Europe's Cookie Rules Are Broken — And the Proposed Fix Makes It Worse

Every day, hundreds of millions of Europeans click through cookie pop-ups. This is not a user interface problem — it's a symptom of a broken legal architecture that fails citizens, damages the European economy, and offers no real privacy protection in return. The proposal to introduce Browser Level Consent, far from fixing the problem, fails on its own merits and will cost European businesses €40–50 billion per year in lost revenue — a 30–35% decline. The expansion to OS providers introduced by the Cyprus Presidency creates further concerns about giving intermediation power to these providers. Twelve member states have already called for an impact assessment – such consequential changes shouldn't proceed without one that comprehensively assesses the proposed cookie regime.

What Is the Problem?

Currently, the deployment of cookies and tracking technologies is subject to overlapping dual governance:

- The ePrivacy Directive acts as a strict gatekeeper, mandating upfront consent simply to place or access a cookie, regardless of the data's intended purpose or the actual risk to the user.
- Subsequently, the GDPR governs the processing of that data. Unlike the ePrivacy Directive, the GDPR provides a sophisticated, risk-based framework offering six distinct legal bases tailored to specific purposes and risk profiles.

This sequential application creates a regulatory deadlock. Because the ePrivacy Directive demands blanket consent upfront, it effectively neutralizes the GDPR's flexible, risk-based system, rendering alternative legal bases irrelevant. The practical result is widespread "consent fatigue," driving users toward "accept all" or "reject all" clicks that create friction without providing genuine privacy protection and without unlocking the full economic value of the digital data generated through the cookies.

Why the Omnibus Proposal Does Not Solve This

The Digital Omnibus was meant to fix the ineffective cookie regime. Instead, it makes compliance harder and costlier — without improving privacy outcomes. Rather than unifying the dual governance structure, the Commission introduces **an additional layer** of complexity: a new preliminary threshold requiring operators to classify whether data collected via a cookie is personal or non-personal, then applying diverging consent requirements based on that determination.

Today, a company must navigate two overlapping legal frameworks before deploying a cookie. Under the proposal, it must navigate yet another complex layer and as a result: classify the data, apply the relevant consent rule for that category, and justify the processing under the GDPR. In practice this means:

- **Higher compliance costs:** Every website operator would have to conduct a preliminary data classification exercise before even reaching the consent question. For SMEs without dedicated legal teams, this adds new legal risk and advisory cost that did not previously exist.

- **Greater legal uncertainty:** Operators would have to determine in real time whether cookie data is "personal" — a classification the CJEU itself has found context-dependent but is, nevertheless, contested by regulators. Getting it wrong means applying the wrong consent regime and exposure to enforcement under multiple frameworks simultaneously.

The proposal adds a new decision point at the front of the chain while leaving the underlying consent burden intact. More complexity, more cost, no measurable privacy gain.

Why Browser / OS Level Consent Is Not the Answer

The consent intermediation mechanism introduced in the EC's proposal (Article 88b in the EC proposal, renumbered to Article 8b and most recently Article 8a by the Council) mandates that web browsers and (according to the Presidency's 21 May compromise text) OS providers, serve as consent gatekeepers. It requires them to provide technical means for users to give, refuse and withdraw consent via automated machine readable signals that all controllers must respect. This mechanism is fundamentally flawed on its own terms . Under the GDPR, valid consent must be specific and informed. A single browser/OS prompt that applies universally to all websites, across all purposes and contexts, meets neither criterion. It cannot produce legally valid consent when the user clicks "yes," nor can it produce a meaningful refusal when the user clicks "no," because in both cases the user lacks the contextual information mandated by the GDPR.

Today, site-level consent rates in Europe average around 70%[1]. Under a centralised browser/OS prompt, consent rate could drop to as low as 25%[2]. Implementing the mechanism would also require every website to build and maintain APIs to communicate its purposes to the browser/OS — a significant technical and financial burden, particularly for small sites.

Users who say "no" gain no new substantive protection — the GDPR's core principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, already apply — but lose access to the ad-funded services they rely on. Meanwhile, non-compliant actors who already ignore consent signals face no new constraint. The mechanism imposes massive economic costs while delivering zero additional privacy benefit — and undermines the legal standard it claims to implement.

The expansion to OS providers only further risks concentrating consent intermediation power in the hands of a very small number providers, who themselves compete in the advertising market. The new anti-self-preferencing clause (Article 8a(7a)) acknowledges but does not resolve this structural conflict of interest – it delegates safeguards to a future standard-setting process with no guaranteed timeline or enforcement mechanism.

[1] Didomi, Consent Collection in 2025, 2025, p. 12-15.
[2] Baviskar et al., ATT vs. Personalized Ads: User's Data Sharing Choices Under Apple's Divergent Consent Strategies, July 2024.

Why This Matters to the European Economy

Economic modelling shows the **Browser / OS Level Consent mechanism will cost European businesses at least €40–50 billion per year** in lost revenue — a 30–35% decline. For every 1% further drop in consent rates, European businesses lose an additional €600–800 million annually[3]. This directly hits the economy.

Without consent, websites cannot fund themselves through advertising. Publishers — including independent news outlets — will be forced behind paywalls or shut down. Citizens will pay more for less information. SMEs — 99% of European companies — lose their most cost-effective channel for reaching customers. On every euro spent on Meta ads, for example, European SMEs make 3.79 euros of revenue[4] – solely this dynamic shows how critical to the European economy is the maintenance of a healthy digital advertising ecosystem.

How to Fix It

The answer is straightforward: **one set of rules, under one law.** Cookie placement and data use should be governed under the GDPR — a modern, risk-based framework already designed for this purpose. This means the legal basis for placing a cookie should depend on what the data is used for, not be subject to blanket consent regardless of context.

What Member States Can Do

In the Council negotiations on the Digital Omnibus happening now:

1. **Urge the Presidency to demand an impact assessment –** evidence from SMEs, publishers, advertisers, and other important industry players must be taken into account and the principle of proportionality respected; the Commission must provide a proper impact assessment of the whole proposed cookie regime.
2. **Delete the Browser / OS Level Consent mechanism (Article 8a, former Article 88b/8b)** — it cannot produce legally valid consent, will diminish the ad-funded internet, and harm citizens and businesses alike. Expansion to OS providers only further risks concentrating consent intermediation power in the hands of a very small number providers, who themselves compete in the advertising market.
3. **Align cookie rules with the GDPR's full set of legal bases** — replace the current blanket consent requirement under ePrivacy Directive Article 5(3) with the purpose-based, risk-calibrated approach under GDPR (Article 6(1)) with six legal bases.

[3] Implement consulting group, Gone in one click, April 2025.
[4] Tadelis et al., Learning, Sophistication, and the Returns to Advertising: Implications for Differences in Firm Performance, April 2023.