Euroconsumers Digital Omnibus Submission

Cookie fatigue

October 2025

I. Executive Summary

The current landscape regarding tracking technologies is characterized by fragmentation and inefficiency, driven by the concurrent application of Directive 2002/58/EC (the e-Privacy Directive, ePD) and the General Data Protection Regulation (GDPR). The ePD specifically governs the storage of, and access to, information on a user's terminal equipment (e.g., cookies), while the GDPR governs the subsequent processing of that information when it constitutes personal data. This overlap results in inconsistent enforcement and a high compliance burden.

For users, the requirement for site-by-site consent has led to pervasive "cookie consent fatigue", driving many to automatically accept choices they do not fully understand. This environment has been systematically exploited by entities employing illegal, harmful choice architecture often leading to involuntary consent.

For businesses, the regulatory uncertainty discourages legitimate technological advancement and inhibits the use of non-invasive data-driven insights, particularly regarding website optimization and performance.

Euroconsumers[1] is committed to finding solutions that empower and protect consumers, while creating the space for responsible innovations that benefit consumers to grow. We believe consumer trust and business innovation are not opposing goals, but mutually reinforcing pillars of a fair, sustainable, and competitive digital economy. It is in this spirit that we put forward a set of pragmatic options for your consideration on the current legislation governing tracking technologies.

We see win-win potential for consumers and businesses in a structural legislative overhaul that integrates cookie rules into the GDPR framework, addressing the legal fragmentation. A dual-pillar strategy could achieve the objectives of enhanced user privacy, reduced fatigue and increased data availability for businesses:

1. Clarified legal basis for personalization (user experience): move away from a strict consent-only approach to personalization by establishing legitimate interest as the default legal basis, while strictly regulating its content, ensuring transparency and providing an easy opt-out mechanism.
2. Redefined legal certainty (business enablement): facilitate the use of essential and non-invasive technologies by codifying a conditional legal exemption for Privacy-Enhancing Analytics (PEA) under strict GDPR data minimization principles. This ensures businesses can acquire basic operational data without relying on the intrusive consent model.

1 **About Euroconsumers:** Gathering five national consumer organisations and giving voice to a total of more than 6 million people in Italy (Altroconsumo), Belgium (Testachats/Testaankoop), Spain (OCU), Portugal (DecoProteste) and Brazil (Proteste), Euroconsumers is the world's leading consumer group in innovative information, personalised services and defence of consumer rights. Our European member organisations are part of the umbrella network of BEUC, the European Consumer Organisation. Together we advocate for EU policies that benefit consumers in their daily lives.

II. Diagnostics of regulatory failure and user harm

The current consent-based system creates a powerful financial incentive for digital businesses to manipulate user choice manifesting through pervasive harmful choice architecture. Enforcement bodies across the EU, such as the Italian[2], Belgian[3] and Spanish DPA[4], have actively targeted these illegal practices. Violations include: overwhelming users with too many options (overload); concealing important choices (concealment); or making it deliberately laborious and difficult to reject cookies (obstacle).Specifically prohibited design choices include making the "accept all" button significantly more prominent than the "reject all" option, or requiring more clicks to refuse cookies than to accept them (known as a failure of "click parity"). Furthermore, pre-checked boxes, which imply consent through inaction, are already deemed non-compliant with the specific, informed and unambiguous consent standards required by the GDPR.

While retrospective enforcement remains essential, it alone cannot solve the systemic problem. As long as the mechanism for legally required monetization (via targeted advertising) is directly tied to the single, transactional interaction of the banner, the business logic will favor subtle manipulation. The regulatory design itself encourages the use of such harmful patterns.

A. Establishing a clarified legal basis for personalization

The current system of mandatory user consent for personalization does not entirely make sense for consumers. Personalization often significantly improves the customer experience and is likely to be accepted by most consumers. An opt-in requirement often simply adds another layer of transactional interaction (e.g., another cookie banner) that exacerbates user fatigue.

Instead of a transactional consent model, the legislation should therefore clarify that legitimate interest (Article 6(1)(f) GDPR) can serve as the default legal basis for personalized non-sensitive commercial practices that are not directed at minors, provided they meet strict safeguards. This expansion would reduce the need for the repetitive consent banner.

We suggest an alternative approach to regulating personalization, by focusing on content and control:

1. Transparency and explanation: data subjects should be provided with a clear, prominent, and comprehensive explanation of the profiling logic, the categories of data used for personalization and the benefits and potential consequences of the practice.

2. Easy deactivation (opt-out): the personalization practices must be subject to an unambiguous, easily locatable, and immediately functional right to object (opt-out), in accordance with Article 21, par. 2 of the GDPR. This must be available with minimum

2 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9996609

3 https://www.jdsupra.com/legalnews/belgian-supervisory-authority-sanctions-8222615/

4 https://cookieinformation.com/resources/blog/spanish-data-protection-authority-aepd-issues-cookie-fines/

friction on every interface where the personalization is applied.
3. Prohibition of the exploitation of vulnerabilities: the most critical limit is a prohibition on personalized commercial practices that exploit individual vulnerabilities (e.g., economic situation, known mental or physical frailties, or age-related inexperience). These limits must apply not only to personalized advertising but to all forms of personalization.

III. Facilitating data availability through legal clarification and exemption

To balance the need for enhanced user privacy with the necessity for businesses to operate, innovate, and optimize their services, the legislation should provide clear legal pathways for non-invasive data use that do not rely on the intrusive consent model.

A. Creating an exemption for Privacy-Enhancing Analytics (PEA)

Current interpretation often demands consent for all non-essential cookies, even those used purely for generating statistical reports, creating significant regulatory friction. To facilitate increased data availability for site functionality, a narrowly defined legal exemption from the consent requirement could be established for the use of first-party cookies and similar technologies when used exclusively for generating aggregated, de-identified statistical reports on website performance and functionality.

This exemption, termed Privacy-Enhancing Analytics (PEA), would need to be subject to stringent and mandatory technical safeguards to ensure that user privacy is not infringed. These safeguards include: (1) the data must be strictly first-party, prohibiting sharing with external organizations for ancillary purposes such as advertising; (2) mandatory technical anonymization or de-identification measures, such as IP address masking, must be implemented; and (3) there must be an absolute prohibition on cross-site tracking or profiling of individual users.

By explicitly defining and codifying a PEA safe harbor, the legislative framework would provide the necessary legal certainty for businesses needing basic performance metrics, overriding current DPA interpretations that often require consent for such activities under the ePD.This would simultaneously reduce the incentive to use manipulative consent banners and facilitate legitimate data availability.

B. Clarifying legitimate processing for functional technologies

In addition to this, we also suggest further clarifying the legal basis for technologies essential for core service functionality. The legislation could provide explicit guidelines confirming that processing necessary for security purposes (e.g., fraud prevention, protection against malware, network security) or fundamental user experience e.g., remembering an explicit language setting or shopping cart persistence) may rely on the

legitimate interest basis (Article 6(1)(f) GDPR).

While essential cookies—those absolutely necessary for the functioning of the service requested by the user—do not require prior consent but must be disclosed, clarity is required to prevent scope creep in other functional areas. The legal assessment must confirm that the data subject's reasonable expectation of privacy does not override the business's interest in secure and functional service delivery.

IV. Structural and procedural alignment: integrating tracking rules into the GDPR

Achieving strong alignment with EU data protection law requires legislative action to formally incorporate tracking rules into the GDPR structure.

A. The legal mechanism for full integration

The most comprehensive proposal for achieving harmonization is to repeal Article 5(3) of the ePD and replace it with a new, dedicated chapter within the GDPR (e.g., Chapter V-bis: Protection of privacy in electronic communications). This new chapter would govern the technical rules related to accessing terminal equipment (cookies, fingerprinting, and other tracking technologies).

This integration would address the persistent overlap between the ePD and GDPR and the political failure of the separate ePR initiative. By moving device access rules into the GDPR, the legislation achieves a technology-neutral, future-proof structure where all subsequent technological tracking methods are automatically subjected to core GDPR principles, such as data minimization, and are governed by a single, unified set of rules. Crucially, this action automatically places the enforcement and interpretation of these rules under the centralized coordination of the EDPB, eliminating Member State-specific divergence in technical standards.

B. Enhanced transparency through mandatory standardization (Icons)

To ensure that users receive clear and straight-forward information and options, the new framework should mandate the use of standardized, universally recognized data protection icons alongside any required transparency notices or layered privacy policies.

The inherent complexity of legal language often renders lengthy privacy notices ineffective. The use of standardized icons—symbols or graphic elements representing data processing activities—makes information simpler, clearer, and immediately understandable. The Italian Data Protection Authority (Garante) demonstrated the viability of this approach through a successful contest in 2021, selecting effective icon sets designed to simplify the

mandatory information required under Articles 13 and 14 of the GDPR[5].

Mandating the adoption of a unified, machine-readable icon set would close the gap between legal requirements and human comprehension.

5 https://www.edpb.europa.eu/news/national-news/2021/easy-privacy-information-icons-yes-you-can-italian-dpa-launches-contest_en


euroconsumers
GROUP
ALTROCONSUMO
DECO PROTeste
ocu
proteste
testachats
testaankoop