Furthermore, such a mechanism significantly compromises the economic viability of ad-supported business models. This leads to a substantial decline in publisher revenues, restricts the ability to acquire new users, and diminishes the overall effectiveness of advertising campaigns, ultimately stifling innovation and threatening the diversity of the entire European digital ecosystem.

It does not reflect how Europeans access digital services today

A browser-based model is outdated in a world of apps, connected devices, and AI-driven interfaces. Extending this logic to other platforms would repeat the same competition and control issues. It lacks a reliable way to synchronize preferences across domains and devices, resulting in a fragmented and technically inconsistent user experience.

It undermines European digital services and consumer trust

Browser-level consent weakens the direct relationship between services and users, limiting transparency and tailored choices. Crucially, web browsers lack the necessary instruments to verify the actual data practices of individual entities. This lack of oversight creates a vacuum that allows for potential abuses and the improper use of data.

It creates serious legal tension with GDPR's definition of consent

GDPR requires consent to be specific, informed, and context-dependent. A pre-set, browser-level signal applied uniformly cannot meet this standard, reducing consent to a generic, automated choice rather than a meaningful, service-specific decision. In a result, centralised, machine-readable

signals may be effective for expressing rejection ("no" across sites), it will be challenging for such mechanisms to deliver a valid "yes" that meets EU requirements.

This is why article 88b, in its current form, should be removed. Consent must remain granular and tied to specific services, preserving the direct relationship between users and digital providers.

2. Data uses where consent is impractical

The core problem behind consent fatigue is not just the volume of requests, but their lack of relevance. Users are routinely asked to approve a wide range of data uses (analytics, advertising, personalisation, cybersecurity, fraud prevention, and data sharing) all bundled together in dense, complex banners that are difficult to navigate. The answer is, therefore, not to shift this entire bundle to the browser level, but to break it apart: focus consent on the data uses that genuinely matter to users, while establishing clear and principled legal bases for routine operational uses that do not raise the same level of privacy concern.

Article 88a of the Commission's proposal already recognises certain exemptions, such as audience measurement and service security, but its scope is too narrow to work in practice. We therefore call for these exemptions to be clarified and broadened to cover a fuller set of operational uses, including:

Service security and maintenance - accessing or storing data to safeguard services, detect cyber threats, and ensure technical performance is essential. Users directly benefit from this and generally expect it as a baseline.

Fraud prevention and detection - monitoring fraudulent behaviour, preventing account takeovers, and securing transactions protects users.

Analytics and audience measurement- understanding how services are used or how campaigns perform is a basic operational need. This data is aggregated and not directly identifiable, and frequently relies on specialised third-party providers delivering transparent, comparable and verifiable market data, developed in line with a recognised methodology and supporting trusted audience measurement standards. Independent measurement requires cross-publisher deduplication and combining with data from other services from the provider or from a third party.

Self-marketing - communicating with existing customers about related products and services falls within an expected relationship. EU law already reflects this: Article 13(2) of the ePrivacy Directive allows such practices with an opt-out, and GDPR Recital 47 recognises direct marketing as a legitimate interest.

Frequency capping - limiting how often users see the same advertisement improves user experience by avoiding repetitive and intrusive ad exposure.

3. Proposed alternative of Article 88a

We advise replacing the current fragmented approach with a single, coherent regime grounded in Article 6 GDPR. In principle, storing or accessing personal data on terminal equipment should be lawful where it complies with the GDPR and relies on one of its recognised legal bases. **Consent should not be treated as the sole or default requirement in all circumstances.**

In particular, we recommend explicitly confirming that processing based on legitimate interests remains available, subject to the established balancing test ensuring that users' rights and reasonable expectations are not overridden. This would provide greater legal certainty while preserving a high level of data protection.

To address practical implementation challenges, we advise **introducing a clear list of operational processing activities that should not require consent.** These include, for instance, the transmission of communications, the provision of user-requested services, service performance and security, fraud prevention, limited analytics, contextual advertising and certain forms of direct self-marketing to existing customers. In such cases, controllers should be able to rely on alternative legal bases under the GDPR, provided that all applicable safeguards are respected. This approach would make it possible to restrict cookie banners to genuinely meaningful situations, thereby reducing users' consent fatigue and improving the overall quality of consent where it is actually required.

In addition, we recommend recognising the **role of Privacy-Enhancing Technologies (PETs) as a means of mitigating risks to individuals**. Where such technologies are effectively deployed, processing should be facilitated within the same framework, thereby encouraging the uptake of privacy-preserving solutions. To ensure consistency and trust, we further recommend empowering the Commission to define technical standards and criteria for recognised PETs through implementing acts, in close cooperation with the European Data Protection Board. This would ensure that only technologies meeting robust, state-of-the-art privacy benchmarks benefit from this approach, while preventing misuse or superficial compliance.

We would also like to draw your attention to the proposed stricter requirements for obtaining consent. The envisaged six-month blocking period for a new request for consent following a refusal is too long and should be reduced to three months in order to meet practical requirements. The rule that a new request is not permitted if consent has already been given is also impractical. Particularly in the case of dynamic websites with frequently changing providers, it must be possible to easily obtain new consent for these partners. There is no explicit regulation on how to deal with the addition or removal of providers.