ANALYSIS 39/2025 / 11 December 2025

EU data processing consent reform must account for market incentives

Proposed streamlining of EU rules on consent for processing of personal data should account for how digital-market incentives shape implementation

Paul Richter, Tillman Schenk

Giving consent online in Europe: the state of play

Across most websites, users' personal data flows through a complex system involving publishers, third-party vendors, analytics providers and advertising technologies, making large-scale data sharing a routine part of online business models. For example, the retail site Zalando shares users' personal data with many different third-party vendors, including Facebook Pixel, Google Ads, Pinterest, Snapchat and TikTok[1].

European Union rules, in particular the general data protection regulation (GDPR, Regulation (EU) 2016/679) and the ePrivacy Directive (Directive 2002/58/EC as amended by Directive 2009/136/EC), aim to give users meaningful control over their personal data. For many types of data processing, these regulations require online entities to obtain users' consent before handling personal data or storing cookies and other tracking technologies on devices. This requirement is usually implemented via the online consent banners that users routinely encounter.

This approach to managing consent often fails to live up to regulatory expectations, or to genuinely support users' interests. Among the top 10,000 European websites, fewer than 15 percent deploy consent banners that are fully GDPR-compliant (Nouwens *et al*, 2025). Internal audits by the Transparency and Consent Framework – an initiative of the online advertising industry (IAB Europe, 2024) – likewise reveal that many consent-

management solutions under this widely used industry standard fall short of compliance.

Persistent regulatory under-enforcement enables this patchy compliance; the responsibility for ensuring that consent banners comply with EU law lies with national data protection authorities, many of which are chronically under-resourced and which have differing interpretations of the rules (FRA, 2024).

Yet the deeper reason for these patterns lies in firms' commercial interests. The industry's approach to implementing the GDPR and ePrivacy Directive is driven by strong profit incentives to structure consent options in ways that increase user acceptance rates. This frequently arises in the form of 'dark patterns' – misleading and manipulative website designs and configurations intended to steer users toward disclosing more personal data.

Even if fully compliant, the consent system presents significant practical problems for users. Visitors are confronted with numerous consent decisions each time they access a website, which leads to user fatigue (Martens, 2025). As a result, people often make choices that fail to reflect the way they weigh privacy costs against the benefits of sharing their data.

Farronato *et al* (2025) show that many users have nuanced preferences, yet binary shortcuts push them to share either more or less than they would ideally choose. They found that consumers would be better off if they could set blanket preferences, reducing consent burden and helping users make choices that truly align with how they want their data handled. Setting preferences globally lets users configure everything once, at a time that's convenient, rather than while they're trying to accomplish another task. This makes them more likely to take the time to make more informed choices that align with their preferences.

Proposed changes to consent rules

In this context, the European Commission proposed a digital omnibus on 19 November 2025 – a draft law that would amend several EU digital laws as part of a simplification drive aimed at strengthening EU competitiveness (European Commission, 2025a). According to the staff working document accompanying the proposal, a large portion of the expected reduction in administrative burden for consumers and firms would stem from revisions to the GDPR and the ePrivacy Directive to simplify online consent

management[2]. These changes affect everything from the situations in which user consent is required to browser-level controls and the design of consent banners.

Lightening the load of consent banners

The Commission's proposal would reduce significantly the number of situations in which publishers must ask for consent. Firstly, the Commission proposes to integrate elements of the ePrivacy Directive into the GDPR regarding processing of information stored on user devices. At the same time, it proposes to amend these provisions by defining a set of low-risk data-use purposes that would no longer require consent. In addition, the Commission also proposes narrowing the definition of 'personal data', thereby reducing the range of situations in which the GDPR applies. Through these proposed reductions in scope, the Commission claims that 50 percent of private websites and 80 percent of public websites would no longer have to rely on consent and the use of cookie banners[3].

In principle, excluding low-risk activities from the scope of the GDPR and reducing unnecessary consent prompts is a natural first step to tackle users' consent banner fatigue. Yet questions remain about whether companies may interpret these exceptions too broadly in practice, reducing user control. While these reductions may ease compliance burdens, the Commission must ensure that the resulting rebalancing does not unduly diminish individual protections (Mariniello, 2025).

Ability for global consent

Where publishers and vendors still require consent, the Commission's proposal seeks to shift consent management away from website-level banners and toward centralised, user-controlled settings. Users would be able to set their privacy preferences for various types of data processing through their web browser, which would respond to consent prompts automatically.

This would offer a centralised and accessible way for users to accept or refuse data processing, significantly reducing repeated interactions with consent banners. However, delegating implementation to browser providers raises concerns. Many browsers profit from the sharing of personal data and therefore have limited commercial incentives to facilitate such user-friendly mechanisms. They could, for instance, design confusing and difficult to navigate interfaces to hinder users from rejecting personal data-sharing.

The Commission also explicitly encourages alternative technical solutions, including the potential use of agentic AI systems, which would process information on user preferences and companies' stated uses of personal data to manage consent decisions on behalf of users. However, without clearer expectations or tangible support, the proposal's brief mention of agentic AI systems is unlikely to spur such solutions. Industry has little incentive to build user-empowering consent tools, and the few promising solutions that do exist often fail to gain traction[4]. The Commission should take on a more proactive role, for example by funding research into innovative consent tools, or by creating an EU certification for trusted consent tools.

Lastly, one large exemption undermines the omnibus' broader aim of establishing a consistent and user-centred consent framework: media service providers[5] would not be required to respect automated consent signals and may continue relying on traditional consent banners. The Commission justifies this exemption as necessary to protect the financial basis of independent journalism. But limiting this exemption to media organisations appears arbitrary: although supporting independent journalism is a valid aim, the same logic could arguably extend to other sectors that also rely on data-driven revenue. A similar outcome could be achieved by mandating the global consent signal to include industry-specific preferences, so that users can choose different privacy settings for sectors such as news media if they wish.

Addressing dark patterns

Finally, the Commission directly addresses several common dark patterns used in consent collection. First, it stipulates that users must be able to give or refuse consent through a single-click mechanism, simplifying consent choices. In addition, it prohibits websites from repeatedly prompting users for consent after a refusal in the hope of eventually securing approval. Under the proposed rules, publishers are barred from requesting consent again for six months.

These steps may help tackle some dark patterns, but they are reactive and largely address the symptoms rather than the underlying cause. As long as consent banner designs are mainly guided by the preferences of websites and vendors, new dark patterns will continue to appear, and actual practices will fall short of regulatory intent. If the companies that design consent interfaces benefitted from aligning their design choices with user interests, dark patterns would go away naturally.

Conclusions

Taken together, the reforms proposed in the digital omnibus are an effort to streamline the consent experience and include some promising proposals. Yet the effectiveness of these changes will depend ultimately on how they are implemented in an environment in which the underlying incentives remain unchanged. Organisations that benefit from extensive data collection will continue to interpret ambiguous rules broadly, design interfaces strategically and search for new ways to encourage acceptance wherever flexibility is available.

To make the reforms effective, the Commission should focus directly on the market dynamics that have limited the effectiveness of the consent rules so far, aligning incentives with users' interests. This could include subsidising or certifying consent tools that are designed around user preferences rather than advertising objectives. A different approach would be for users to choose a consent management system and let companies bargain with the system providers for access to users. In that way consent management platforms would have monetary incentives to make their system attractive to users.

In addition to aligning firm incentives, the Commission should adopt further measures. For instance, it must give much clearer guidance on the implementation of the global consent signal. Although the proposal refers to a standardised signal, the description remains too limited to ensure consistent and user-centred deployment. Without more detailed specifications on both the technical format and the interface through which users express their preferences, the design of the signal will likely be heavily influenced by companies whose business models depend on extensive data collection. Clear and prescriptive requirements would help ensure that the signal reflects user choices rather than commercial priorities.

Enforcement must be strengthened if the reforms are to achieve their intended effect. The Commission should encourage member states to ensure that their data protection authorities have sufficient resources to consistently monitor compliance, investigate violations and apply corrective measures. Stronger oversight is essential to detect when organisations stretch or manipulate the rules in ways that undermine user autonomy, and to ensure that such practices are addressed promptly rather than becoming entrenched in the market.

Ultimately, the success of any changes to the EU's rules on online consent will depend on whether reforms are supported by a regulatory and market environment that ensures consistent, reliable and impartial implementation. Without clearer incentives, stronger guidance and credible enforcement, well-designed adjustments risk being applied unevenly or even undermining the regulatory intent.

References:

European Commission (2025a) 'Proposal for a Digital Omnibus', COM(2025) 837 final, European Commission, available at https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

European Commission (2025b) 'Staff Working Document accompanying the Digial Omnibus and the Digital Omnibus on AI', SWD(2025) 836 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025SC0836&qid=1765377777736

FRA (2024) *GDPR in practice – Experiences of data protection authorities*, European Agency for Fundamental Rights, available at https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities

Farronato, C., A. Fradkin and T. Lin (2025) 'Designing consent: Choice architecture and consumer welfare in data sharing', *NBER Working Paper* 34025, National Bureau of Economic Research, available at https://www.nber.org/papers/w34025

IAB Europe (2024) *TCF Compliance Report*, available at https://iabeurope.eu/wp-content/uploads/IAB-Europe-TCF-Compliance-Report-2024.pdf

Martens, B. (2025) 'The European Union needs more than the digital omnibus to make digital services competitive', *Analysis*, 8 December, Bruegel, available at https://doi.org/10.64153/NIRG1605

Mariniello, M. (2025) 'Efficiency and distribution in the European Union's digital deregulation push', *Policy Brief* 31/2025, Bruegel, available at https://www.bruegel.org/policy-brief/efficiency-and-distribution-european-unions-digital-deregulation-push

Nouwens, M., J.B. Kristensen, K. Maalt and R. Bagge (2025) 'A Cross-Country Analysis of GDPR Cookie Banners and Flexible Methods for Scraping Them', mimeo, available at https://arxiv.org/abs/2503.19655

Endnotes

1 Information on the vendors Zalando shares personal data with can be found behind multiple clicks on the cookie banner that pops up when visiting their site: www.zalando.be.

2 For details of other aspects of the digital omnibus, see Martens (2025).

3 Note that these figures represent the proportion of total websites that would not need to use cookie banners with the proposed changes and not the decrease in frequency of cookie banners; some website already do not require cookie banners since they don't use cookies nor process personal data. See European Commission (2025b), page 50.

4 Examples include browser plugins that automatically complete consent banners, such as Consent-O-Matic, and privacy dashboards that help users manage data permissions across services, such as ErnieApp. Other tools focus on maximum privacy, such as the Ghostery plugin and the Brave browser. Despite their potential, these tools have not been widely adopted.

5 As defined in the European Media Freedom Act (Regulation (EU) 2024/1083), Article 2(2).

Bruegel
Rue de la Charité
33,
B-1210 Brussels
(+32) 2 227 4210
info@bruegel.org

Bruegel.org

© Bruegel 2026. All rights reserved. Short sections, not to exceed two paragraphs, may be quoted in the original language without explicit permission provided that the source is acknowledged. Opinions expressed in this publication are those of the author(s) alone.