Clifford Chance

The Digital Omnibus and the economic effects of centralising consent

June 2026

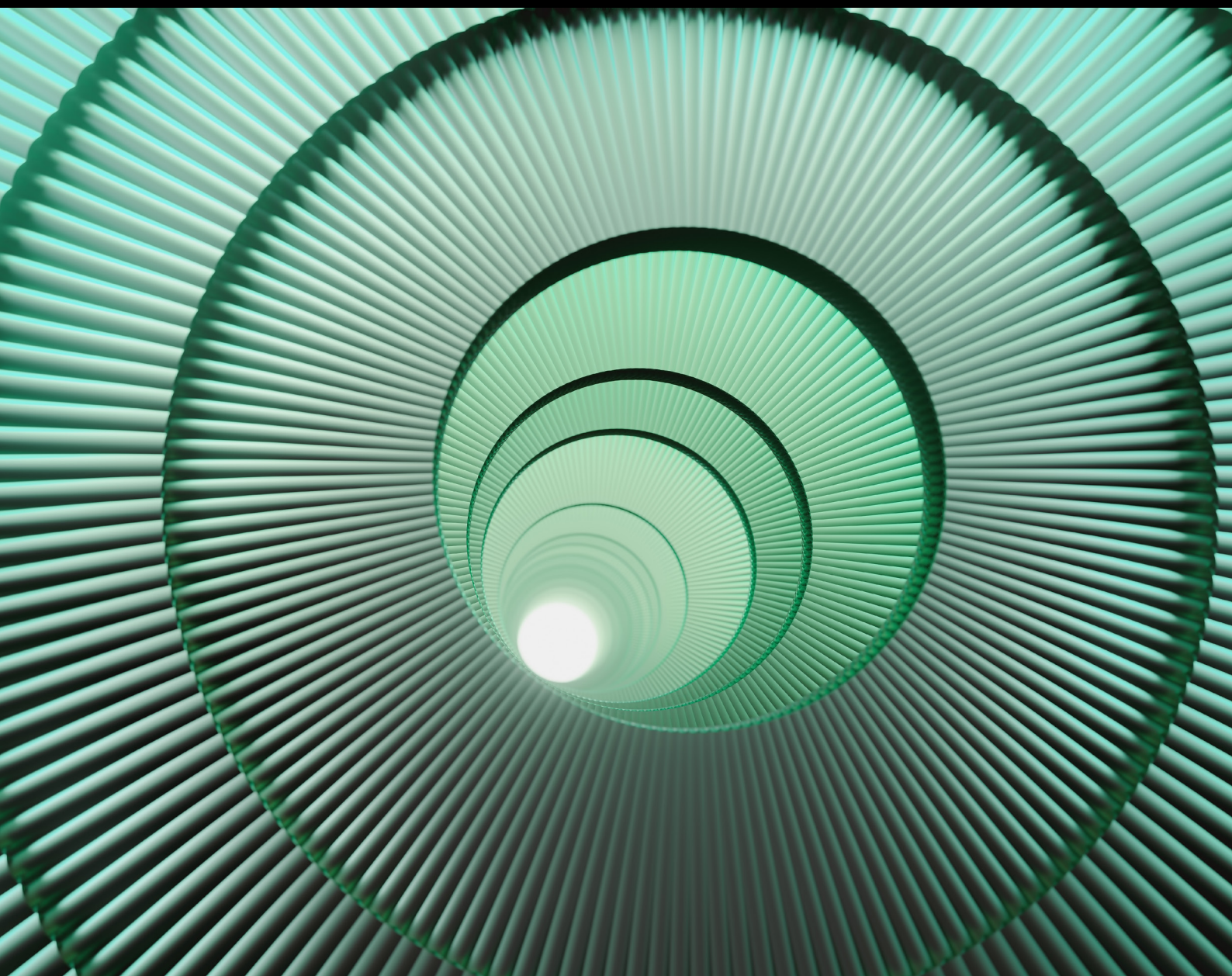


Table of contents

About the authors 04

Executive summary 06

1 Introduction and overview 09

2 The Digital Omnibus – a high-level overview 12

2.1 The quest for changes 12

2.2 Economic rationale behind the Digital Omnibus 14

2.2.1 Compliance costs 14

2.2.2 Innovation 15

2.2.3 Legal certainty 16

2.2.4 Effects on consumers 16

2.2.5 Competitive dynamics 16

2.3 The intended and unintended effects of Article 88b GDPR 17

3 Article 88b: open questions and trade-offs 18

3.1 The current consent architecture 18

3.1.1 The role of Consent Management Platforms ('CMPs') 19

3.1.2 The IAB Transparency and Consent Framework ('TCF') 21

3.1.3 The shortcomings of the site-level model 21

3.2 Theoretical economic effects of Article 88b 21

3.2.1 Data subjects 22

3.2.2 Data controllers: publishers, e-commerce websites and online services 25

3.3 Overview of the Commission impact estimates for Article 88b 34
3.3.1 User-side effects 34
3.3.2 Firm-side effects 37
3.4 Unaddressed channels 38
3.4.1 Additional user-side effects 39
3.4.2 Firm-side effects 40
3.4.3 Data intermediaries (browsers, CMPs, and others) 42
3.5 Legal and interpretive questions 43

4 Policy options 44
4.1 Signal design and defaults 44
4.2 Coherence with the broader legal framework 45
4.3 Differentiated treatment across purposes and actors 46
4.4 Implementation, experimentation and monitoring 47

5 Conclusion 48

Glossary 50

References 52

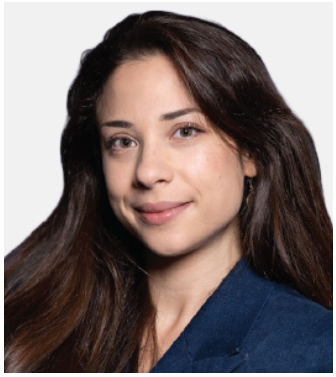
About the authors



Professor Francesco Decarolis

Francesco Decarolis is a full professor of economics at Bocconi University, Milan, where he specialises in industrial organisation, competition economics, public procurement and the regulation of digital markets.

He is a CEPR research affiliate and associate editor of Econometrica and the Review of Economic Studies. He has advised the European Commission, the Italian government and antitrust authorities, and has coordinated major European Research Council projects on public procurement integrity and competition in digital markets.



Cristiana Firullo

Cristiana Firullo is a PhD candidate in information science at Cornell University and an IvyPlus scholar at Stanford University's Department of Economics. Her research focuses on behavioural and industrial organisation economics, exploring how data protection rules and personalisation algorithms affect market outcomes and consumer welfare.

She previously worked at Oxera Consulting LLP (Oxford, UK), where she specialised in antitrust and economic analysis for digital firms. Cristiana holds a BSc and MSc in economics from Bocconi University (Milan). She has research experience in economics and information systems, primarily through large-scale field experiments examining how users respond to choice architectures and online advertising environments.

Acknowledgements

This paper builds on earlier research published in November 2025, entitled "Unlocking growth: exploring the economic impact of GDPR for tomorrow's Europe". It is published by Professor Francesco Decarolis, Full Professor in the Department of Economics at Bocconi University, Cristiana Firullo, PhD Candidate at the Department of Information Science at Cornell University and the law firm Clifford Chance LLP.

Clifford Chance LLP contributed to the development of the paper by supporting the research process, including input on relevant legal and regulatory considerations.

We are grateful to Amazon for providing financial support for this paper.

Disclaimer

The views expressed in the paper are solely those of Professor Decarolis and Cristiana Firullo and any inaccuracies or oversights are their sole responsibility. Nothing contained herein should be construed as legal advice or an endorsement by Clifford Chance LLP or Bocconi University.

While this work has received financial support from Amazon, neither Amazon nor any other stakeholder bears responsibility for its final content.

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals, nor is it designed to provide legal or other advice.

Supported by
amazon

Executive summary

The Digital Omnibus delivers a measured and largely well-targeted simplification of the EU's data protection framework. The consolidation of breach reporting, the harmonisation of data protection impact assessments (DPIAs), the clarification of automated decision-making, and the introduction of a legitimate-interest basis for AI training collectively respond to the simplification mandate articulated in the Draghi and Letta Reports. Within the boundaries of the Digital Omnibus's stated ambition, these are coherent and evidence-based reforms.

This paper reviews the merits of the proposed reforms in the Digital Omnibus along the dimensions outlined above, and then focuses on a key provision, Article 88b GDPR that introduces a new horizontal architecture under which user consent is communicated through automated, machine-readable signals at the level of the browser or operating system – which we often refer to as "centralised consent management" in this paper.

Whether the Article 88b proposals are adopted in their current form or not, it is hoped that the analysis advanced in this paper will be a valuable contribution to any debate about centralised consent management approaches.

By relocating consent capture from the website to the browser layer, the provision concentrates the effective control of consent to a small set of intermediaries whose incentives are not necessarily aligned with those of users, controllers, or the open web. As such, it triggers a chain of supply-side adjustments in the advertising value chain, to SMEs and independent publishers, and to the Adtech industry; and it does so on the basis of a design specification that is delegated to a subsequent (undefined) standards process. These effects are not addressed in the Commission's own Staff Working Paper, which estimates only the direct user-side benefits and the direct compliance-cost savings for businesses.

The analysis is based on a combination of economic theory, empirical evidence from the economics of privacy literature, including studies of the market effects of the GDPR (Aridor, Che and Salz 2023; Peukert et al. 2022; Johnson et al. 2023), cookie consent requirements (Johnson and Shriver 2024), and Apple's App Tracking Transparency (ATT) framework (Skiera and Koschella 2023; Aridor et al. 2025; Deisenroth et al. 2024), and insights from comparable regulatory interventions. It identifies the main mechanisms through which the Digital Omnibus is expected to operate, and evaluates their likely effects on competition, innovation, compliance costs, and the effects on users. For provisions whose effects remain uncertain, the analysis adopts a structural approach, mapping the relevant causal channels and the design parameters that determine the direction and magnitude of the outcomes.

This study traces four channels through which centralised consent management, as proposed in Article 88b, are likely to operate:

1. **On competition**, the centralisation of consent capture at the browser and operating-system level risks creating a new class of consent gatekeepers and strengthens the position of intermediaries already well placed in first-party data collection.

2. **On digital advertising markets**, reduced availability of cross-site behavioural signals operates as a de facto tax on personalised advertising, redistributing spend toward platforms that can identify and profile users through their own login systems and first-party data (e.g., e-commerce or social platforms where users are signed in), and compressing the open programmatic ecosystem on which independent publishers rely.

3. **On SMEs and independent publishers**, the loss of access to data flows is particularly damaging because, unlike large platforms, they have no comparable alternative: they cannot fall back on logged-in user data or subscription revenue at scale. A similar pattern arose following Apple's ATT framework where the costs fell disproportionately on smaller players, while firms with large first-party data reserves were better positioned to adapt.

4. **On consent fatigue**, it eliminates a friction without resolving the informational failures that have made site-level consent ineffective, and risks eroding the supply of ad-funded services on which a substantial share of users, SMEs and independent publishers currently rely.

The impact of these effects ultimately depends on five design parameters that the current text of Article 88b leaves unspecified: the granularity of the consent signal, the configuration of the default setting, the relationship between Article 88b and non-consent legal bases such as legitimate interest, the degree of differentiation across purposes of processing and types of actors, and the architecture through which implementation is monitored and adjusted over time. This paper distils these into four policy levers: the design of the signal and its defaults; the coherence of Article 88b with the broader legal framework; the differentiation of obligations across purposes and actors; and the implementation, experimentation and monitoring of the new regime.

Legislators may wish to consider the following policy options from this analysis, with the goal of understanding the economic effects of the regulation:

1. First, the parameters that determine economic outcomes, namely increases or reductions in consumer or firms' surplus, should not be left entirely to the standards process foreseen in Article 88b(4). These choices are substantively political and have first-order economic consequences and therefore require a higher degree of transparency and accountability in their determination.

2. Second, legislators should assess in advance and monitor how the costs and benefits of Article 88b are distributed across firms of different sizes. Aggregate cost–benefit estimates can mask sharply uneven effects: an intervention that produces net savings on average may still impose severe losses on SMEs and independent publishers while leaving larger players largely unaffected. This is not an argument for applying different standards to different firms (addressed separately in Section 4.3), but for measuring distributional effects before the architecture is locked in place.

3. Third, the interaction of Article 88b with the broader legal framework should be clarified before it enters into force, in particular with respect to alternative legal bases and overlapping regulatory obligations such as the consent requirement under the ePrivacy Directive for non-personal data, in order to avoid creating additional uncertainty where the Digital Omnibus aims to reduce it.

4. Fourth, the implementation pathway should incorporate mechanisms for experimentation, adjustment, and monitoring given the irreversibility of an intervention that will, by construction, reshape the consent surface for digital services in the EU.

The wider lesson that the Digital Omnibus exercise leaves for the next stage of EU data regulation, including the Digital Fitness Check and the broader GDPR review process, is that the trade-offs at issue do not run along a single binary axis. The economic implications of a data protection intervention depend on what it restricts, on whom, and through which channel. A framework that does not differentiate along those dimensions will continue to produce outcomes that diverge, sometimes sharply, from its stated objectives. Article 88b illustrates the cost of that omission. The opportunity ahead is to address it before the next round of reform repeats it.

1 Introduction and overview

This paper provides an economic assessment of the Digital Omnibus, with particular attention paid to the proposed new Article 88b GDPR. This would be a fundamental change to consent management infrastructure, however, a meaningful economic impact assessment of its expected market effects has not yet been conducted. This paper seeks to explore some of the issues and questions that any such study would likely cover.

This paper builds on earlier evidence on the economic consequences of EU data protection law, notably regarding compliance costs, regulatory fragmentation, and consent fatigue. Whereas prior work documented these outcomes after nearly a decade of the GDPR, the present analysis shifts perspective to an evaluation of how proposed measures under the Digital Omnibus are likely to impact market participants, from independent retailers and SMEs to advertisers, publishers, and consumer choice.

In November 2025, the European Commission proposed the Digital Omnibus, the most ambitious attempt to date to simplify and consolidate the EU's data regulatory framework. The Digital Omnibus proposes to amend the GDPR, the ePrivacy Directive, the Data Act, and the NIS 2 Directive, while repealing the Data Governance Act, the Free Flow of Non-Personal Data Regulation, the P2B Regulation, and the Open Data Directive. Our overall assessment, developed in the sections that follow, is that the proposed package substantially delivers on its simplification objectives. Article 88b, however, is a notable exception. Rather than streamlining existing obligations, it introduces a new horizontal requirement that users must be able to express their preferences regarding access to and processing of data stored in terminal equipment through "automated, machine-readable signals", communicated at the level of the browser, operating system, or comparable software environment. Controllers are required to recognise and comply with these signals across services, effectively centralising consent capture within browsers, operating systems, or a limited number of consent management platforms (CMPs), at the expense of smaller platforms and independent retailers. This browser level consent architecture is layered on top of existing consent requirements under the GDPR and ePrivacy Directive. In this respect, Article 88b contradicts the simplification aims of the Digital Omnibus and the Commission's recognition that the accumulation of rules has adversely affected Europe's competitiveness.

The Digital Omnibus is itself best understood against the backdrop of a substantially altered global context. The European Union's share of global GDP has declined from approximately 22% in 2015 to roughly 14% in 2024, while other major economies, notably China and the US, have kept on growing at a substantially faster pace than Europe. The technological acceleration associated with AI has further reshaped the European debate on data regulation, raising the strategic value of large-scale, diverse datasets and exposing frictions in the existing data-protection framework. Initiatives like the recent World Data Organization launched in China at the end of March 2026 exemplify an emerging tri-polar landscape. In this context, the Digital Omnibus is most accurately understood not as a marginal refinement of a dominant regulatory model but as a response to the risk of furthering a condition of diminished economic gravity and a loss of opportunity to catch up in the most innovative economic sectors. Consistent with this framing, the methodological commitment of this paper is to practically identify and single out rules and provisions that have demonstrably worked from those that have not, rather than defending the existing regulatory architecture as a whole or rejecting the proposed simplifications in isolation.[1]

Different stakeholders draw sharply different conclusions about what Articles 88a and 88b would mean for market participants.[2] The central concern, voiced by parts of the advertising and publishing industry, is that Article 88b, and other centralised consent mechanisms, would concentrate a critical function in a small number of intermediaries such as browsers, operating systems and a small number of consent-management platforms, which would risk amplifying their market power and distorting competition. Smaller platforms and independent retailers might lose the ability to engage their customers directly and to communicate the value of their personalised services, which translate into lower advertising revenues for them and publishers that rely on data-driven monetisation. These concerns are not merely theoretical. In December 2025, the Italian Competition Authority (AGCM) fined Apple €98.6 million for abuse of a dominant position, finding that its ATT framework unilaterally imposed asymmetric consent requirements on third-party developers and that equivalent privacy protection could have been achieved through means less restrictive of competition.[3] The empirical literature points the same way: privacy interventions of this kind reduce consent rates and advertising revenue, with the sharpest losses concentrated among smaller operators that cannot fall back on first-party data (Kraft, Skiera and Koschella 2023; Aridor et al. 2025).

This paper has a dual purpose. First, it provides a concise assessment showing that the Digital Omnibus largely achieves its simplification objectives. Second, it focuses on the provision introducing automated, machine-readable consent mechanisms at the browser level (via Article 88b) and studies the possible effects on competition, digital advertising markets, SMEs, and consumers. Importantly, Article 88b is one of the very few proposed provisions whose material economic and competition effects remain untested. Unlike the bulk of the package — whose simplification benefits are well documented and broadly uncontested — Article 88b introduces a structural change to the architecture of online consent whose downstream effects on competition, advertising markets, and benefits for consumers have not been empirically assessed. This makes legislative calibration especially critical, as the design choices made at this stage will determine whether the provision delivers on its simplification objectives or instead introduces additional complexity and generates material market distortions that are difficult to reverse once the mechanism is deployed at scale.

We note that, while the rest of the Digital Omnibus package aims to alleviate compliance burdens and streamline overlapping obligations, Article 88b GDPR introduces a new mandatory technical and compliance architecture and an internal inconsistency which is likely to add to the regulatory burden. We flag some of the key concerns here.

1 The two studies document the fragmentation of cross-border data governance: the first maps how data transfer rules increasingly diverge across jurisdictions, while the second proposes a multilateral "World Data Organization" to bridge the resulting institutional gap. See Rong, K., Ling, Y., Yang, T., & Huang, C. (2025). Cross-border data transfer: patterns and discrepancies. Journal of International Business Policy. https://doi.org/10.1057/s42214-025-00209-7 Rong, K., Liu, T., Zhao, C., Kou, H., & Yang, T. (2026). World Data Organization: Filling the Institutional Gap in Cross-Border Data Governance. Journal of Digital Economy. https://doi.org/10.1016/j.jdec.2026.04.001

2 See the joint position of German business associations of 13 March 2026 criticising Articles 88a–88b for undermining data-driven business models and market structures, and the EDPB–EDPS Joint Opinion 2/2026 (10 February 2026), which supports simplification objectives but raises concerns about legal certainty, safeguards, and the impact on fundamental rights.

3 AGCM, decision of 22 December 2025, fining Apple €98.6 million under Art. 102 TFEU for abuse of dominance in relation to its App Tracking Transparency framework (press release A561). Accessible at https://en.agcm.it/en/media/press-releases/2025/12/A561

1. **Competition:** Article 88b concentrates the technical point of consent capture within browsers and operating systems. This has the potential to effectively create a new class of "consent gatekeepers" and amplifies the market power of intermediaries already well-positioned in first-party data collection. By concentrating user data collection between a smaller pool of actors, this can undermine SMEs' ability to compete in the advertising ecosystem, making it difficult or impossible for smaller platforms and independent retailers to directly engage with their customers and personalize their experiences. Moreover, Article 88b is likely to transform rather than simply eliminate the role of Consent Management Platforms ("CMPs"). By shifting consent capture toward browsers, operating systems or standardized machine-readable signals, the provision might reduce the value of banner-centric CMP services. At the same time, it might strengthen CMPs capable of becoming the technical and legal infrastructure layer for interpreting browser-level signals, maintaining audit trails, ensuring interoperability with the TCF and other standards, and translating general signals into GDPR-compatible, purpose-specific consent. The recent creation of the European CMP Association (ECMPA), co-founded by Usercentrics, Axeptio, Didomi and iubenda in March 2026, is consistent with this interpretation. European CMP providers appear to view Article 88b not as a marginal simplification, but as a structural redesign of the consent infrastructure in which they need a collective voice.
2. **Digital advertising markets:** non-media advertisers have limited independent access to first-party data, whereas media publishers will benefit from sector-specific exemptions to retain such access. Advertising expenditure would therefore be liable to shift toward publishers who are able to continue offering personalised inventory, compressing the diversity of the advertising ecosystem and strengthening large, vertically integrated platforms relative to the open web.
3. **SMEs:** centralised consent mechanics deprive smaller platforms and independent retailers of the opportunity to engage directly with customers and to communicate the value of personalised experiences.
4. **Consumers** who will lose the ability to express differentiated preferences across brands, sectors and service types – a design which risks masking rather than solving the information frictions that consent instruments are meant to address.

2 The Digital Omnibus – a high-level overview

In a recent review study that was released right before the publication of the Digital Omnibus, we conducted an extensive review of the economic impacts of the GDPR, which considered the rich economic and business analyses conducted in a decade of this regulation. That study, titled "Unlocking growth: exploring the economic impact of GDPR for tomorrow's Europe" (Unlocking Growth, henceforth) was motivated by the observation that Europe faces a critical moment where slow growth, heavy regulation, and rising geopolitical pressures are pushing policymakers to simplify rules and boost competitiveness. While reforms have been proposed, the aim of that study was to offer a deep understanding of the main economic challenges created by data protection laws and to illustrate a series of effective and proportionate policy options for better data regulation choices to improve Europe's innovation and growth prospects. In particular, the highlighted policy options were aimed at enhancing coherence, restoring proportionality, rationalising data subject rights and resolving regulatory fragmentations.

This section of the study provides a high-level overview on whether the Digital Omnibus is aligned with such policy options, and, relatedly, whether the package delivers on its simplification objectives. We distinguish between (i) provisions whose expected effects can be assessed based on economic theory, existing evidence and regulatory experience, and (ii) provisions – notably Article 88b – where the effects remain open and warrant closer examination at this stage, given both the novelty of the proposed mechanism and the complexity of the markets it would reshape.

2.1 The quest for changes

The Digital Omnibus does not emerge in a vacuum, but it responds to a sustained line of policy diagnosis that has identified the current data protection and digital regulatory framework as a structural drag on innovation, investment and competitiveness in the European Union, particularly for SMEs. In Unlocking Growth, we offered a systematic empirical and economic assessment of the operating impact of the GDPR and articulated the principal directions for legislative reform.[4] It is against this diagnosis that the simplification ambitions of the Digital Omnibus should be evaluated. In Unlocking Growth, we identified five interconnected sources of economic frictions arising from the current framework: compliance burdens, innovation effects, user-side frictions, regulatory fragmentation and SMEs vulnerability.

4 See Decarolis, F., Firullo, C. (2025), "Unlocking growth: exploring the economic impact of GDPR for tomorrow's Europe", November. Available at https://www.cliffordchance.com/content/dam/cliffordchance/Thought_Leadership/unlocking-growth-economic-impact-of-gdpr-decarolis-firullo.pdf

1. **Compliance burdens.** The bulk of GDPR-related cost falls not on the one-off technical investments undertaken around 2018, but on the ongoing operational layer the regulation generates: legal interpretation, documentation, monitoring, periodic auditing, and the upkeep of records of processing. This pattern reflects a fundamental feature of the GDPR's principles-based design, whose interpretive uncertainty translates directly into recurring operational expenses, and is amplified by the unresolved interaction between the GDPR and the ePrivacy Directive. The cumulative layering of more recent instruments (the Digital Services Act (DSA), Digital Markets Act (DMA), Data Act, AI Act, NIS2) adds further governance and reporting obligations onto the same data flows, with recent estimates suggesting that the aggregate cost of EU digital rules could approach €124 billion per year (Foy et al. 2025). Because these costs are largely fixed (Demirer et al. 2024), they weigh disproportionately on SMEs and have contributed to the rise in market concentration observed in data-heavy industries after 2018 (Frey and Presidente 2024).

2. **Innovation effects.** There is evidence of a measurable contraction of innovation activity in EU data-intensive sectors after 2018. Venture capital investment in EU startups fell relative to the U.S., with effects concentrated among younger and more data-intensive firms (Jia et al. 2021), and a transatlantic "pullback" of US-led deals in EU ventures has been documented in subsequent work (Jia et al. 2025). The slowdown is also visible at the product level: the mobile-app market saw higher exits without proportional new entry, in what one study describes as a "lost generation of innovative products" (Janßen et al. 2022), and post-2018 EU developers have shifted toward fewer, larger SDK providers, with potentially anticompetitive consequences (Jin et al. 2024). Beyond the financing channel, the GDPR's principles-based design generates persistent uncertainty over the lawful basis for novel processing activities, particularly for AI model training, which has led to the postponement or relocation of data-intensive projects to less-regulated jurisdictions.

3. **User-side frictions.** It is well known how enhanced data subject rights have improved user transparency but have only partially translated into economic benefits. A consolidated body of work in privacy economics (Acquisti, et al., 2015 and 2016) has documented those behavioural frictions, including bounded rationality, decision fatigue, present bias, and heterogeneous preferences, which systematically limit users' ability to exercise their formal rights, producing a persistent gap between protective intent and experienced outcomes.[5] The privacy paradox, first formalised in this literature and subsequently quantified in field studies such as in Athey et al. (2017), captures this gap. Stated privacy preferences correlate only weakly with revealed consent decisions, which are heavily shaped by interface design, defaults and prompt framing (Acquisti et al., 2017, Lupiañez-Villanueva et al. 2022).[6] Farronato et al. (2025) test consent behaviour under what they label a "neutral" design, namely a consent interface in which the accept and reject options are equally prominent, require the same number of clicks, and use non-steering language. They find that more than half of users continue to accept tracking even under those conditions. This isolates a cognitive component to the consent failure that interface reform alone cannot resolve and that undermines the informed-consent assumption on which much of the regulatory framework rests.[7]

4. **Regulatory fragmentation.** Although the GDPR is directly applicable, its enforcement has been markedly inconsistent across Member States. National data protection authorities (DPAs) retain significant discretion in interpreting key provisions such as legitimate interests, the conditions for valid consent, and in setting enforcement priorities. Unlocking Growth highlights how this divergence interacts with covert incentives at the supervisory level, including career concerns and visibility-driven enforcement, producing patterns of intervention that are neither fully predictable nor uniform across the single market. The continued presence of the ePrivacy Directive alongside the GDPR adds a further layer of inconsistency, particularly on cookies and online data collection. For firms with cross-border operations, the practical result is duplicative compliance work, parallel legal review, and a "race-to-the-top" adjustment to the strictest national interpretation, all at odds with the Single Market objective the GDPR was meant to advance.

5 Acquisti, A., L. Brandimarte and G. Loewenstein (2015). "Privacy and Human Behavior in the Age of Information." Science 347(6221): 509–514. Acquisti, A., C. Taylor and L. Wagman (2016). "The Economics of Privacy." Journal of Economic Literature 54(2): 442–492.

6 Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang and S. Wilson (2017). "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." ACM Computing Surveys 50(3): 1–41.

7 Farronato, C., Fradkin, A. and Lin, T., 2025. Designing consent: Choice architecture and consumer welfare in data sharing (No. w34025). National Bureau of Economic Research.

5. **SMEs vulnerability.** The GDPR's compliance costs are largely fixed and indivisible (Demirer et al. 2024; Gal and Aviv 2020), so they weigh much more heavily on SMEs than on large platforms with mature compliance functions. Exposed firms have experienced on average an 8% drop in profits and a 2% drop in sales (Frey and Presidente 2024), data-acquisition costs have risen by roughly 20% (Demirer et al. 2024), and web traffic and e-commerce revenues in segments reliant on third-party data have fallen by 11.7% and 13.3% respectively (Goldberg et al. 2024). Because smaller firms cannot easily absorb these costs, formal or effective non-compliance is widespread, generating a moral hazard problem and a competitive landscape tilted in favour of large incumbents that can build full compliance infrastructures. The downstream effect, particularly visible in digital advertising and data-driven services, is a shift toward first-party data and a weakening of cross-firm data ecosystems, with independent controllers and processors progressively squeezed out — precisely the kind of dynamic the Digital Omnibus simplification ambitions are meant to address.

   To address this diagnosis, the Unlocking Growth study identified four policy options (PO): enhancing regulatory coherence and consistency through harmonised European Data Protection Board (EDPB) guidance and simplified certification mechanisms (PO1); promoting proportionality through risk-based approaches and regulatory sandboxes (PO2); clarifying and rationalising data subject rights, including explicit criteria for excessive requests and standardised assessment tools (PO3); and simplifying overlapping frameworks, in particular by aligning the GDPR with the ePrivacy regime and permitting alternative lawful bases for non-intrusive processing (PO4). Each of these directions maps onto one or more of the friction channels just described: PO1 and PO2 address compliance burdens, regulatory fragmentation and SME vulnerability; PO3 targets the residual frictions on the user side and the costs generated by disproportionate procedural obligations; and PO4 speaks both to the operational cost layer and to the consent-related frictions stemming from the unresolved GDPR–ePrivacy interaction. Together, these four policy options define the simplification mandate against which the Digital Omnibus can most coherently be evaluated.

2.2
Economic rationale behind the Digital Omnibus

We identify and discuss five economic mechanisms through which the Digital Omnibus is expected to produce its effects: reducing compliance costs, promoting innovation, strengthening legal certainty, improving benefits for consumers, and levelling the competitive playing field between large platforms and smaller firms.

2.2.1.
Compliance costs

The most direct and measurable channel through which the Digital Omnibus is expected to deliver value is the elimination of duplicative obligations. Breach reporting is consolidated through a single-entry point via the European Union Agency for Cybersecurity (ENISA), replacing 27 separate DPA notification procedures with a common template, a harmonised threshold, and a 96-hour deadline (Art. 33–34). However, there are risks with maintaining a single-entry point of failure, as inconsistences in reporting terminology and thresholds can create a centralisation risk, with the broad dissemination of sensitive data running counter to key operational resilience and security principles under the GDPR. National Data Protection Impact Assessment (DPIA) lists — which required cross-border controllers to consult up to 27 divergent frameworks — are replaced by a single EU-level list (Art. 35). And Art. 88a consolidates cookie-related processing involving personal data under a unified GDPR-based framework, effectively creating a One Stop Shop for cookie enforcement and remedying the current divergent approach to cookie enforcement at a Member State level and the related compliance inefficiencies. However, this simplification is partial rather than complete: where cookie-related processing does not involve personal data, Art. 5(3) of the ePrivacy Directive continues to require consent for the storage of, or access to, information on end-users' terminal equipment. Controllers handling mixed cookie estates will therefore remain subject to both regimes. This is precisely where Article 88b changes the assessment. While Article 88a reduces fragmentation by moving cookie-related processing of personal data into a GDPR-based enforcement structure, Article 88b introduces a separate technical layer for machine-readable consent signals. Unless its interaction with the GDPR, the residual ePrivacy regime and the DMA is clarified, the provision risks reintroducing uncertainty at the implementation stage rather than reducing compliance costs.

The reform of Data Subject Access Requests (DSARs) (Art. 12) reduces the operational burden of manifestly excessive or abusive requests. In each case, the mechanism is straightforward: fewer obligations, fewer forms, fewer hours — lower costs. However, where other proposed provisions would reduce uncertainty, Article 88b's introduction of automated, machine-readable consent mechanisms at the browser level with undefined specifications, is likely to lead to an increase in compliance costs, contrary to the Digital Omnibus' simplification agenda and the Commission's objective of ensuring compliance with the EU's data protection framework comes at a lower cost. We tackle this in Section 3.

2.2.2. Innovation

A defining feature of EU technology regulation, setting it apart from both the United States and China, has been its systematic neglect of innovation as a policy objective, despite innovation being the primary engine of productivity growth and long run effects in digital economies. As the Draghi Report forcefully argues, the central weakness of Europe's digital rulebook is not that it protects the wrong values, but that it consistently fails to engage with how regulation shapes incentives to innovate. The GDPR is emblematic in this respect: notwithstanding the centrality of personal data to modern digital services, the concept of innovation does not appear once in its text.[8] Against this backdrop, the Digital Omnibus marks a notable shift in tone: "innovation" appears thirty three times in the proposal, raising the question of whether this rhetorical change is matched by meaningful reform. Accordingly, the analysis that follows assesses the Digital Omnibus on its merits, distinguishing provisions that genuinely advance the innovation objective from those that do not.

Indeed, the Digital Omnibus attempts to remove several regulatory barriers that the Unlocking Growth study identified as deterrents to data-intensive innovation in the EU. The new legitimate interest basis for AI training (Art. 6(1)(f)) allows processing without explicit consent, subject to appropriate safeguards and an unconditional right to object — addressing a structural competitive disadvantage relative to non-EU jurisdictions. However, the clarification of automated decision-making (ADM, Art. 22) offers incremental rather than substantial progress. By confirming that contract-based ADM is lawful regardless of whether a human could have decided — while preserving the right to human review – the amendment resolves a narrow interpretative dispute but leaves the broader architecture of Art.22(1) untouched. The exemptions remain too narrow: as fraudsters deploy AI-generated synthetic identities and deepfakes at scale, the efficient detection and blocking of such activity depends on automated tools that the current Art.22 exemption framework does not straightforwardly authorise.

8 The GDPR does contain limited, indirect references that can be associated with innovation objectives. Most notably in Recitals 4, 7 and 50, which emphasise the need to balance data protection with other fundamental rights such as the freedom to conduct a business, and to allow further processing under conditions of compatibility. In addition, the framework for scientific research and certain lawful bases (including legitimate interest) has been interpreted as enabling data-driven activity in specific contexts. However, these elements remain implicit, fragmented, and operationalised primarily as exceptions or balancing clauses, rather than as a structured or affirmative innovation mandate. As such, they do not amount to an explicit recognition of innovation as a core regulatory objective within the GDPR architecture.

2.2.3.
Legal certainty

Regulatory uncertainty imposes costs even when the underlying rules are sound because firms must invest in interpreting ambiguous obligations rather than in productive activity. Digital Omnibus reduces this friction at several points. The harmonisation of DPIA criteria and breach reporting thresholds eliminates the need for country-by-country legal analysis. And Art. 88a's replacement of the fragmented ePrivacy and GDPR cookie consent regime with a single One Stop Shop for enforcement aims to resolve a decades-old source of legal ambiguity.

One key provision in this area deserves specific attention. The proposed clarification of the definition of "personal data" (Article 4(1) GDPR) sought to reflect the CJEU's approach in EDPS v. SRB (C 413/23 P), under which pseudonymised data is not automatically personal data for a given entity where that entity does not have means reasonably likely to re-identify the individual. If adopted, a major "if" as public commentary from Member States' authorities, DPAs and certain lawmakers reflects strong criticism, the amendment would reduce compliance costs for a substantial set of processing activities—particularly in analytics, AI training, and health research—and would shift the longstanding debate on identifiability toward a more explicitly entity-relative assessment. However, as alluded to above, subsequent legislative review discussions indicate that this provision is unlikely to be retained as proposed. The opposing voices include a joint EDPB–EDPS opinion criticising its "negative" formulation and concerns expressed by several Member States that it would unduly narrow the material scope of EU data protection law. Whether a revised version re-enters the text during negotiations remains to be seen. Article 88b, by contrast, introduces a novel obligation with undefined technical specifications, an uncertain scope, and unresolved interactions with existing GDPR legal bases—thus re-introducing legal and economic uncertainty precisely where the rest of the package aims to remove it.

2.2.4.
Effects on consumers

The provisions above also generate direct benefits for data subjects. Art. 88a's six-month moratorium on re-requesting refused consent, combined with the exemptions for audience measurement and service security, substantially reduces consent fatigue, which is the most visible friction in the current regime. The clarification of data subject rights under Art. 12, while restricting the scope for excessive requests, preserves access for individuals with genuine informational needs.

2.2.5.
Competitive dynamics

Several provisions address the Unlocking Growth study's finding that regulatory complexity disproportionately burdens smaller firms. The single DPIA list and the single-entry point for breach reporting is expected to remove fixed compliance costs that fall more heavily on SMEs. The legitimate interest basis for AI reduces a barrier that previously advantaged large firms with the resources to obtain and manage explicit consent at scale. And the extension of SME simplifications to small mid-caps broadens the scope of proportionate treatment. The mechanism is well-understood: when regulatory costs are partially fixed, simplification disproportionately benefits smaller firms and reduces the competitive advantage that incumbents derive from their ability to absorb compliance overhead. At the same time, existing evidence suggests that not all privacy interventions produce this levelling effect, as we will discuss in the next section.

2.3
The intended and unintended effects of Article 88b GDPR

Despite the valuable simplification proposals in the Digital Omnibus described above, Article 88b is likely to have significant intended and unintended consequences. This provision introduces a requirement for controllers to ensure that their online interfaces can interpret automated, machine-readable browser/device-level user consent signals. The economic rationale behind the proposal rests on a simple trade-off: higher implementation costs for browser providers, who must offer the required technical means, in exchange for lower cognitive costs for users, who would no longer need to express their privacy preferences site by site. However, as discussed in Section 2.1, this trade-off is far from exhaustive. Article 88b carries potential regulatory risks for both users and firms across each of the five mechanisms examined above. More fundamentally, its economic effects cannot be assessed on the basis of the existing evidence alone — because the channels through which it operates are multiple, indirect, and partially offsetting.

Beyond these direct and indirect effects, Article 88b also generates interactions with other provisions in the package and other EU digital laws that could produce additional complexity. The interaction with AI training should be framed narrowly. Article 88b does not generally override the legitimate-interest basis introduced for AI training under Article 6(1)(f). The interaction arises only where the relevant training data are obtained through access to, or processing of, information stored in users' terminal equipment. In those cases, a browser-level refusal signal could reduce the data available for AI training even where the GDPR lawful basis is available. Where training data are collected independently of terminal-equipment processing, the two regimes operate separately. If Article 88b layers a separate technical standard and exemption structure on top of Article 88a, it risks reintroducing the regulatory fragmentation that 88a was designed to eliminate. In addition, companies who are designated as 'gatekeepers' under the EU Digital Markets Act (DMA), will still be required to obtain consent under Article 5(2) DMA for various types of processing, in addition to the consent requirements introduced by the Digital Omnibus, undermining much of the efforts to improve consent fatigue that this proposal is designed to resolve. Moreover, the combination of Article 88b with the residual ambiguity around the definition of "personal data" in Article 4(a) concentrates the cost of adaptation on actors that lack alternative monetisation architectures, including small and medium-sized enterprises and independent publishers.

In what follows, Section 3 reviews the available evidence: from the academic literature, the Commission's Staff Working Paper, and real-world precedents such as Apple's ATT to assess what is known about each of these channels and where the evidence falls short. It then identifies the type of analysis that would be needed to resolve the open questions before Article 88b's design is finalised. Throughout the analysis that follows, we treat the Commission's November 2025 proposal as the baseline text, while noting that the design choices identified below are precisely the issues that any subsequent legislative negotiation would need to resolve.[9]

9 As we will discuss in Section 4.1, the most consequential revision reframes the obligation by requiring consent to be expressed "for specific categories of purposes" rather than as a single binary signal. These texts are not agreed positions and the final wording may differ; we treat them only as indicators of the direction of travel within Council. Their content converges with several of the policy options examined in Section 4, and we return to it in Section 4.1.

3 Article 88b: open questions and trade-offs

Article 88b introduces a structural change in the consent architecture that underpins the EU's data protection ecosystem. By shifting consent from the website level to the browser level, it alters the relationship between every category of market participant: data subjects, who no longer express preferences site by site; controllers, who must interpret and respect an automated signal they did not design (Art. 88b(1)); browser providers who become the infrastructure through which consent is communicated (Art. 88b(6)); and processors, whose business models depend on the cross-site data that the signal is designed to restrict. But Article 88b's influence extends well beyond data protection. It has substantial implications for the digital advertising ecosystem that represents the primary economic engine through which free online content and services are funded. By restricting the availability of tracking data for non-essential purposes, Article 88b triggers a chain of market adjustments: a shift from behavioural to contextual advertising, a redistribution of advertising expenditure across market participants, and a potential contraction in the supply of ad-funded services available to consumers. These effects are not addressed in the Commission's Staff Working Paper, which estimates only the direct user-side benefits (reduced consent fatigue) and the direct compliance cost savings for businesses.

This section proceeds in three parts. First, it describes the consent architecture ecosystem. Second, it sets out the theoretical economic effects of Article 88b on each category of market participant, tracing the causal channels through which the provision is expected to alter incentives, revenues, and market structure. Third, it reviews the available empirical evidence — from the academic literature, real-world precedents, and the Commission's own impact assessment — evaluating what is known, what is assumed, and where the evidence falls short.

3.1 The current consent architecture

When a user visits a website in the EU, the controller must obtain consent before placing non-essential cookies or conducting non-essential device-based processing. In practice, data controllers implement this through a Consent Management Platform (CMP).
The CMP presents a banner, captures the user's choices (e.g., "accept all," "reject all," or more granular preferences), stores those choices, and communicates them to the site's advertising, analytics, and measurement partners. This site-level flow governs which data can be collected and which vendors may receive it.

The need for informed consent creates a market where every involved agent sustains a specific cost. For controllers, the current regime involves both direct costs (CMP licensing fees, technical integration, ongoing maintenance) and indirect costs (legal review of consent configurations, monitoring for compliance, responding to regulatory changes in CMP settings). For users, the costs are primarily in time and attention. For the advertising ecosystem, the costs manifest as reduced data quality (because consent choices are noisy and inconsistent) and operational complexity (because each publisher's consent configuration may differ).

A foundational distinction underpins this architecture and is implicit in much of the policy debate around Article 88b: the difference between "first-party cookies" — those set by the domain the user is currently visiting, typically supporting login state, shopping carts, language preferences, the basic delivery of the service, and personalisation — and "third-party cookies", set by domains other than the one being visited and used predominantly by ad-tech intermediaries to construct cross-site behavioural profiles, and support retargeting. Under the ePrivacy Directive (Art. 5(3)), both categories are subject to a consent requirement, save for cookies strictly necessary to provide a service explicitly requested by the user.[10] However, this derogation covers most operational first-party cookies but rarely third-party ones. As a result, the consent banners that have populated the site-level architecture have always been, in economic substance, banners about third-party cookies: the elements the user is asked to evaluate, and that risk being rejected, are overwhelmingly third-party processing operations rather than the first-party functionality of the service the user has chosen to consume. This asymmetry has been reinforced by browser-level evolution independent of regulation, as in the case of Safari's Intelligent Tracking Prevention since 2017, Firefox's Enhanced Tracking Protection (default since 2019) — all of which have targeted third-party tracking while leaving first-party cookies untouched.[11]

The rest of the subsection aims to describe the current consent architecture by describing the role of Consent Management Platforms and the IAB Transparency Framework but also discuss existing evidence on the fallacies of the site-level elicitation of consent.

3.1.1. The role of Consent Management Platforms ('CMPs')

Consent Management Platforms are the infrastructure through which abstract legal consent requirements are operationalised into granular, per-site, purpose-specific decisions. They surface the user interface that elicits consent, maintain auditable records of choices and withdrawals, manage vendor lists and purpose definitions in line with EU requirements, and expose those permissions to downstream services embedded on the page. For cross-border publishers, CMPs also standardize compliance operations across properties and jurisdictions. While CMP implementations vary in quality and have been criticised for dark patterns, inconsistent design and imperfect consent signalling, they perform a concrete legal and technical function: they translate purpose-specific consent requirements into audit, interoperable signals across publishers, vendors and advertising intermediaries.

10 Directive 2002/58/EC, as amended by Directive 2009/136/EC, Art. 5(3).

11 See Wilander (2017), Intelligent Tracking Prevention, WebKit Blog, June 5. Accessible at https://webkit.org/blog/7675/intelligent-tracking-prevention/, and Mozilla Press Center (2019), Firefox Now Available with Enhanced Tracking Protection by Default, June 4. Accessible at https://blog.mozilla.org/press/2019/06/firefox-now-available-with-enhanced-tracking-protection-by-default/

Except for the US-based OneTrust, most of the leading Consent Management Platforms operating in the EU are European firms, largely because they were designed from inception to comply with GDPR requirements.[12] The leading CMP providers operate on a subscription model. Publishers pay a recurring fee that varies with the number of domains, sessions, and regulatory jurisdictions covered. For a mid-sized publisher operating across the EU, annual CMP costs can range from several hundred to several thousand euros; for large media organisations managing dozens of domains and millions of sessions, costs are significantly higher. The global CMP market was valued at approximately USD 1 billion in 2024, with Europe accounting for roughly 30% of that market.[13] In functional terms, CMPs are the translation layer between the GDPR's principles of specific, informed, granular consent and the operational reality of an ecosystem composed of hundreds of distinct processing purposes and vendors. A theoretical economic argument would be that the quality of consent they enable is substantial and it includes the ability to accept analytics but not advertising, to consent to one processor but refuse another, to calibrate consent by purpose rather than by blanket refusal.

However, the economic case for CMPs does not turn on the quality of the consent they elicit from users on which the evidence is, at best, mixed. Stated and revealed privacy preferences are only weakly correlated (Farronato et al. 2025); most users accept all processing irrespective of granularity (Nouwens et al. 2025); and the behavioural literature consistently documents that decision fatigue suppresses engagement with purpose-level controls (Acquisti et al, 2015; 2016). If anything, the weakness of elicited consent as a welfare instrument is one of the stronger arguments for reforming the GDPR's consent architecture — a concern the Digital Omnibus addresses in part.

Two features of this arrangement explain why the function is not easily replaced. First, consent is not a one-off output but a continuously maintained service: CMPs store proof of consent, propagate it to downstream processors, and keep the configuration aligned as vendor lists, legal requirements and technical standards change. A publisher could in principle build this in-house, but the recurring cost of monitoring, updating and re-integrating against a moving standard makes doing so prohibitive for all but the largest operators. Second, the IAB Transparency and Consent Framework ("TCF") illustrates the scale of the task: it took years to standardise consent signalling for programmatic advertising alone. Article 88b would require an equivalent machine-readable repository spanning every processing purpose across the entire web, which is an undertaking of a different order of magnitude, to be delivered on a statutory timeline short enough that the resulting protocol risks being obsolete by the time it takes effect.

Browsers are no more likely to take on this role. Article 88b(6) makes the browser the channel for the consent signal, but carrying the signal is not the same as running the infrastructure behind it. Browser vendors have never moved into the consent-management business: they did not buy CMPs even when CMPs were looking for buyers, and taking on the function now would expose a few large platforms to exactly the antitrust and privacy-liability risks they have worked to avoid, as the dispute over Google's Privacy Sandbox shows. Someone still must store the consent, share it with processors, and keep the system current as standards change. If publishers cannot do this cheaply and browsers will not do it at all, the work stays with the CMPs. That is why Article 88b is more likely to concentrate the sector than to empty it.

12 The leading Consent Management Platforms serving the EU market are predominantly European firms, designed from inception to comply with GDPR requirements. Germany's Usercentrics, which merged with the Danish Cybot (parent of Cookiebot) in 2021, is among the largest. France hosts Didomi (enterprise-focused) and Axeptio (design-centric); Italy's iubenda and Germany's Consentmanager serve the SME segment. Non-EU providers with meaningful EU market share include the U.S.-based OneTrust, Osano and Sourcepoint (the last headquartered in New York but with offices in London, Berlin and Paris), and the U.K.-based CookieYes — all of which operate European data and contractual infrastructures to meet EU regulatory requirements.

13 Values estimated between USD 0.7 – 1.8 billion globally in 2024/2025, based on different scope definitions. See Straits Research (2025), Market Reports World (2026), and Business Research Insights (2026).

3.1.2.
The IAB Transparency and Consent Framework ('TCF')

The operational backbone of the current system is the IAB Europe Transparency and Consent Framework (TCF), now in its second major version (TCF v2.2). The TCF is not a CMP — it is the technical standard that enables CMPs to communicate consent decisions downstream through the programmatic advertising chain. The process works as follows. When a user makes a consent choice on a CMP banner, the CMP generates a machine-readable string — the "TC string" — that encodes exactly which purposes the user has consented to (e.g., analytics yes, personalised advertising no) and which vendors are authorised to process data on that basis. This string is then passed in real time to every participant in the ad auction where banner ads are sold, typically in real time: the supply-side platform, the ad exchange, the demand-side platforms, and the data management platforms. Each participant reads the string and determines whether it has legal permission to bid on, serve, or measure the ad impression. TCF adoption is widespread as most of the European publishers use TCF-compliant CMPs, and the framework is integrated into the bidding infrastructure of all major ad exchanges. This means that the current consent architecture represents a standardised, interoperable system that the programmatic advertising industry has built its operations around over several years.

3.1.3.
The shortcomings of the site-level model

Despite the substantial investment that publishers and ad-tech firms have made in TCF integration, the site-level consent model displays well-documented shortcomings that cut across users, controllers, and intermediaries. On the user side, individuals face repeated, heterogeneous prompts whose cumulative time and attention costs degrade decision quality and produce choices that do not reliably reflect actual privacy preferences (Farronato et al. 2025); implementations vary widely, and many steer users toward acceptance through unequal button prominence, multi click “reject” paths, pre-selected categories and withdrawal procedures more burdensome than initial consent. On the controller side, publishers incur ongoing work to configure banners, update vendor lists, monitor legal changes, and keep programmatic pipelines aligned with evolving standards. On the ad-tech side, because each publisher controls its own CMP configuration, the resulting consent data can be fragmented and difficult to reconcile, adding friction and uncertainty to campaign delivery and measurement. Nouwens et al. (2020) found that only 11.8% of CMP implementations in the EU met the minimum requirements of EU law. Matte et al. (2020) found that a significant proportion of CMPs registered positive consent even when users had not consented. Santos et al. (2021) found systematic non-compliance with GDPR requirements across major CMP providers. Although DPAs have issued fines for non-compliant consent practices — most notably the French CNIL's enforcement actions against Google and Facebook — enforcement remains uneven across Member States, and most non-compliant implementations operate without sanction.

3.2
Projected economic effects of Article 88b

Article 88b proposes to replace this decentralised, site-level architecture with a centralised, browser-level one. The following section analyses the theoretical economic effects of that shift on each category of market participants. We study the theoretical economic effects of Article 88b for each of the three main economic agents: **data subjects, controllers, and processors.**

3.2.1.
Data subjects

Under the current regime, users face a repeated decision problem. Each website visit presents a consent choice with non-trivial cognitive costs: the interface varies across sites, the language is often opaque, and the consequences of the choice are not immediately observable. The rational response for most users — as documented extensively in the behavioural economics literature — is to accept the default, which in practice means accepting tracking. This is the consent fatigue problem: the volume and complexity of consent requests degrade the quality of the decisions users make, producing outcomes that do not reflect genuine preferences. Article 88b addresses this by converting a repeated, high-friction decision into a one-time, low-friction setting. Farronato et al. (2025) estimate a substantial welfare improvement from browser-level consent, measured primarily through the elimination of time costs associated with repeated site-level decisions. However, the same study finds that stated privacy preferences are only weakly correlated with revealed choices, that most users dismiss consent banners without making an explicit decision, and that there is substantial confusion about what default settings do. This suggests that the economic benefits come from eliminating the cost of the decision process itself — not from producing choices that better reflect users' actual privacy preferences.

We argue that the problem of uninformed defaults is not resolved by Article 88b; it is relocated from the website to the browser, and it can cause additional unintended consequences. Whoever sets the browser's default effectively determines the outcome for most users.

What data subjects choose when they opt-in or opt-out

In the context of providing "informed" consent for the treatment of their personal data, higher privacy can simultaneously reflect higher demand for safety and lower demand for both marketing exposure and digital products. However, existing evidence shows that data subjects might not be fully informed about this choice, and they might conflate dimensions that are, in fact, analytically distinct. What surveys and consent interactions typically capture under the single heading of "privacy" bundles together at least three demands that users value differently and that point in opposite directions:

1. **a demand for free or subsidised digital products** — search engines, social media, e-commerce, AI assistants, and recommendation systems that are largely funded by the processing of personal data.
2. **a concern about data safety** — whether personal information is adequately protected against unauthorised access, breaches, and misuse; and
3. **a preference about marketing and personalisation** — whether and to what extent users want their data to be used to tailor advertising, recommendations, and service experiences.

These three demands share common roots at the level of firm implementation — the same data infrastructure simultaneously governs security, personalisation, and monetisation — but they call for different regulatory instruments. Marketing-related preferences are well served by choice-based mechanisms (consent management, opt-out tools, machine-readable signals); data safety is best served by firm-side obligations (security standards, breach notification, accountability); and the continued availability of ad-funded products depends on whether data processing remains economically viable in the first place. Collapsing the three under a single label of "privacy concern" produces aggregate signals that appear to mandate ever more restrictive consent regimes, while the underlying user demand may in fact be for safer data usage rather than less data processing and for the continued availability of services that the restriction itself would jeopardise. The literature does not generally interpret observed demand for "more privacy" as equivalent to a demand for less data processing. Rather, users often value the benefits generated by data use, including personalisation, convenience, security, and access to free services, while expressing concerns about misuse, unauthorised access, or loss of control over personal information.[14]

14 See Acquisti, Brandimarte and Loewenstein (2015); Acquisti, Taylor and Wagman (2016); Athey, Catalini and Tucker (2017); Brynjolfsson et al. (2024); Colnago, Cranor and Acquisti (2023).

In what follows, we describe both "short-term" and "long-term" effects of an opt-out centralised signal on the economic effects for data subjects, considering both direct and indirect consequences of the provisions within the ecosystem.

Short-term effects

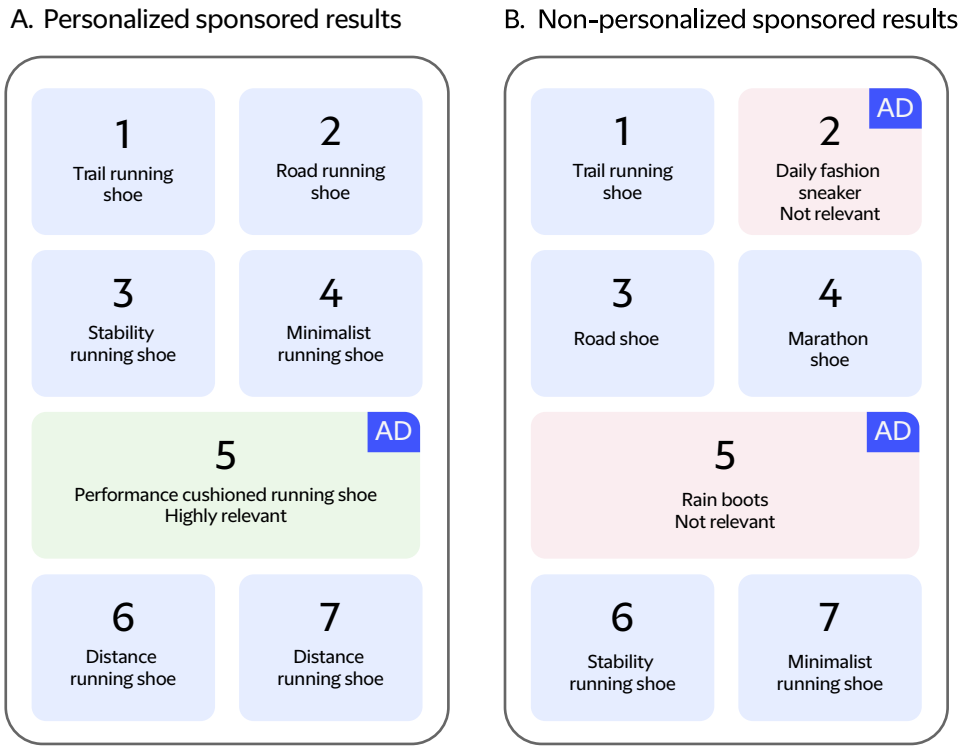
Users also depend on the quality of the services users consume, and personalisation in an empirically documented component of that quality. Evidence from large online retailers shows substantial surplus gains from personalised rankings, recommendations and discovery surfaces. These benefits flow to users through lower search costs and higher-relevance matches (Ursu 2018; Donnelly et al., 2024). Depending on its final implementation and interpretation, Article 88b may constrain the use of personal data for advertising purposes while leaving other forms of service personalisation less affected. This distinction is important because from the user's perspective, recommendations, rankings, sponsored placements, and other discovery mechanisms are often experienced as part of a single interface rather than as separate technical functions.

The resulting asymmetry within the user experience is not trivial. In many digital environments, advertising relevance derives from a combination of contextual signals (such as the content of a page, a product category, or a search query) and user-specific signals derived from prior interactions with the service. If advertising becomes more reliant on contextual signals while other parts of the service remain personalised, users may encounter a divergence between the relevance of organic recommendations and the relevance of sponsored content. This distinction should not be interpreted as a shift from relevant to irrelevant advertising. Contextual advertising can remain highly relevant and effective. Rather, the difference is between contextual relevance and personalised relevance. While contextual signals identify what may be relevant within a given environment, personalised signals can help identify what is relevant for a particular user within that environment. For some categories of products and services, the loss of this additional layer of information may affect product discovery, recommendation quality, and the overall coherence of the user experience.

Figure 1 provides an illustrative example. A user browsing a product page may receive a sponsored recommendation that is informed both by the context of the page and by previous interactions with the service. Under a more restrictive consent environment, the same recommendation may remain contextually relevant but no longer reflect information about that user's prior purchases, preferences, or browsing history. The resulting difference is not necessarily visible in every interaction, nor is it expected to be uniform across advertising formats, but it illustrates one channel through which Article 88b may affect user experience. The magnitude of these effects remains uncertain and is likely to differ substantially across formats. As discussed below, intent-triggered advertising such as sponsored search and marketplace listings is generally less exposed to these constraints than advertising models that depend more heavily on behavioural profiles and cross-site information.

Figure 1:
Example of personalised and non-personalised sponsored search results

The figures below illustrate a stylised example of how restrictions on the use of personal data may affect sponsored recommendations. In scenario (A), the recommendation is informed both by the context of the page and by information derived from the user's previous interactions with the service. In scenario (B), the recommendation remains relevant to the context but is no longer tailored to the individual user. The example is intended to illustrate the distinction between contextual relevance and personalised relevance rather than to represent any specific platform or advertising system.



More fundamentally, the effects discussed above highlight the difficulty of treating consent as a fully informed optimisation problem. A user's choice simultaneously affects privacy, personalisation, advertising relevance, service quality, and, indirectly, the economic viability of ad-funded content. These interactions are complex, vary across services, and often become visible only over time.[15] It is therefore difficult to assume that users can accurately anticipate and optimise across all of these dimensions when expressing a single consent preference. Rather than eliminating complexity, a centralised consent architecture may simply relocate it from repeated site-level decisions to a single but far more consequential choice.

15 Moreover, these interactions are impacted by multiple regulations, for instance by Article 26 of the Digital Services Act on digital advertising.

Long-term effects

Over a longer horizon, Article 88b operates through two mutually reinforcing channels of adjustment, one acting on publisher incentives and one on the broader ecosystem. The first is a dynamic adjustment on the incentive side. By shifting consent expression to a centralised, browser-level signal, the provision weakens the direct observability of data collection practices at the website level: under the current architecture users interact with individual sites and can condition their consent on perceived tracking intensity, design choices, and trustworthiness, while under the new regime the consent decision is made once, in the abstract, across all sites simultaneously. As the pool of trackable users shrinks and the marginal value of each trackable user rises, this reduction in observability can induce opportunistic behaviour by less scrupulous publishers toward the remaining consenting users. In equilibrium, this produces adverse selection on the user side, with the more privacy-sensitive users disproportionately exiting the consent pool.[16] The underlying publisher-side mechanism that drives this dynamic is developed in Section 3.2.2 below.

The second channel is a supply-side adjustment on the ecosystem. Most ad-funded services users consume depend on the revenue that Article 88b restricts, and the adverse selection dynamic above amplifies this pressure: as the consent pool thins and its composition shifts toward less-monetisable users, effective advertising revenue per user declines further, intensifying the supply-side adjustments that follow. If these adjustments reduce the availability or quality of free content, users ultimately pay for the friction reduction through a contraction in the set of services available to them. The net effect on users is therefore the sum of (i) a direct gain from reduced consent friction, (ii) a mixed effect from personalisation, service personalisation preserved, advertising personalisation lost, (iii) an equilibrium distortion arising from moral hazard and adverse selection, and (iv) an indirect loss from reduced availability of ad-funded content. Existing evidence does not allow the relative magnitudes of these four effects to be recovered, and their aggregation determines whether Article 88b improves or reduces net benefits for users. As we discuss in the next section, the implementation of Article 88b may also threaten the survival of many small online businesses whose profitability rests on their ability to monetise through advertising.

3.2.2.
Data controllers: publishers, e-commerce websites and online services

Article 88b affects data controllers through a single mechanism — a browser-level refusal signal cuts off access to non-essential processing — but its economic incidence varies sharply across business models. Controllers whose monetisation depends on third-party behavioural data used to target advertising across the web face direct revenue compression; controllers whose monetisation rests on first-party data collected through the ordinary delivery of the service, and who sell sponsored placements within their own properties, retain the core of their personalisation capacity but lose specific functionalities at the margin. Because the two models respond very differently to the same provision, any assessment of Article 88b's effects on the controller side must treat them separately.

16 Aridor et al. (2023) study the effects for different type of users after the introduction of the GDPR.

Ad-based businesses

The economics of online publishing rest on a fundamental exchange: users receive content for free, and publishers monetise the attention through advertising. The value of that advertising depends on how precisely it can be targeted. Behavioural advertising — which uses data about the user's browsing history, interests, and demographics — commands a significant premium over contextual advertising, which matches ads to the content of the page rather than the profile of the reader. However, when a browser communicates a refusal signal for non-essential processing, the controller loses access to the behavioural data that supports premium ad pricing. The controller's options are limited: shift to contextual advertising (lower revenue per impression), introduce or increase subscription fees (feasible only for controllers with strong brand loyalty), or reduce costs by lowering content quality or volume. For many categories of ad-funded services — weather forecasts, recipe databases, product catalogues, local community boards, niche local newspapers — subscription is not a viable alternative because users are unwilling to pay for content they expect to be free, and the contraction therefore falls on content quality, diversity, and availability. The long-run effect is a compositional shift in the publishing ecosystem towards large, subscription-capable brands and away from small and independent publishers whose ad-funded model is structurally more fragile.

First, it is important to note that the compliance burden falls on all controllers, regardless of whether they possess first-party data. Having first-party data does not exempt any controller from the obligation to respect browser-level signals. Companies that operate significant cross-site advertising businesses may face constraints on their ability to use first-party data outside their own properties, depending on the final implementation and interpretation of the consent architecture. Second, the media services exemption under Art. 88b(3) would create a two-tiered approach to consents, distinguishing between "media service providers" and non-"media-service providers", requiring companies to identify GDPR-exempt "media service providers" that may override central consent choices, and those that are required to adhere to them. Not only is this two-tiered approach technologically challenging to implement, but it introduces an additional layer of complexity, which is likely to increase user confusion, as users would continue to encounter consent banners when visiting media sites.

Using the definition of "media services" from the European Media Freedom Act (EMFA), publishers can qualify for the exemption if they are invested with **editorial responsibility**, namely if the principal purpose of the service — or of a dissociable section thereof — consists in providing programmes or press publications to the general public, by any means, in order to inform, entertain, or educate, under the effective editorial control of a media service provider (EMFA, Regulation (EU) 2024/1083, Art. 2(1); editorial responsibility defined in Art. 2(3)). For example, **news aggregators** perform a recognisably informational function and, yet they fall outside the Art. 88b(3) exemption because editorial responsibility over the press publications they surface remains with the original publishers.[17] Their economic exposure is particularly high as they rely almost exclusively on ad-supported free distribution and they typically operate without login (and therefore with limited first-party data), and depend on the very cross-site behavioural signals that a browser-level refusal interrupts. The same logic could extend to AI answer engines that synthesise third-party content (Mistral, Perplexity, Google AI Overviews, ChatGPT search mode), to price-comparison and vertical-search platforms (Skyscanner, Trivago), to consumer review services (Trustpilot, Tripadvisor), and to specialised content databases (weather, recipes, community message boards). Together these services channel a substantial and growing share of the informational flows through which users navigate the contemporary digital environment — yet the exemption as currently drafted leaves them entirely within the scope of Article 88b.

From an economic standpoint, it is possible to envision the most likely consequences for those businesses by looking at real-world precedents. For example, while Apple's ATT and the mechanism suggested by Article 88b differ in enforcement layer, scope of data restricted, and implementing actor, they both remove a large share of users from

39.4% decline in firm-wide revenue for high-Meta-exposure e-commerce firms.

Aridor et al. (2025) estimates

17 According to the 2025 Reuters Institute Digital News Report, across markets search engines (45% weekly use) and social media or video networks (43%) are now the dominant gateways to online news, with dedicated aggregators reaching 16% of users weekly and AI chatbots emerging as a source of news for the first time — used by 7% of respondents weekly overall, and by 15% of those under 25. See Newman, N., Ross Arguedas, A., Robertson, C. T., Nielsen, R. K., & Fletcher, R. (2025). Digital News Report 2025. Reuters Institute for the Study of Journalism, University of Oxford. Available at https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025. Gateway statistics from Section 1, "News Gateways and Notifications" (p. 59); AI chatbot usage from Executive Summary (p. 11) and Graph 47; aggregator-specific figures from "AI-Driven Aggregators Increase Their Reach" (p. 31).

trackable status simultaneously and propagate through the same transmission chain in the advertising value chain. The direction and distributional shape of effects documented under ATT are therefore informative for anticipating the incidence of Article 88b, even where magnitudes cannot be transferred. Kraft, Skiera and Koschella (2023) document a 19.41% decline in publisher ad revenue from Apple users in the United States, with cross-country effects between 1.23% and 11.79%. Aridor et al. (2025) estimate a 37% reduction in Meta click-through rates for conversion-optimised campaigns and a 39.4% decline in firm-wide revenue for high-Meta-exposure e-commerce firms, concentrated among smaller firms. The table below summarises the main differences between Article 88b and the Apple ATT framework in several dimensions.

Table 1 note: ATT and Article 88b differ in legal basis, technical implementation and scope. The comparison does not imply that the magnitude of ATT effects can be directly extrapolated to Article 88b. Rather, ATT is used as the closest available real-world precedent because both interventions operate through a common economic mechanism: a sudden reduction in the availability of behavioural tracking signals, followed by adjustments in advertising markets, publisher revenues, and competitive dynamics.

Table 1:
Comparing Apple App Tracking Transparency (ATT) and Article 88b GDPR

Dimension	Apple ATT	Article 88b GDPR	Implication for this study
Legal source	Unilateral platform policy implemented by Apple	EU-wide regulatory intervention	Different institutional origin
Implementing actor	Single private company	Legislators, standard bodies and market participants	Different governance structure
Layer of implementation	Operating-system level (iOS)	Browser-level and potentially device-level consent architecture	Different technical layer
Scope	Mobile app ecosystem	Open web and potentially a broader range of digital services	Article 88b may affect a wider set of actors
Geographic coverage	Primarily Apple users	Entire EU digital ecosystem	Article 88b potentially broader in reach
Data affected	Cross-app tracking and identifier sharing	Non-essential processing and browser-level consented data flows	Not identical, but both affect behavioural targeting
Mechanism	Large share of users becomes non-trackable simultaneously	Large share of users may become non-trackable simultaneously depending on defaults and implementation	Common transmission channel
Main affected actors	Advertisers, app developers, publishers, ad-tech intermediaries	Advertisers, publishers, ad-tech intermediaries, CMPs, browsers and controllers	Similar categories of affected actors
Advertising impact	Reduced availability of behavioural targeting signals	Reduced availability of behavioural targeting signals	Similar economic mechanism
Distributional effects	Larger effects on smaller firms and firms relying on third-party data	Similar effects predicated by economic theory	ATT provides evidence on likely incidence
Competition concerns	Potential strengthening of firms with large first-party data reserves	Similar concerns regarding firms with proprietary identify graphs and first-party data	Similar competitive dynamics
Evidence available	Observed and measurable outcomes	Ex ante assessment only	ATT provides the closets available empirical benchmark

Additionally, Article 88b may generate a novel form of **moral hazard** for publishers by weakening the direct observability of tracking practices at the website level. Under the current consent architecture, users interact with individual websites and can condition their consent on perceived tracking intensity, design, and trustworthiness. By shifting consent expression to a centralised, browser level signal, Article 88b increases the informational distance between users and websites. As the pool of users shrinks and the marginal value of collectable data rises, this change may induce opportunistic behaviour by less scrupulous publishers toward the remaining consenting users, through more aggressive data extraction or monetization practices. This deterioration in user experience feeds back into beliefs: a forward-looking user who anticipates higher ex post exploitation may rationally choose to opt out under the new regime even if consenting was optimal before. In equilibrium, this interaction amplifies adverse selection on the user side, as privacy sensitive or sophisticated users disproportionately exit the consent pool, further increasing the incentives for moral hazard among publishers. The mechanism parallels environments studied in auction and mechanism design models with joint moral hazard and adverse selection, where reduced observability and endogenous participation constraints interact to undermine efficient outcomes.[18]

From the perspective of data availability for EU firms' growth and innovation, the economic argument developed above suggests that Article 88b is, in important respects, self-defeating. By restricting access to data precisely where scale and learning effects matter most, the provision risks weakening the conditions for innovation it purports to facilitate. In this light, the concerns raised by several industry organisations — most prominently German business associations — rest on a sound and internally consistent economic rationale, rather than on mere opposition to regulation as such.

Browsers

Under Art. 88b(6), browser providers acquire a new and significant role: they become the infrastructure through which consent is communicated across the entire web. This creates two effects. First, a direct compliance cost: browser providers (excluding SMEs) must develop and maintain the technical means for users to set and communicate their preferences. Second, and more consequentially, a gatekeeping dynamic: the browser's default setting determines the effective consent rate for the entire web. The provider's own incentives may not be aligned with either benefits for user or market efficiency. A browser provider that also operates an advertising platform (such as Google with Chrome) faces a conflict of interest. A browser provider that competes on privacy (such as Apple with Safari) may default to "refuse" for competitive rather than privacy-maximising reasons.

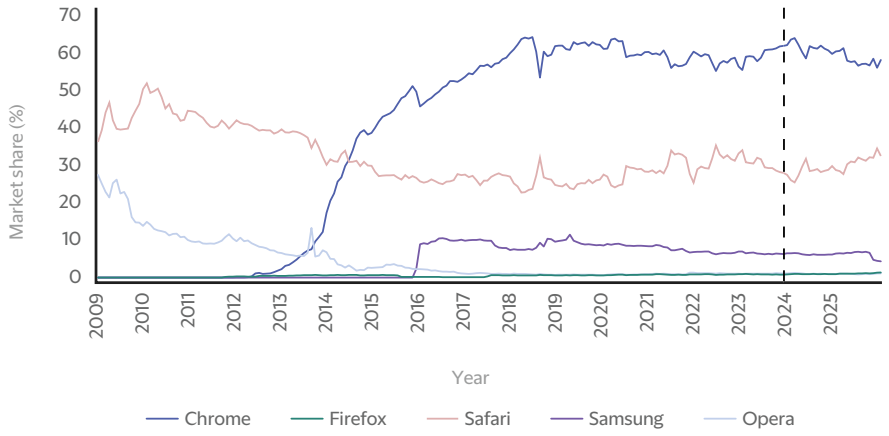
In the EU, browsers are among the core platform services covered by the DMA, being the primary interface through which users access the open web and interact with online content alongside app stores. This is why they are considered a strategic bottleneck within mobile ecosystems (Competition and Markets Authority, 2022). Both globally and within the European Economic Area (EEA), the mobile web browser market has long been highly concentrated. Data from StatCounter indicate that Safari and Chrome have jointly accounted for around 90% of mobile browser usage in most EEA countries over the past decade, as illustrated in the figure below. The introduction of the DMA's browser choice screen — marked in the figure by the vertical dashed line in March 2024 — has not been accompanied by significant shifts in usage patterns. This persistent dominance is closely linked to the structure of the two leading mobile operating systems. Safari is pre-installed and set as the default browser on Apple devices, while Chrome is pre-installed and prominently positioned on Android devices.

18 See Manelli and Vincent (1995) for foundational results on mechanism design under adverse selection and incentive constraints; Lopomo, Persico and Villa (2011) for dynamic environments where participation, moral hazard, and selection interact; and Decarolis (2014) for evidence that reduced observability and weak monitoring can induce opportunistic behavior that feeds back into participation decisions and selection. Ryan (2020, Econometrica) provides complementary empirical evidence on how changes in information and enforcement environments affect both behavior and selection. While these contributions arise in different institutional settings, they share a common mechanism—scarcity combined with limited observability exacerbates moral hazard and induces adverse selection—closely analogous to the consent-architecture shift implied by Article 88b. Manelli, A. and D. Vincent (1995), "Optimal Procurement Mechanisms," Econometrica; Lopomo, G., N. Persico and A. Villa (2023), "Optimal Procurement with Quality Concerns," American Economic Review; Decarolis, F. (2014), "Awarding Price, Contract Performance, and Bids Screening: Evidence from Procurement Auctions," American Economic Journal: Applied Economics; Ryan, N. (2020), "Contract Enforcement and Productive Efficiency: Evidence from the Bidding and Renegotiation of Power Procurement Contracts in India," Econometrica.

Figure 2:
Market share of browsers as volume of mobile traffic in the EEA (2009 – 2026)

Source: StatCounter, accessed on 04/22/2026.

The figure below makes self evident one of the central problems with Article 88b: it concentrates the effective control over consent at the browser and operating system level, precisely in a market that is already highly concentrated. One could further note that the gatekeepers active in this service are all US-based, contrary to a CMP market where EU players keep a significant role. Indeed, the market shares of EU browsers are negligible.



"Safari and Chrome have jointly accounted for around 90% of mobile browser usage in most EEA countries over the past decade"

Data from StatCounter

Processors: ad-tech intermediaries and CMPs

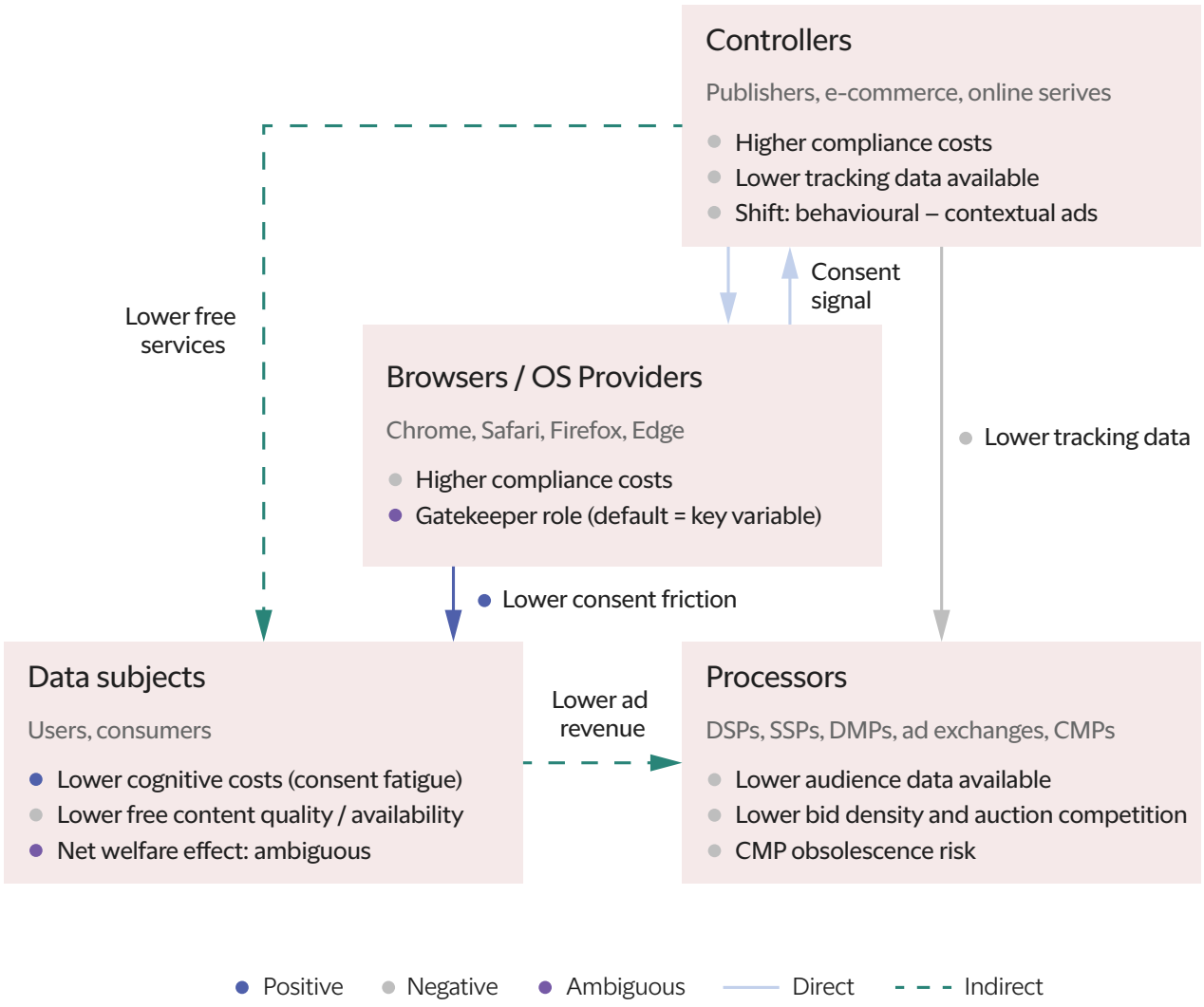
The programmatic advertising ecosystem — demand-side platforms (DSPs), supply- side platforms (SSPs), ad exchanges, and data management platforms (DMPs) — derives its value from the ability to match advertisers with relevant audiences at scale. In the related but different market for internet search, search engine optimization (SEO) and search engine marketing (SEM) help publishers and advertisers to better target their offering to user search queries and search engine responses. The European digital advertising market reached EUR 118.9 billion in 2024, surpassing EUR 100 billion for the first time (IAB Europe AdEx Benchmark 2024), with programmatic advertising growing by 18.4% year-on-year. This segment has been built around the availability of cross-site tracking data to construct audience profiles, run real-time bidding auctions, and optimise campaign delivery.

Article 88b directly reduces the data available to this ecosystem: when a browser-level signal restricts non-essential processing, the behavioural signals that intermediaries rely on become scarcer, and the value chain adjusts accordingly. Fewer trackable impressions reduce the precision of audience targeting; reduced precision lowers the value of each impression in the auction; lower per-impression value reduces bid competition and auction density; and reduced auction revenues translate into lower CPMs for publishers.[19] Similarly, in the activity of those intermediaries active in search, SEO and SEM, a reduction in the tracking ability directly maps into less effective optimization and ad targeting.

The net effect on the ad-tech sector is a contraction in the value of data-dependent intermediation and a redistribution of market power toward actors that can operate independently of cross-site tracking. Whether this produces a competitive advertising market depends on the magnitude of the data loss, the speed of adaptation to alternative targeting methods (contextual advertising, first-party data strategies, privacy-preserving techniques such as Google's Privacy Sandbox), and the extent to which browser providers themselves become new gatekeepers in the consent architecture. None of these variables can be determined from existing evidence.

19 See Decarolis and Li (2026), who show how changes in ancillary services and the information environment in ad-tech markets propagate through auction outcomes, participation decisions, and revenue distribution across publishers and advertisers.

Figure 3:
Expected effects of Article 88b on market participants



Asymmetric exposure across advertising formats

The transmission described above is not uniform across advertising formats and conflating them obscures the actual distributional effect of Article 88b. The economic literature distinguishes between "intent-triggered advertising" — where the ad is selected at the point of user interaction and matched to inventory through a contextual signal generated by the user's own action, such as a query, a product category, or the topic of the page — and "profile-triggered advertising", where the ad is served independently of any contemporaneous user signal and targeting relies on behavioural profiles constructed across sites.

Sponsored search, marketplace sponsored listings, and the contextual layer of retail media fall within the first category. Their value derives from matching the current interaction context to available inventory such as a search query, product category, page content, or aggregate engagement pattern, while more nuanced personal data can add value at the margin, especially for measurement, frequency management, audience refinement, attribution, and off-site retargeting (Edelman, Ostrovsky and Schwarz 2007; Blake, Nosko and Tadelis 2015; Ursu 2018, Decarolis and Rovigatti 2021).

Open programmatic display and third-party retargeting fall within the second, and their value depends much more directly on cross-site behavioural profiles. Empirical evidence of privacy-driven shocks is mostly concentrated in the latter category: the e-Privacy Directive and the GDPR reduced display click-through rates and publisher revenue by double-digit percentages while leaving search advertising largely unaffected (Goldfarb and Tucker 2011; Johnson, Shriver and Du 2020; Aridor, Che and Salz 2024; Peukert et al. 2022). The post-ATT experience reinforces the pattern: Google Search remained insulated, whereas platforms monetising through profile-based delivery — most prominently Meta — absorbed revenue losses an order of magnitude larger (Wernerfelt et al. 2022; Kraft, Skiera and Koschella 2023).

These asymmetries are central to the analysis of Article 88b. A measure that uniformly restricts cross-site tracking is not uniform in its economic incidence: it operates as a de facto tax on profile-triggered advertising, falling most heavily on the open programmatic market and the independent publishers it supports, while leaving search-based advertising and marketplace-embedded sponsored placements comparatively less heavily exposed on average. The within-category heterogeneity is, however, far from negligible: within search, the concentration of cross-site behavioural signals reinforces the buyer-side concentration documented in Decarolis and Rovigatti (2021), benefiting advertisers and intermediaries with direct platform access and large-volume agency relationships while compressing the position of smaller advertisers and the independent publishers that rely on programmatic search inventory. The revenue differential between behavioural and contextual delivery remains contested — industry sources cite a premium of approximately 60% for behaviourally targeted advertising, while academic evidence suggests a more modest 4% revenue lift per impression (Marotta, Abhishek and Acquisti 2019) — but even the conservative estimate, aggregated across a EUR 118.9 billion market, implies substantial redistribution.

The structural incidence of Article 88b

Under the new market structure likely to emerge from the implementation of Article 88b, based on the discussion above, large platforms are likely to retain a significant share of their service-side personalisation capabilities, as ranking, recommendation, and discovery systems may continue to rely on first-party signals used in the ordinary delivery of the service. What Article 88b restricts is personalization for advertising purposes: behavioural selection of sponsored placements, off-site retargeting, and the monetisation of first-party audiences for ad-tech partners. This distinction matters because personalisation of the service — the tailoring of rankings, recommendations, and discovery surfaces — is itself an improvement to the user experience, with empirical work documenting substantial consumer utility gains from personalised ranking and recommendation systems (Ursu 2018; Donnelly et al. 2024). Sponsored placements within personalised environments cannot be cleanly separated from this architecture: a non-personalised sponsored slot embedded within an otherwise personalised ranking introduces a visible relevance discontinuity that erodes the coherence of the service experience. Article 88b, by separating service personalisation from advertising-related purposes, may therefore generate internal incoherence in digital services where sponsored and organic discovery are experienced by users as part of the same interface.

Independent ad-tech intermediaries, by contrast, lose their primary input. The Apple ATT precedent illustrates the pattern: Kraft et al. (2023) document a 21% fall in publisher ad revenue from Apple users across 19 countries, while Aridor et al. (2025) find that Meta-optimised advertising experienced a 37% reduction in click-through rates and e-commerce SMEs suffered revenue declines of 8–40% relative to less-exposed firms. Smaller firms bore a disproportionate burden because they lacked the first-party data reserves and diversified advertising channels available to larger competitors. Direct extrapolation from ATT to Article 88b requires caution — ATT operates at the OS level, affects mobile app tracking rather than web cookies, and was implemented by a single firm rather than by regulation — but the direction of the effect is consistent with economic theory: privacy restrictions that apply uniformly across the ecosystem disproportionately disadvantage actors that depend on third-party data, while reinforcing the competitive position of those with proprietary first-party data. Kesler (2020) and Johnson et al. (2023) document similar concentration effects following earlier privacy regulations

Expected impacts on Consent Management Platforms.

The economic effect of Article 88b on Consent Management Platforms (CMPs) cannot be read off the cookie banner alone. The banner is only the visible layer of what CMPs do: behind it, they translate consent into purpose-specific, auditable records, manage vendor lists, maintain TCF interoperability, and critically transmit consent decisions, together with the associated data, to downstream processors. Article 88b targets the banner-display function directly, but it does not by itself remove this back-end infrastructure. The effect on CMPs is therefore better understood as a redistribution of value than as elimination: whether a given function is displaced or survives (and may even grow) depends on how the machine-readable standard is designed.

The likely effect is therefore a redistribution of value within the CMP sector rather than a uniform gain or loss. Pure-play CMPs whose revenues depend mainly on site-level banner implementation may face margin compression. Larger privacy-suite providers, or CMPs able to reposition themselves as standards, interoperability and audit infrastructure may benefit from centralisation. This also creates a competition concern: Article 88b could reduce one form of consent fragmentation while concentrating consent infrastructure in a smaller number of technically and legally sophisticated intermediaries. Recent market developments support this interpretation. In March 2026, several European privacy-tech providers created the European CMP Association (ECMPA), a Brussels-based non-profit association co-founded by Usercentrics, Axeptio, Didomi and iubenda. The association was established in response to the Digital Omnibus and the broader move toward browser-level privacy signals, with the objective of giving European consent infrastructure a collective voice in discussions with EU institutions, data protection authorities and standardisation bodies.

ECMPA's stated priorities map directly onto the unresolved design choices under Article 88b. First, it emphasises GDPR-compatible contextual consent: browser-level signals may reduce user friction, but they do not by themselves resolve the legal requirement that consent be specific, informed and purpose-based. Second, it supports technology-neutral interoperability across browsers, compliance infrastructures, AI assistants and future European Digital Identity Wallets. Third, it frames consent infrastructure as a question of European digital sovereignty, because the design of the standard will influence whether European privacy-tech providers remain central to the compliance architecture or whether value shifts toward larger global platforms and compliance suites. The creation of ECMPA is therefore informative for the economic assessment of Article 88b. CMPs themselves appear to view the provision not as a marginal simplification of cookie banners, but as a structural redesign of the consent infrastructure. The relevant policy question is not whether CMPs disappear, but which CMP functions survive, which are displaced, and whether the new architecture preserves open, interoperable and legally robust consent management or instead creates a new layer of consent gatekeepers.

One important aspect regards the interaction between Article 88b and the broader EU competition framework. One possible outcome would be the gradual internalisation of consent-management functions by browser or operating-system providers. However, this should not be taken for granted. Browsers and operating systems are already recognised as core platform services under the Digital Markets Act, and recent developments in EU merger policy (this is, for instance, the case of the current draft of the revised merger guidelines) place increasing scrutiny on acquisitions of complementary assets that may reinforce market power within digital ecosystems. Consent-management infrastructure combines interoperability, compliance, auditability and user-interface functions, making it a potentially strategic complement to browser and operating-system services. As a result, the future evolution of the CMP sector is likely to depend not only on technological substitution but also on competition-policy constraints. This suggests that Article 88b may be more likely to trigger a reorganisation of CMP functions than their wholesale absorption by browser or operating-system providers.

A final consideration concerns the standards process itself. The design of the machine-readable indications required under Article 88b(4) creates a structural conflict of interest: CMPs benefit from standards complex enough to require expert integration, while browsers and controllers benefit from standards simple enough to implement internally. A simple-by-design standard would accelerate the displacement of banner-centric providers and amplify the effects described above, while a complex-by-design standard would cushion them. Either way, the likely effects also run counter to the digital sovereignty objectives articulated elsewhere in the Commission's strategic agenda (Draghi 2024; Letta 2024): a measure designed to simplify the EU's consent architecture risks contracting a predominantly European privacy-tech layer or accelerate consolidation towards non-EU global compliance platforms.

3.3
Overview of the Commission impact estimates for Article 88b

In this section, we provide a structured assessment of the evidence presented in the Commission's Staff Working Paper (SWP) which accompanies the Digital Omnibus Package, in relation to the modernisation of the cookie policy.[20] The Commission's quantitative assessment should be read with an important limitation in mind. It is not a full economic impact assessment of Article 88b. The estimates focus primarily on direct user-side benefits from reduced consent prompts and on selected business cost savings associated with cookie-banner management. They do not quantify the wider market effects analysed in this paper: changes in advertising yields, publisher revenues, SME exposure, ad-tech intermediation, CMP market structure, browser implementation costs, or the competitive consequences of shifting consent capture to a smaller number of technical intermediaries. Three key points frame this assessment.

First, the SWP is not an Impact Assessment (IA) in the formal sense, but it is a working document accompanying the Digital Omnibus package, and its quantitative claims do not carry the procedural weight or the sensitivity testing typical of a Better Regulation IA.[21] Second, the cookies-regime savings account for roughly 85% of the €1.34 billion in annual recurring savings the SWP attributes to the entire Digital Omnibus, and for approximately €3.4 billion of the €5.05 billion projected by 2029.[22] The robustness of the cookies estimates is therefore a load-bearing question for the credibility of the package as a whole. Third, several of the inputs feeding these estimates pre-date the Digital Omnibus by a considerable margin. The per-website compliance cost is anchored to a 2014 European Commission evaluation revisited in the 2017 ePrivacy Regulation impact assessment;[23] the share of websites displaying cookie banners (41%) is drawn from a Deloitte study cited in the same 2017 IA; the user-adoption rate underpinning the productivity savings is extrapolated from a 2016 Eurobarometer survey; and the 3.5-second per-banner figure is an EC-chosen midpoint between estimates that "start as low as two seconds" and the Legiscope (2024) estimate of five seconds.[24] Only the SME panel results (September–October 2025) and the IAB Europe 2025 study were collected within the Digital Omnibus reform process itself.

Finally, the SWP's quantitative apparatus is built around two channels: the operational cost of running cookie banners and the time users spend clicking them. Anything that happens behind the banner — distributional effects across firms of different sizes and data endowments, advertising-revenue redistribution, publisher economics, walled-garden migration, the structural incidence on the EU CMP industry — is neither modelled nor systematically discussed. We return to these unaddressed channels in Section 3.4.

3.3.1
User-side effects

One important motivation behind the proposal concerns the "consent fatigue" users are exposed to, and that it is caused by the current consent elicitation regime. The SWP emphasizes that the status quo is widely perceived as deficient by users, businesses and supervisors, supporting the political rationale for an intervention. The Commission's own 2022 evaluation of Directive 2002/58 records converging supervisory assessments: only 3 of 30 competent authorities consider that Article 5(3) ePrivacy "functions well", with 13 rating it "fair" and 3 "poor" and finds that 62% of consulted businesses identify Article 5(3) as a problem.[25]

20 See European Commission, Staff Working Paper, Sec. 1.3.
21 On the contrast between Staff Working Documents accompanying simplification packages and full Better Regulation Impact Assessments, see Better Regulation Guidelines 2025, Chapter 3. Accessible at https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en
22 SWP, Annex II, Summary of cost savings estimates, p. 132.
23 SWP, §1.3.1, p. 46, fn. 75 (citing COM(2017) 10 final, Part 1, p. 37).
24 SWP, §1.3.1, fn. 83.
25 European Commission (2022), Evaluation of Directive 2002/58/EC, cited at SWP §1.3.1, pp. 45–46, fns. 72–73.

Table 1:
Methodological note:

This section applies consistent evidence grading framework to each claim. Each implied claim of the SWP is evaluated in the following dimensions.

Evidence Strength	External Validity	Policy Relevance
• High = experimental/ quasiexperimental evidence directly relevant. • Medium = observational evidence or strong analogies from related interventions. • Low = theoretical reasoning, anecdotal evidence, or extrapolation from distant contexts.	How transferable is the evidence to the EU's Art. 88b context? • High = same mechanism studied in comparable market. • Medium = different mechanism or market but plausible analogy. • Low = substantial differences that limit transferability.	How directly does the evidence inform Art. 88b design or implementation decisions? • High • Medium • Low

Firstly, according to industry studies cited by the Commission, 54% of users randomly accept all cookies and 26% randomly reject all of them when faced with a banner, simply to access the content they wish to see.[26] This evidence has two analytically distinct implications. First, taken at face value, the figures imply that approximately four out of five users currently produce, at the site level, an outcome the Commission itself considers uninformed, materially undermining the protective intent of the consent requirement. Second, and less benignly for the proposal, the same evidence raises a structural question about the centralised remedy. If, faced with a site-by-site choice, users overwhelmingly select a polar "accept-all" or "reject-all" option on the basis of fatigue rather than considered preference, there is no reason to expect that a single, one-time setting expressed centrally via the browser under Article 88b would be qualitatively more deliberative. The same cognitive shortcut that produces a near-random click at the site level will produce a near-random click at the browser level, with the salient difference that this single choice will then propagate, by design, across every controller the user subsequently encounters. The proposed mechanism therefore risks scaling the randomness rather than curing it: an opt-in or opt-out chosen on autopilot becomes the standing position the user expresses to the entire web, with many corresponding outcomes in terms of privacy, personalisation and user experience. While the randomness of the signal might also reflect the higher cognitive effort of the frequent elicitation of consent, such a causal relationship does not seem to have been established by the current literature on privacy and data protection. On the other hand, real world examples such as the Apple ATT seem to have been characterised by a similar pattern of polar outcomes that are difficult to interpret unambiguously as the expression of considered preference.

26 IAB Europe (2025), Optimisation over Reform: Understanding EU Consumers' Perception and Knowledge of the Ad-Funded Internet and Related Privacy Rights Issues, cited at SWP §1.3.1, p. 45, fn. 70.

Following the rollout of ATT, opt-out rates of the order of 75–85% have been documented in early studies; trackable traffic on Apple devices fell by approximately 55 percentage points; and advertising revenue was reallocated away from independent publishers and smaller developers and towards platforms with proprietary first-party data.[27] These outcomes are consistent with two competing readings: a revealed-preference reading, under which users, when offered a clear binary choice, prefer not to be tracked; and a framing-and-default reading, under which the prominence and the wording of the ATT prompt itself drove the polarity. Disentangling the two requires data the existing literature does not provide. What can be said with confidence is that the relevant empirical question for Article 88b, or any analogous proposal, is not whether centralisation reduces consent friction, but whether the polar outcomes it produces correspond to user preferences more closely than the near-random outcomes observed at the site level. On the available evidence, that question remains open.

Beyond the qualitative case for or against centralisation, the SWP estimates the current productivity loss from time spent on cookie banners at €11.2 billion per year in gross terms, or €3.36–5.6 billion per year once the time is re-weighted at 30–70% of the after-tax wage to reflect the leisure-time character of most browsing.[28] While we acknowledge that the evidence in the reduction of cognitive effort is also well supported by existing academic literature (see Farronato et al., 2025), the SWP estimates and conclusions are not supported by a structural empirical analysis, but rather stemming from anecdotal evidence and strong assumptions based on results from a survey that was focusing on a different subject and that was administered in the last decade.[29] As we have described in the previous sections, the user effect on users under Article 88b are a complex result of the interaction between the user preferences for privacy, marketing, and personalization, and the quality of the internet that might result under this proposed regime.

Table 2:
Assessment 1: User side effects

Claim	Evidence Strength	External Validity	Policy Relevance
Centralised browser-level consent reduces user time costs / friction (the effort channel)	High	Medium	Medium
Centralised browser-level consent improves the quality of consent decisions (the deliberation channel)	Low	Low	N/A
Overall	Medium	Medium	Medium

27 Kraft, Skiera and Koschella (2023) document a fall of 55 percentage points in trackable traffic and an approximately 21% drop in advertising revenue from Apple users for publishers in the months following ATT roll-out. See also Aridor, Che, Hollenbeck, Kaiser and Liu (2025) on the broader empirical aftermath of ATT, and Deisenroth et al. (2024) on revenue reallocation effects across firm size.

28 SWP §1.3.1 pp. 47–48; SWP §1.3.3 p. 51

29 SWP §1.3.3, p. 51 fn. 93, citing the European Commission's 2016 Eurobarometer on ePrivacy via COM(2017) 10 final, Part 3, p. 15. The 60% figure underpinning the 200-million-user adoption assumption refers to respondents reporting that they had at some point changed some browser privacy setting — a question whose object differs structurally from the adoption of a centralised, machine-readable signal under Article 88b, a mechanism that did not exist at the time of the survey.

3.3.2
Firm-side effects

The principal quantification the SWP advances in this domain concerns the compliance burden borne by data controllers under the current ePrivacy regime, and the savings they would realise from its reform. The Commission estimates the recurring cost of cookie-banner compliance at approximately €1.64 billion per year.[30] The Article 88b reform, in conjunction with a whitelist covering an estimated 60% of currently used cookies, is expected to enable 50% of private-sector websites and 80% of public-sector websites to dispense with the consent banner altogether, generating recurring savings of €820 million per year for businesses and €320 million per year for the public sector.[31] Taken together, the cookies-regime savings represent 85% of the €1.34 billion in annual recurring administrative-cost savings attributed to the entire Digital Omnibus.

The assessment on data controllers presents some critical aspects, which make both internal consistency and external validity weak from a causal point of view. The first concern is the vintage of the inputs. The €400-per-website baseline is derived by inflating, at a 2% annual rate, a €900 figure originally produced for the European Commission's 2014 evaluation of the ePrivacy Directive and re-deployed in the 2017 Impact Assessment accompanying the proposal for an ePrivacy Regulation.[32] The 41% banner-displaying share is drawn from a Deloitte study cited in the same 2017 Impact Assessment.[33] Both inputs precede the maturation of the post-GDPR-enforcement web and the industrialisation of the consent-management-platform market.

Table 3:
Assessment 2: Data controller

Claim	Evidence Strength	External Validity	Policy Relevance
Per-website compliance baseline (€400/yr × 41% × 10M sites = €1.64 bn baseline)	Low	Low	High
50% private + 80% public no-banner adoption post-reform	Low	N/A	High
Recurring savings of €820 M/yr (business) + €320 M/yr (public)	Low	Low	High
Distributional incidence is uniform across controllers	Low	Low	High
Overall	Low	Low	High

30 The Commission assumes an average annual compliance cost of €400 per website over a three-year website lifespan, and the proportion of the 10 million active websites in the Union currently display a cookie banner to be around 41%. See the SWP §1.3.1, p. 47.
31 SWP §1.3.3, Table 6, pp. 51–52; aggregate reported at Annex II, p. 132.
32 Commission Staff Working Document, Impact Assessment Accompanying the Proposal for an ePrivacy Regulation, COM(2017) 10 final, Part 1, p. 37, cited at SWP §1.3.1, p. 46 fn. 75.
33 Deloitte study cited at COM(2017) 10 final, Annexes, p. 14, re-cited at SWP §1.3.1, p. 47 fn. 78.

A second concern is that the SME Panel conducted by the Commission in September–October 2025 produced annual cookie-banner cost figures that the main text of the SWP summarises as ranging between €100 and €2,000, and that Annex I documents in more granular form as ranging from €50 to €1,500, with only a small minority of respondents reporting between €2,000 and €5,000.[34] The modal value of the distribution lies markedly below the €400 baseline embedded in the aggregate calculation. During the reality check focus group on the Article 5(3) ePrivacy framework, a business association reported maintenance costs of €100,000–€500,000 per year for a mid-sized publisher, but a civil-society representative expressly contested the representativeness of that figure, arguing that the cost of maintaining a standard third-party cookie banner is "negligible" and that service suppliers operate at substantially lower price points.[35]

The SWP records both positions but uses only the publisher figure in its calculation. A third internal-consistency issue concerns the behavioural assumption underpinning the 50% adoption rate: the same SME Panel reports that 37 of 61 respondents indicated they would continue to rely on a cookie banner even where the collection of personal data for audience measurement and website statistics ceased to require consent, citing transparency obligations and legal-uncertainty considerations.[36] Since audience measurement is one of the principal uses brought within the proposed whitelist, the 50% no-banner adoption assumption rests on a behavioural hypothesis that the SWP's own evidence directly contradicts.

The third concern is distributional, as the SWP applies a single average compliance cost to all data controllers, treating the population as homogeneous in cost structure and in incidence of the reform. The most consequential heterogeneity, however, runs in the opposite direction. Controllers without first-party data, such as independent publishers, smaller ad-tech players, ad-funded services sitting outside the Article 88b(3) media-services exemption, are likely to lose their primary input for monetisation. The €820 million aggregate, even taken at face value, distributes savings and unmodelled losses very differently across firm types from what a single average suggests. The SWP does not analyse this distributional incidence, although it is precisely the channel through which the reform produces its competitive and structural effects, to which Section 3.4 returns.

3.4 Unaddressed channels

The SWP impact estimates capture the direct benefits of reforming the cookie regime: lower compliance costs for businesses, reduced consent fatigue for users, and productivity gains from fewer banner interactions. What the assessment does not address are the indirect channels through which Article 88b may affect the same users and businesses via changes on the supply side of the digital economy. Effects on market structure, advertising revenue distribution, publisher economics, and competitive dynamics are not quantified and, in most cases, not discussed. Yet these are precisely the channels through which regulatory changes feed back into the quality, diversity, and availability of the content and services that users ultimately consume. To the extent that such adjustments reduce content quality or consumer choice, the net effects on users may differ from what the direct estimates suggest. Each of these channels each is grounded in economic theory, supported by at least directional empirical evidence, and directly relevant to the design choices that Article 88b leaves open. Importantly, both scholars and policymakers have devoted limited attention to the rich set of indirect consequences of data sharing practices.

We note that there is a lack of solid awareness that digital ecosystems are sustained thanks to data sharing practices, which have been promoting innovation, growth and the deployment of disruptive technologies that characterise our days. Regulation has a special responsibility in the digital era as they can determine the nature and extent of data flows, which ultimately influence both first-party improvements and third-party advertising practices. Advertising incentives have been sustaining the existence of publishers that offer free services and high-quality content to users, and who are the very first economic actor that are likely to suffer from not informed decisions on data sharing practices. As the cycle closes, the ultimate effects of regulation are likely to be expected on users, who might suffer reduced or lower-quality digital products.

34 SWP §1.3.1, p. 47 (range reported as €100–€2,000) and Annex I, Chapter III, p. 110 (more granular range €50–€1,500, with a minority at €2,000–€5,000).
35 SWP Annex I, Chapter IV (Reality Check on the cookie policy framework), reporting both positions.
36 WP Annex I, Chapter III, p. 110.

In what follows, we analyse two possible scenarios: "refuse-by-default" and "accept-by-default". According to the Commission's own 2016 Eurobarometer, the first scenario captures the option preferred by 69% of EU citizens, and whose SWP cites and rejects on the ground that it would "go against the aim of making sufficient data available".[37] We devote particular attention to this scenario because it can create potential adversarial redistribution effects, which are paradoxical to the original intent and objective of the regulator. What has not been fully explored and internalised by the regulator is the potential for welfare losses that stem from a reduction in data sharing practices.

3.4.1. Additional user-side effects

As discussed in the previous section, the SWP reduces the discussion on user-side effects to the computation of time and effort savings, without considering the substantial indirect effects that might stem from the adoption of Article 88b. In fact, the costs and benefits of accepting or rejecting cookies go beyond the mere cost of clicking, with downstream effects on content quality, service availability, or advertising-funded business models. As noted earlier, users are more likely to randomly accept or reject all cookies at the site-level. If this was true under the proposed regime, the user decision would propagate the randomness and non-informativeness of the decision alongside all the browsing activity. The economic consequence of the centralised signal varies sharply with the design of the default, which Article 88b leaves unspecified.

Under a "refuse-by-default" configuration, the centralised signal would mechanically withdraw cookie-based tracking from the larger part of the EU's browsing surface. The empirical evidence on comparable interventions, most directly Apple's App Tracking Transparency, documents not the disappearance of advertising but the reallocation of spend away from the long tail of independent publishers and towards platforms with proprietary first-party data, accompanied by a contraction in publisher revenue per impression of the same order of magnitude as the contraction in trackable traffic.[38] From the user's standpoint, the consequence is not the absence of advertising but the contraction of the ad-funded service supply that today subsidises, in whole or in part, weather, recipes, local news, community boards, productivity tools and a long list of other services consumed for free; the economic loss runs through paywalls, where viable, through reduced editorial output, where not, and through outright closures in the limit.

Under an "accept-by-default" configuration, the proposal produces a symmetric but inverse outcome: the centralised signal, expressed without deliberation, becomes a standing authorisation to track that propagates across every controller the user encounters; behavioural advertising continues largely unaffected; and the consent requirement under Article 5(3) is operationally satisfied without any meaningful decision having been made. The protective rationale of the reform is then hollowed out, in informational terms indistinguishable from the random clicking it sought to replace. One possible consequence of acceptance by default could be an increase in the amount of advertising users are exposed to. However, recent evidence suggests that users' valuation of online digital products (such as social media networks) is not offset by the presence of advertising, suggesting either very small effects or the presence of benefits such as product discovery.[39] Brynjolfsson et al., 2024).

37 SWP §1.3.4, p. 53, citing the Commission's Eurobarometer on ePrivacy (2016).
38 Kraft, Skiera and Koschella (2023) document a fall of approximately 55 percentage points in trackable traffic and a 21% drop in publisher advertising revenue from Apple users following ATT roll-out. See also Aridor, Che, Hollenbeck, Kaiser and Liu (2025) and Deisenroth et al. (2024).
39 Brynjolfsson et al., 2024, "The Consumer Welfare Effects of Online Ads: Evidence from a Nine-Year Experiment", American Economic Review: Insights.

In neither scenario does the SWP attempt to estimate the welfare consequence on the user, despite having identified the benefits for users as one of the proposal's central justifications. One important mechanism at play in both scenarios is well known and documented in the behavioural economics literature and consists of default biases. The SWP treats the choice of default as outside the scope of its assessment, both because the text of Article 88b leaves it unspecified and because the standards process foreseen in Article 88b(4) will determine it ex post. The behavioural-economics literature on defaults predicts that the default will be the operative determinant of outcome, with adoption rates of any non-default option typically observed in the range of 5–20%.[40] The welfare calculus of the proposal therefore depends, in the first instance, on a parameter the SWP does not model and that the Commission has, on the only piece of relevant survey evidence it cites, declined to set in the direction empirically preferred by EU citizens. The cumulative implication is that the SWP's quantification of user-side welfare captures one component of a larger welfare equation in which the second-order channels run, in plausible orders of magnitude, in the opposite direction. Whether the net effect on users is positive, neutral or negative cannot be inferred from the materials the SWP provides; what can be inferred is that the answer turns on parameters the SWP does not address.

3.4.2. Firm-side effects

The supply-side consequences of Article 88b operate through a single structural mechanism, the contraction of cookie-based audience identifiers across the EU's browsing surface, but their incidence on different categories of supply-side actors is far from uniform. The SWP treats the controller population as homogeneous in cost structure and the intermediary population as exogenous to its quantification. The empirical evidence on comparable interventions, and the economic theory on which it is built, suggest that both choices systematically obscure the redistributive consequences of the reform.

1. The first set of effects concerns the compliance costs imposed by the new architecture, which the SWP does not estimate on the supply side. The implementation of a centralised, machine-readable consent signal requires three coordinated technical investments. Data controllers must build and maintain the capacity to receive, parse and honour browser-issued signals, a capability that does not exist in most current web architectures and that requires infrastructure across the controller's full operational stack. Browsers, on whose technical conformance the operational efficacy of the reform depends, must develop and maintain the means for setting, persisting and communicating consent preferences according to standards that have yet to be specified under Article 88b(4). The aggregate of these costs is not estimated, and their distribution across actors of different size, geographic origin and degree of vertical integration is not modelled.
2. The second set of effects concerns the redistribution of advertising revenue. The causal chain is well-attested in the privacy economics literature: a regulatory restriction on cross-site data flows reduces the precision of audience targeting, which reduces the value per impression on the publisher side, which reduces bid competition, which reduces CPMs achievable by independent publishers. The empirical magnitude of this chain has been documented most directly in the studies of Apple's App Tracking Transparency. Kraft, Skiera and Koschella (2023) report a fall in trackable traffic on Apple devices of approximately 55 percentage points and a 21% contraction in publisher advertising revenue from Apple users in the months following roll-out, and Aridor et al. (2025) and Wernerfelt et al. (2024) document the asymmetric character of these effects across firm size and data endowment.[41] The SWP does not engage this material, does not transpose its findings to the Article 88b context, and does not register the magnitude of the revenue reallocation that comparable regulatory interventions have produced.

40 On default effects in privacy contexts specifically, Acquisti, Brandimarte and Loewenstein (2015) and Acquisti et al. (2017); on the structurally analogous pattern in other consequential decision settings, Madrian and Shea (2001) on retirement defaults and Johnson and Goldstein (2003) on organ donation defaults.
41 Kraft, Skiera and Koschella (2023); Aridor, Che, Hollenbeck, Kaiser and Liu (2025); Deisenroth et al. (2024).

3. The third set of effects concerns the resulting competitive distortions. A privacy intervention that applies uniformly across the ecosystem does not produce uniform incidence. All data controllers remain subject to the obligation to respect the browser-issued signal wherever personal data falls within the scope of the GDPR; the exemption foreseen in Article 88b(3) is confined to media services on the narrow definition discussed in Section 3.2 above. The relevant asymmetry is therefore not one of immunity from the regulation but of resilience to it. Controllers with proprietary identity graphs and first-party data of sufficient scale might still be able to keep their targeting and personalisation capability through internal data flows that do not depend on cross-site cookies, whereas controllers without such resources have no equivalent fallback and lose their primary input for monetisation outright. The empirical pattern documented in the broader literature, namely increased market concentration following privacy regulation (Kesler 2020), data-collection restrictions disproportionately benefiting large platforms with proprietary data positions (Johnson et al. 2023), and smaller firms bearing the larger share of the adjustment cost under ATT, is therefore the predictable rather than the exceptional outcome of a regulation that treats unequal starting positions identically. The salience of this dynamic for competition authorities is not theoretical: the UK Competition and Markets Authority intervened in the Google Privacy Sandbox case precisely on the ground that an across-the-board removal of third-party cookies would entrench the relative position of operators whose data architecture is structurally better placed to absorb the constraint.[42]
4. The fourth set of effects concerns the downstream consequences for ad-funded content and services and the related walled-garden dynamic. A significant share of online services consumed by EU citizens, including weather, recipes, product catalogues, local news, community boards and productivity tools, operates on an ad-funded model whose viability depends on the level of advertising revenue per user that publishers can sustain. Where that revenue contracts, publishers face a constrained menu: lower-value contextual advertising, subscription fees (not viable for the great majority), reduced editorial output, or outright closure. The walled-garden effect compounds the contraction. As independent publishers reduce offerings, large platforms with proprietary identity graphs might still be able to provide their ad-supported service thanks to first-party data. However, this will still come at a cost as a large number of first-party data cookies used for advertising purposes are also used for analytical and other purposes. The rational user response is to migrate consumption toward those platforms. The structural result is a regulatory intervention that achieves its formal objective of fewer cross-site cookies while producing greater concentration of user data and user attention in the hands of the small number of actors best resourced to adapt. This is the inverse of the proposal's stated rationale.

Underpinning the magnitude of every effect described above is the design choice the SWP does not discuss: the default that browsers will set under the Article 88b(4) standards process. A refuse-by-default standard amplifies all four sets of effects by mechanically applying the constraint to the larger part of the EU's browsing surface; an accept-by-default standard renders the provision substantially inert in practice, but only at the cost of the protective rationale discussed in Section 3.4.1. In neither case can the default be treated as a neutral implementation detail. The welfare effects, the revenue effects and the competitive effects of Article 88b all depend on a parameter the SWP does not specify, and the standards process foreseen in Article 88b(4) will determine ex post. This same parameter, as discussed in the next section also raises legal questions about the validity of consent expressed centrally without per-controller deliberation, questions that the SWP does not address either.

42 UK Competition and Markets Authority, Investigation into Google's Privacy Sandbox browser changes, ongoing case file. On the broader empirical pattern, Kesler (2020) and Johnson, Shriver and Goldberg (2023).

3.4.3.
Data intermediaries (browsers, CMPs, and others)

Beyond data subjects and data controllers, Article 88b reshapes the operational position of a third class of actors: the intermediaries who handle the consent signal and the data flows that depend on it. This class includes, most prominently, the providers of consent-management platforms (CMPs), the ad-tech intermediaries including ad exchanges, demand-side and supply-side platforms, whose targeting capabilities rest on cookie-based identifiers, and the browsers that, under Article 88b(4) and (6), become the operational conduits of the centralised consent signal. Unlike the user side and the controller side, the intermediary side is engaged by the SWP only at the level of design: through the standards process foreseen in Article 88b(4) and the channel obligation foreseen in Article 88b(6). It is not the subject of any quantified impact assessment. The SWP does not estimate the compliance cost imposed on browsers by the obligation to develop and maintain a machine-readable signal infrastructure; and it does not engage with the empirical literature on the distributional and competitive effects of comparable interventions on ad-tech intermediaries.

1. **The first concern relates to browsers**, on whose technical and commercial response the operational efficacy of Article 88b ultimately depends. The SWP characterises browsers as "well-placed" to support data subjects in setting consent preferences (SWP §1.3.2.4, p. 49), and grounds this characterisation in the institutional centrality of browsers to user navigation; it does not, however, quantify the compliance cost of developing, maintaining and updating a standards-conformant signal infrastructure, nor does it consider the distributional incidence of that cost across the four browser engines that account for the overwhelming majority of EU traffic.

2. **The second concern relates to CMPs**. The SWP does not name the CMP industry in its quantitative apparatus, but the design choices it makes around Article 88b(4) determine, in the first instance, whether the CMP function is preserved or displaced. A simple-by-design machine-readable standard — consistent with the Commission's stated simplification objectives — would allow site operators to implement compliance directly and progressively narrows the role of CMPs. A complex-by-design standard preserves, and may even strengthen, that role. The SWP does not engage this trade-off. The omission carries strategic weight: the European CMP segment was largely built around the consent-collection requirements of the GDPR and is predominantly EU-domiciled, while the global compliance platforms positioned to absorb a simplified standard are predominantly non-EU based. A reform whose stated rationale includes the strengthening of European competitiveness, but whose intermediary-side incidence runs in the opposite direction, requires at least an explicit assessment that the SWP does not provide.[43]

3. **The third concern relates to ad-tech intermediaries more broadly.** The SWP treats Article 88b as a banner-level intervention without considering how the contraction of cookie-based identifiers propagates through the real-time-bidding architecture on which most non-walled-garden advertising relies. The empirical literature on comparable interventions — most directly the studies on Apple's App Tracking Transparency (Kraft et al. 2023; Aridor et al. 2025; Wernerfelt et al. 2024) and the UK Competition and Markets Authority's investigation of Google Privacy Sandbox — documents substantial distributional effects on this segment: a fall in trackable traffic of approximately 55 percentage points, a reallocation of advertising revenue away from independent intermediaries and towards platforms with proprietary first-party data, and the regulatory acknowledgment that interventions in tracking architecture can produce competition effects requiring independent scrutiny. The SWP does not cite this literature, does not transpose its findings to the context of Article 88b, and does not register that its silence on these channels is itself a methodological choice.

4. **The fourth concern is therefore structural rather than empirical.** The standards process foreseen in Article 88b(4), and the design choices it embeds, function as free parameters that determine the welfare consequences across all three intermediary categories simultaneously. The reform's incidence on browsers, on CMPs and on ad-tech intermediaries is not separately given by the text of Article 88b; it is given by the technical specification that the standards process will produce. The SWP treats the standards process as an executory step and does not engage its substantive economic content.

43 On the structural conflict of interest between CMPs and browsers in the design of the machine-readable standard, see also Section 3.2 above.

3.5
Legal and interpretive questions

A threshold legal question is whether, and under what conditions, consent expressed through a centralised machine-readable signal can satisfy the GDPR requirements of being freely given, specific, informed and unambiguous. A browser-level signal may reduce user friction, but it does not automatically solve the legal problem of purpose-specific consent. Unless the standard specifies how general preferences are mapped onto concrete processing purposes, vendors, controllers and contexts, controllers may remain exposed to enforcement risk for relying on signals that DPAs later treat as insufficiently specific or insufficiently informed.

This point is central to the economic assessment. If centralised consent is legally uncertain, Article 88b may not reduce compliance costs; it may instead create a new layer of legal risk, as controllers will need to interpret, document and defend how browser-level signals translate into valid consent for specific processing activities. Conversely, a harmonised EU-level framework specifying the conditions for valid centralised consent could reduce fragmentation, but only if it preserves purpose specificity and auditability.

While the focus of this report is on the economic mechanisms and implications of Article 88b, the analysis developed above raises a set of important legal and interpretive questions that are likely to be first-order determinants of its ultimate effects. These questions go to the scope, internal coherence, and interaction of the proposed provision with the existing EU data protection framework.

A full treatment of these issues lies beyond the scope of this study. However, given their potential to shape both implementation and economic outcomes, it is useful to flag the most salient areas where legal uncertainty remains and where alternative interpretations could materially affect the results discussed in the previous sections.

Four issues are particularly relevant in this respect:

- **Scope of "non-essential purposes":** the scope of what is considered "non-essential" processing and therefore triggering Article 88b is crucial as it will determine the effective reach of browser-level consent signals and, in turn, the magnitude of the constraints imposed on data-driven business models.
- **Interaction with GDPR legal bases:** in particular, whether and to what extent a browser-level refusal signal overrides or limits the use of alternative legal bases under the GDPR such as legitimate interest remains unclear, with direct implications for data availability and innovation incentives.
- **Interaction with Article 5(2) DMA:** for designated gatekeepers, the coexistence of consent obligations under the DMA and Article 88b is likely to lead to user confusion and inconsistencies in compliance.
- **Residual role of the ePrivacy framework:** contrary to the Digital Omnibus stated aims of simplification, Article 88b has been introduced alongside the existing consent requirement under the ePrivacy Directive for non-personal data, raising the prospect of continued fragmentation.

These legal questions are not merely interpretive details but are crucial to determining whether Article 88b ultimately advances or undermines the broader objectives of simplification, innovation, and competitiveness that underpin the Digital Omnibus.

4 Policy options

This study has analysed the Digital Omnibus through an economic lens, particularly focusing on Article 88b, where there has been no meaningful economic impact assessment of its expected market effects. The analysis shows that, while the broader package largely advances its simplification objectives, Article 88b introduces a significant and costly overhaul to the existing consent architecture that is likely to have negative downstream effects on independent retailers, SMEs and user choice. In addition, contrary to the simplification objectives of the broader package, Article 88b introduces additional complexities, including duplicating consent regimes under the GDPR, DMA, and ePrivacy Directive for non-personal data, and introducing unspecified standards for the interpretation of machine-readable indications of user choice at the browser level.

Against this backdrop, the policy options discussed below are organised around four key areas legislators should consider in accordance with the broader objectives of growth, innovation, and competitiveness that underpin the Digital Omnibus: the design of the central signal and its defaults; the coherence of Article 88b with the broader legal framework; the differentiation of obligations across purposes and actors; and the implementation, experimentation and monitoring of the new regime.

4.1 Signal design and defaults

The first set of policy options concerns the design of the central signal itself with its granularity, its default configuration, and its technical specification. These parameters are not implementation details first-order determinants of the effects of Article 88b, since they shape how the new consent architecture operates at the interface level for users and at the integration level for firms. The first design choice concerns the granularity of the signal. A blanket browser-level refusal collapses heterogeneous user preferences into a single binary, replacing repeated low-quality decisions with a single high-impact but equally uninformed default. The benefit in terms of reduced consent fatigue is limited: it lowers cognitive costs while simultaneously narrowing the space of meaningful user choice.

A policy option in this direction is to design more granular or context-sensitive signals, including mechanisms allowing users to revise preferences across categories of services or types of processing. Informal Council Presidency texts circulating at the time of writing indicate that this concern is already shaping ongoing negotiations. The revised Article 88b proposal advanced under the Cypriot Presidency reframes the underlying obligation by requiring consent to be expressed "for specific categories of purposes" through automated, machine-readable means, rather than as a single binary signal. The revision responds to concerns raised by industry that a browser-level binary signal would not satisfy the GDPR's "specific" and "informed" consent requirements. While these texts are not agreed positions and the final wording may differ, their content, however, reinforces the policy option developed in this section: granular, purpose-specific signals are legally necessary and should be reflected. The second design choice concerns the default configuration. Behavioural evidence on the persistence of default effects is unusually robust, and the choice between a refuse-by-default and an accept-by-default regime is therefore a key predictor of the economic effects in the ad-tech ecosystem, rather than a technical detail. Default settings are likely to determine outcomes in practice for a large share of users, regardless of whether the signal architecture is in principle reversible. The third design choice concerns the technical standardisation of the machine-readable signal. Implementation should aim to ensure simplicity and interoperability, ensuring that the signal does not generate new layers of technical uncertainty or require extensive infrastructure investments across the ecosystem. Fragmentation at this level would offset the simplification gains that the Digital Omnibus seeks elsewhere.

4.2 Coherence with the broader legal framework

A second set of policy options concerns how Article 88b interacts with the rest of the regulatory architecture, both within the GDPR and across adjacent legal instruments. Without explicit clarification of these interactions, the new consent architecture risks producing the opposite of the Digital Omnibus's stated simplification objectives, generating regulatory uncertainty rather than reducing it. The first concern is internal to the GDPR: the relationship between the browser-level consent signal under Article 88b and other lawful bases for processing, most notably legitimate interest as revised by Article 88c. The Digital Omnibus seeks to promote innovation by clarifying the availability of the legitimate interest legal basis, particularly for AI training. This objective can be undermined if browser-level refusal effectively overrides alternative processing grounds across the board.

A policy option is to clarify the relationship between legal bases, clarifying whether and under what conditions the signal applies to processing grounded in legitimate interest or other non-consent bases. Preserving alternative lawful bases for non-intrusive or high-social-value processing would reduce regulatory uncertainty and lower the risk-adjusted cost of innovation. The second concern is the relationship between Article 88b and the broader regulatory ecosystem, particularly the residual consent requirements under the ePrivacy Directive for non-personal data. In the absence of clarification, firms may face parallel or duplicative obligations, undermining the simplification objective of the Digital Omnibus. A policy option is to specify, at the level of the Digital Omnibus itself or through accompanying guidance, how the new consent architecture interacts with these residual frameworks both substantively, in terms of which obligations apply, and procedurally, in terms of how compliance is demonstrated.

A third, broader concern emerges in relation to newer EU digital regulation when Article 88b is considered alongside the consent requirements under Article 5(2) DMA. Firms who have been designated as gatekeepers under the DMA would not only need to comply with the consent signals under Article 88b but the consent requirements under Article 5(2) DMA, and potentially the ePrivacy Directive when processing non-personal data. Multiple and overlapping consent requirements adds to rather than simplifies EU's

digital rulebook, in contrast to the simplication aims of the Digital Omnibus.

Moreover, the analysis highlights that one of the central risks associated with Article 88b is its potential to constrain data availability precisely in those domains where scale and learning effects are critical to innovation. While the Digital Omnibus seeks to promote innovation through the introduction of legitimate interest as a viable legal basis for AI training, this objective can be undermined if browser-level signals effectively override alternative processing grounds. Therefore, legislators should prioritise ensuring a coherent hierarchy of legal bases, that clarifies when the overlapping consent regimes under Article 88b, the ePrivacy Directive and the DMA apply, and how they interact with the proposed legitimate interest legal basis for AI training. Preserving alternative lawful bases for non-intrusive or high-social-value processing would reduce regulatory uncertainty and lower the risk-adjusted cost of innovation.

4.3
Differentiated treatment across purposes and actors

A third set of policy options concerns the uniform character of Article 88b. A blanket signal applied identically across all non-essential purposes and all categories of firms conflates situations whose economic and social implications diverge sharply. Differentiation operates along two distinct axes — by purpose of processing and by type of actor — and both are central to whether the welfare effects of the provision turn out positive or negative in aggregate.

Article 88b instead adopts a horizontal, technologically uniform approach that does not differentiate across the economic functions that data serves, nor across the actors and activities that depend on it.

The underlying intuition is well established in the economic literature (see, among others, the recent work of Fu et al., 2025). When firms are allowed to use information about what consumers prefer, for instance in terms of which brands and products, competition intensifies and prices fall, with gains for users. More generally, different categories of data play distinct economic roles. Information revealing user intent, such as search queries, product clicks, or dwell time, and facilitates matching can intensify competition, while other forms of information, such as demographics, inferred income, or cross-website behaviour, may enable forms of surplus extraction, including price discrimination, with potentially adverse effects on consumer welfare. The relevance for Article 88b is not that it directly regulates pricing, but that it operates on the underlying data inputs. A browser-level signal constrains some data flows (in particular, cross-site tracking) but does so in a technologically uniform way, without distinguishing between data that enhances competition and data that may enable surplus extraction. The question for policy design is not whether to restrict data flows, but which data flows should be restricted, a question that a blanket browser-level signal, by construction, does not address.

This distinction at the level of data inputs maps directly onto the two dimensions along which the design of Article 88b operates — the purpose of processing and the type of actor involved.

The first axis concerns differentiation by purpose. The current architecture treats advertising personalisation, security and fraud prevention, bias detection and AI training as functionally equivalent for the purposes of consent capture, even though these activities differ in their welfare implications and in their compatibility with the broader objectives of the Digital Omnibus. A priority for legislators should be to introduce purpose-specific differentiation within the signal architecture, recognising that the costs and benefits of restricting data flows are not uniform across the various categories of processing.

The second axis concerns differentiation by actor. Article 88b is likely to produce asymmetric effects across firms, depending on their access to first-party data and their ability to internalise compliance costs. A policy option is to calibrate the design of the signal so that it does not disproportionately restrict access to data for actors without alternative monetisation channels — in particular SMEs and independent publishers. This could take the form of calibrated exemptions, differentiated thresholds, or supporting mechanisms designed to preserve competitive neutrality. The evidence from

comparable interventions suggests that uniform restrictions can lead to increased market concentration, even when formally neutral in design.

A specific dimension of this actor-level differentiation concerns ad-funded services. A large share of digital content — particularly news and editorial content provided by smaller publishers — is financed through advertising and cannot realistically transition to subscription models. Restrictions on data-driven advertising therefore translate not only into revenue losses for publishers but also into reduced content quality, diversity, and availability for users. An additional policy option is to complement the design of Article 88b with measures that sustain viable revenue mechanisms for content providers that depend on data-driven monetisation.

Finally, the concentration of consent capture at the browser or operating-system level is likely to create new consent gatekeepers. These may include browsers, operating systems but also a limited number of CMPs or privacy-infrastructure providers able to operationalise complex standards at scale. The creation of ECMPA suggests that European CMPs themselves view this as a structural question for the future of consent infrastructure. Legislators should therefore ensure that any centralised signal architecture remains open, interoperable and contestable, rather than shifting control from site-level fragmentation to a smaller group of technical intermediaries.

4.4 Implementation, experimentation and monitoring

A final set of policy options concerns not what is decided but how the new architecture is deployed and assessed over time. The empirical evidence on the effects of consent architectures, particularly on innovation and long-run market structure, remains limited and largely indirect. Locking in design choices before Article 88b's entry into force without mechanisms for adjustment therefore carries non-trivial risk.

One option is to adopt experimental or adaptive implementation mechanisms, such as regulatory sandboxes or staged rollouts, allowing the effects of Article 88b on innovation, competition and user choice to be observed and calibrated before full-scale deployment. This approach is particularly relevant given that several of the parameters discussed above — granularity, default configuration, scope vis-à-vis legitimate interest — interact in ways that are difficult to predict from theory alone.

A second option is to assess and monitor compliance costs systematically across different categories of actors throughout implementation, including SMEs and independent publishers. The current evidence base is particularly incomplete with respect to intermediary costs and transition dynamics, and monitoring the impact of Article 88b on the broader AdTech ecosystem is necessary to ensure the regime can be adjusted based on the observed effects. This monitoring should cover market-structure effects, not only technical compliance. In particular, legislators and regulators should track whether Article 88b leads to concentration in consent infrastructure, displacement or consolidation of European CMPs, reduced access to advertising data for SMEs and independent publishers, and increased dependency on browser or operating-system providers. These outcomes should be treated as core indicators of the regime's performance, not as secondary implementation details.

A third option is to embed distributional analysis explicitly within the implementation framework, so that asymmetric effects on SMEs, independent publishers, and other actors with limited adaptive capacity are tracked over time rather than assumed away. Coupled with experimentation and cost monitoring, this provides the basis for calibrating subsequent regulatory adjustments — whether through guidance, delegated acts, or the broader GDPR review process.

5 Conclusion

The Digital Omnibus represents, overall, a measured and largely well-targeted simplification of the EU's data protection framework. The bulk of the package delivers on the simplification mandate laid out in the Draghi and Letta reports and responds to the negative economic impacts documented in the Unlocking Growth. This has been mainly achieved through the proposed consolidation of breach reporting, the harmonisation of the DPIAs, the clarification of automated decision-making, and the introduction of a legitimate-interest basis for AI training. On the other hand, Article 88b stands out as a provision whose economic effects are both significant and unexplored. Its design choices will determine whether it contributes to the stated Digital Omnibus objectives of growth, innovation, and competitiveness, or whether it introduces new complexity, frictions and distortions into the European digital economy. By relocating consent from the website to the browser, operating systems, and potentially a limited number of CMPs or privacy-infrastructure providers, Article 88b can concentrate a critical regulatory function in a small set of intermediaries whose incentives are not necessarily aligned with those of users, controllers, or the open web. The proposed regime has a high potential to trigger a chain of supply-side adjustments in the advertising value chain, including reduced advertising revenues, weaker personalisation and measurement capabilities, and a greater dependence on first-party data environments controlled by large platforms. The emergence of the ECMPA in March 2026 reinforces this point: European CMPs themselves appear to understand Article 88b as a structural redesign of consent infrastructure rather than a narrow cookie-banner simplification. Yet, the Commission did not conduct a meaningful economic impact assessment of these effects prior to publication.

The contribution of this study has been to highlight the economic impact of Article 88b on the AdTech ecosystem and suggest priority areas for legislators to ensure Article 88b achieves and does not hinder the overall innovation, competitiveness and simplication aims of the broader Omnibus. The policy options outlined above are therefore best understood as elements of a calibration exercise. Three implications follow for the design and implementation of Article 88b.

First, the parameters that determine the welfare outcome under Article 88b (in particular, the default configuration of the signal, its granularity across non-essential purposes, and its relationship with non-consent legal bases such as legitimate interest) should be specified at the level of the Regulation itself, rather than absorbed into the subsequent standards process foreseen in Article 88b(4) without prior calibration. These choices are of substantial importance: for example, the configuration of the default itself determines whether tracking becomes the prevailing outcome for most users or its exception, with first-order consequences for the advertising ecosystem, in particular, SMEs and independent publishers, and for the long-run viability of ad-funded content. Resolving them through a downstream technical procedure transfers what is in substance a legislative decision into a domain where political accountability is weaker and the available evidence base is no stronger than it is at the legislative stage.

Second, distributional effects across firm size, business model and geographic origin should be assessed in advance and monitored over time, rather than recovered, if at all, from aggregate cost–benefit estimates after the architecture is in place. Third, the implementation pathway should incorporate mechanisms for adjustment, such as sandboxes, staged rollouts, and explicit review clauses, given the irreversibility of an intervention that will, by construction, reshape the consent surface of online EU services. Given the structural nature of the intervention and the limited empirical evidence available, careful design, sequencing, and evaluation will be critical to ensure the reform delivers on its intended objectives.

Taken together, these observations point to a broader issue of internal coherence within the EU's digital regulatory framework. If different components of the Digital Omnibus embed inconsistent logics with respect to data use, access, and governance, the resulting equilibrium may diverge from the intended aims of simplification, innovation, and competition. Article 88b illustrates the risk that, in the absence of such coherence, design choices in one domain may offset or even reverse the effects pursued in another.

The wider lesson that the Digital Omnibus exercise leaves for the next stage of EU data regulation, including the Digital Fitness Check and the broader GDPR review process, is that the trade-offs at issue do not run along a single binary axis. The user implications of a data-protection intervention depend on what it restricts, on whom, and through which channel, and a framework that does not differentiate along those dimensions will continue to produce outcomes that diverge, sometimes sharply, from its stated objectives.

Glossary

This glossary defines key concepts and terms used throughout the report. The aim is not to provide exhaustive legal definitions, but to clarify the economic and operational meaning of terms as they are used in the analysis.

Ad-tech (Advertising Technology)
The set of technologies, platforms, and intermediaries that enable the buying, selling, targeting, and measurement of digital advertising. This includes demand-side platforms (DSPs), supply-side platforms (SSPs), ad exchanges, and data management platforms (DMPs).

Behavioural Advertising (Profile-triggered advertising)
A form of digital advertising that relies on data collected across websites and services to build user profiles and target ads based on inferred preferences, interests, or characteristics. It typically depends on third-party tracking technologies.

Browser-level Consent
A consent mechanism in which user preferences regarding data processing are expressed once, at the level of the browser or operating system, and automatically communicated to all websites and services visited thereafter. Under Article 88b, this takes the form of machine-readable signals.

Consent Management Platform (CMP)
A technological solution used by websites to collect, store, and communicate user consent choices regarding data processing. CMPs operationalise legal consent requirements through user interfaces (e.g. cookie banners) and standardised signalling frameworks such as the IAB Transparency and Consent Framework.

Contextual Advertising (Intent-triggered advertising)
A form of advertising that targets users based on the content of the page or the immediate context of the interaction (e.g. search queries) rather than on historical behavioural data. It does not rely on cross-site tracking.

Data Controllers
Entities that determine the purposes and means of processing personal data. In the context of this report, this includes publishers, online platforms, e-commerce websites, and digital service providers.

Data Processors
Entities that process personal data on behalf of controllers. In the digital advertising ecosystem, this includes ad-tech intermediaries such as DSPs, SSPs, and measurement providers.

First-party Data
Data collected directly by a service provider from its own users in the context of elivering a service (e.g. login data, transaction history, on-site behaviour). This data is typically not shared across unrelated services.

Third-party Data / Cross-site Tracking
Data collected across multiple websites or services, typically by entities other than the one directly interacting with the user. It enables behavioural profiling and is central to programmatic advertising ecosystems.

Consent Gatekeepers
Platforms or intermediaries that effectively control the collection and transmission of user consent signals, thereby influencing which data flows are permitted across the ecosystem. Under Article 88b, browser and operating system providers may assume this role.

Machine-readable Signal
A standardised digital instruction, transmitted automatically between systems, that communicates user consent preferences. In the context of Article 88b, these signals replace site-level consent interfaces.

Programmatic Advertising
An automated system for buying and selling advertising space in real time through auctions, typically involving multiple intermediaries and relying on data signals to determine targeting and pricing.

Personalisation
The adaptation of content, services, or advertising to individual users based on available data. The report distinguishes between service personalisation (e.g. recommendations, rankings) and advertising personalisation (e.g. targeted ads).

Consent Fatigue
A behavioural phenomenon whereby repeated exposure to consent requests leads users to make low-effort, non-deliberative decisions (often accepting or rejecting all options), reducing the effectiveness of consent mechanisms.

Default Effect
The well-documented tendency of users to stick with pre-set options. In the context of browser-level consent, the default configuration is a key determinant of aggregate outcomes.

First-party vs. Third-party Monetisation Models
First-party model: revenue generation based on direct relationships with users and proprietary data. Third-party model: revenue generation through data sharing and intermediation, especially in open programmatic advertising.

Walled Garden
A closed digital ecosystem in which a platform controls data access, user interactions, and monetisation opportunities internally, limiting interoperability with the broader web.

References

Acquisti, A., C. Taylor, and L. Wagman (2016). The Economics of Privacy. Journal of Economic Literature 54(2): 442–492.

Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). Privacy and Human Behavior in the Age of Information. Science 347(6221): 509–514.

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. Cranor, S. Komanduri, P. Leon et al. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. ACM Computing Surveys 50(3).

Agarwal, S., D. Lucca, A. Seru, and F. Trebbi (2014). Inconsistent Regulators: Evidence from Banking. Quarterly Journal of Economics 129(2): 889–938.

Alesina, A., S. Ardagna, G. Nicoletti, and F. Schiantarelli (2005). Regulation and Investment. Journal of the European Economic Association 3(4): 791–825.

Aridor, G., Y.-K. Che, and T. Salz (2023). The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR. RAND Journal of Economics 54(4): 695–730.

Aridor, G., Che, Y.K., Hollenbeck, B., Kaiser, M. and McCarthy, D., 2025. Evaluating the impact of privacy regulation on e-commerce firms: Evidence from apple's app tracking transparency. Management Science.

Athey, S., C. Catalini, and C. Tucker (2017). The Digital Privacy Paradox. NBER Working Paper.

Blake, T., C. Nosko, and S. Tadelis (2015). Consumer Heterogeneity and Paid Search Effectiveness. Econometrica.

Brandimarte, L., A. Acquisti, and G. Loewenstein (2013). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science 4(3): 340–347.

Brynjolfsson, E., A. Collis, and F. Eggers (2024). The Consumer Welfare Effects of Online Ads. American Economic Review: Insights.

Casner, B., and M. Leisten (2025). Distributional Consequences of Privacy Regulation. (Working paper).

Christensen, L., A. Colciago, F. Etro, and G. Rafert (2013). The Impact of the Data Protection Regulation in the EU. Report.

Colnago, J., Cranor, L. F., & Acquisti, A. (2023, July). Is there a reverse privacy paradox? An exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. In Proceedings on Privacy Enhancing Technologies Symposium (pp. 455-476).

Cremer, J., Y.-A. de Montjoye, and H. Schweitzer (2019). Competition Policy for the Digital Era. European Commission.

Decarolis, F. (2014). Awarding Price, Contract Performance, and Bid Screening. American Economic Journal: Applied Economics 6(1): 108–132.

Decarolis, F., and G. Rovigatti (2021). From Mad Men to Maths Men: Concentration and Buyer Power in Online Advertising. American Economic Review 111(10).

Decarolis, F., and Firullo, C. (2025), "Unlocking growth: exploring the economic impact of GDPR for tomorrow's Europe", Clifford Chance LLP.

Decarolis, F., and M. Li (2026). Gatekeepers and Self-Preferencing: Incentives and Welfare Trade-offs in Two-sided Markets, SSRN WP n. 6376758.

Demirer, M., D. Jiménez Hernández, D. Li, and S. Peng (2024). Data, Privacy Laws and Firm Production: Evidence from the GDPR. NBER Working Paper.

Dewatripont, M., I. Jewitt, and J. Tirole (1999). The Economics of Career Concerns. Review of Economic Studies 66(1): 199–217.

Draghi, M. (2024). The Future of European Competitiveness. European Commission Report.

Deisenroth, D., Manjeer, U., Sohail, Z., Tadelis, S. and Wernerfelt, N., 2024. Digital advertising and market structure: Implications for privacy regulation (No. w32726). National Bureau of Economic Research.

Dubé, J.-P., et al. (2025). The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing. MIT Sloan.

Edelman, B., M. Ostrovsky, and M. Schwarz (2007). Internet Advertising and the Generalized Second-Price Auction. American Economic Review.

Farronato, C., A. Fradkin, and T. Lin (2025). Designing Consent: Choice Architecture and Consumer Welfare. ACM EC.

Frey, C. B., and G. Presidente (2024). Privacy Regulation and Firm Performance. Economic Inquiry.

Gal, M., and O. Aviv (2020). The Competitive Effects of the GDPR. Journal of Competition Law & Economics.

Goldfarb, A., and C. Tucker (2011). Privacy Regulation and Online Advertising. Management Science 57(1): 57–71.

Goldberg, S., G. Johnson, and S. Shriver (2024). Regulating Privacy Online: An Economic Evaluation of the GDPR. AEJ: Economic Policy.

Holmström, B. (1999). Managerial Incentive Problems: A Dynamic Perspective. Review of Economic Studies 66(1): 169–182.

Jia, J., G. Jin, and L. Wagman (2021). The Short-Run Effects of the GDPR on Venture Capital Investment. Marketing Science.

Jia, J., G. Jin, M. Leccese, and L. Wagman (2025). Transatlantic Venture Investment under GDPR. NBER.

Janßen, R., R. Kesler, M. Kummer, and J. Waldfogel (2022). GDPR and the Lost Generation of Innovative Apps. NBER Working Paper.

Jin, G. Z., Z. Liu, and L. Wagman (2024). The GDPR and SDK Usage. NBER Working Paper.

Johnson, G. (2022). Economic Research on Privacy Regulation. NBER Book Chapter.

Johnson, G.A., Shriver, S.K. and Goldberg, S.G., 2023. Privacy and market concentration: Intended and unintended consequences of the GDPR. Management Science, 69(10), pp.5695-5721.

Kesler, R. (2020). The Effect of Privacy Regulation on Market Concentration. (Working paper).

Laffont, J.-J., and J. Tirole (1991). The Politics of Government Decision Making: A Theory of Regulatory Capture. Quarterly Journal of Economics.

Lupiañez-Villanueva, F. et al. (2022). Behavioural Study on Dark Patterns. European Commission.

Madrian, B., and D. Shea (2001). The Power of Suggestion: Inertia in 401(k) Participation. Quarterly Journal of Economics.

Manelli, A., and D. Vincent (1995). Optimal Procurement Mechanisms. Econometrica.

Marotta, V., V. Abhishek, and A. Acquisti (2019). Online Tracking and Advertising Effectiveness. (Working paper).

Miller, A., and C. Tucker (2011). Encryption and Data Loss. Journal of Policy Analysis and Management.

Niskanen, W. (1975). Bureaucrats and Politicians. Journal of Law and Economics.

Nouwens, M. et al. (2020). Dark Patterns in Consent Management Platforms. CHI Conference Proceedings.

Pollicino, O., F. Paolucci and E. Russo (2026). "The Digital Omnibus on AI: Provisional Agreement of 7 May 2026 and Its Implications for High-Risk AI Systems." Law and Policy Brief, Pollicino AIdvisory, May.

Peukert, C., S. Bechtold, M. Batikas, and T. Kretschmer (2022). Regulatory Spillovers and Data Governance. Marketing Science.

Ryan, N. (2020). Contract Enforcement and Productive Efficiency. Econometrica.

TERA Consultants (2024). Economic Impact of Cookie Policy Enforcement. Report.

Ursu, R. (2018). The Power of Rankings. Marketing Science.

Warberg, L., V. Lefrere, C. Cheyre, and A. Acquisti (2023). Trends in Privacy Dialog Design After GDPR. ACM.

Clifford Chance

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2026

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

**Clifford Chance has entered into association agreements with Clifford Chance Prague Association SRO in Prague and Clifford Chance Badea SPRL in Bucharest.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.