International Center for Law & Economics

Comments of the International Center for Law & Economics

Call for Evidence, Digital Omnibus: Simplifying Rules on Data, Cybersecurity & Artificial Intelligence

14 October 2025

Authored by:

Mikołaj Barczentewicz (Senior Scholar, International Center for Law & Economics)

Kristian Stout (Director of Innovation Policy, International Center for Law & Economics)

Introduction

We thank the European Commission for launching this call for evidence on the forthcoming Digital Omnibus to simplify EU rules on data, cybersecurity, and artificial intelligence. ICLE is a nonprofit, nonpartisan research centre that applies law & economics analysis to technology governance, competition, and consumer-protection policy. Our interest is to ensure that the EU's digital rulebook advances consumer welfare and innovation through clear, predictable, and proportionate rules grounded in evidence and sound economics.

In this submission, we highlight the aspects of the Digital Omnibus proposal that we consider particularly worthy of support (Section I).

In Section II, we comment on the General Data Protection Regulation (GDPR), the key element of the EU digital *acquis* in need for reform, but which is not mentioned in the consultation document.

Given our mission to apply law & economics analysis, in Section III, we comment on the methodology to identify simplification priorities. As an example, we focus on the importance of taking seriously the impacts of policy choices on *business users*. Reform initiatives that fail to do so are likely to fall short in addressing numerous significant barriers to innovation and economic growth posed by EU law.

I. Executive Summary

A. Supported Digital Omnibus Proposals

- **ePrivacy Directive Reform**: Remove Article 5(3) cookie provisions and rely on the GDPR's more flexible framework, eliminating duplicative requirements and the overly restrictive binary-consent model that lacks "legitimate interest" provisions.
- **Cybersecurity Reporting**: Streamline overlapping incident-reporting obligations across the AI Act, GDPR, NIS2 Directive and other frameworks in order to reduce redundant reporting burdens.
- **AI Act Implementation**: Ensure proportionate enforcement that balances innovation needs with compliance, particularly for startups whose resources may be diverted from development.

B. GDPR Simplification

- The consultation omits GDPR reform, despite the Commission's commitment to assess the digital *acquis*; this represents a missed opportunity for meaningful simplification.
- The core problem is not the GDPR's text, but its enforcement structure, which fosters privacy absolutism by enabling data-protection authorities (DPAs) to act as both prosecutor and judge with near-limitless discretion.

- Current enforcement treats privacy as supreme over all other EU objectives, contradicting both the GDPR's own proportionality principles and broader EU economic goals.
- Proposed solutions include embedding proportionality in the main GDPR text and establishing multidisciplinary tribunals not entirely composed of privacy lawyers, in order to balance competing rights and economic realities.

C. Methodological Concerns About Identifying Simplification Targets

- Simplification efforts must consider significant indirect effects, including how restrictions on digital platforms harm their business users.
- Examples of overlooked impacts:
    - DMA enforcement against Meta degrading advertising tools without analysing damage to EU business advertisers.
    - Political advertising shutdown by major platforms due to unclear EU rules.
    - 30% traffic drop for EU hotels after DMA enforcement on Google, benefiting large U.S. travel agencies instead.
- Current impact assessments fail to capture these significant indirect barriers to EU innovation and economic growth.
- This should lead to careful analysis of indirect negative effects of the EU digital *acquis*, including asymmetric regulations (DMA, DSA).

II. The Digital Omnibus Proposals

A. 'Rules on cookies and other tracking technologies laid down by the ePrivacy Directive'

We agree with the Commission that the provisions of the ePrivacy Directive on cookies and technologies used for similar purposes are outdated. A pragmatic solution would be to remove those provisions (in particular, Article 5(3) of the ePrivacy Directive) and rely on the more flexible data-protection framework from the GDPR.

The current interpretation of Article 5(3) has evolved far beyond its original scope, as evidenced by recent European Data Protection Board (EDPB) guidelines that would require consent for URL and pixel tracking, IP-based tracking, certain forms of "local processing" once information (or its derivatives) leaves the device, and other mechanisms such as headers or authentication tokens.[1] This expansive interpretation effectively treats any information exchange between a user device and a

[1] European Data Protection Board, *Guidelines 2/2023 on Technical Scope of Article 5(3) of the ePrivacy Directive* (7 October 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en.

server as requiring prior consent, with only two extremely narrow exceptions: transmission of communications and services "strictly necessary" for explicitly requested functions.

Unlike the GDPR, the ePrivacy Directive offers no "legitimate interest" basis for processing, forcing businesses into a binary choice between obtaining consent or fitting within increasingly narrowly interpreted technical-necessity exceptions. This rigid framework fails to recognize that certain processing activities—such as basic analytics or funding mechanisms for free services—may be essential for sustainable service provision, even if they do not fit a very narrow interpretation of technical necessity.

The disconnect between the restrictive approach embodied by many DPAs' interpretation of the ePrivacy Directive and the GDPR's more nuanced framework creates legal uncertainty and compliance burdens, without clear privacy benefits.

When authorities interpret "necessity" to exclude economic or business necessities, such as revenue generation, they effectively undermine sustainable business models upon which European consumers may rely. This is particularly problematic for SMEs and startups that depend on standard web analytics and advertising technologies to compete effectively in digital markets.

Rather than attempt to implement further patchwork fixes to these outdated provisions, the Commission should recognize that the GDPR already provides comprehensive data-protection rules with appropriate balancing mechanisms. Removing Article 5(3) and related provisions would eliminate duplicative requirements, while maintaining strong privacy protections through the GDPR's more sophisticated and flexible framework.

If full repeal is not feasible, the Omnibus could nonetheless narrow the gap by codifying clear exemptions for analytics, security/fraud prevention, and basic service-quality measurement. Moreover, it would be advisable to align "necessity" under the ePrivacy Directive with the GDPR's proportional, risk-based view of necessity. But the principled solution remains to remove Article 5(3) and govern these practices under the GDPR.

B. 'Cybersecurity related incident reporting obligations'

We welcome the proposal to streamline overlapping horizontal and sector-specific obligations and reporting tools in order to minimise reporting burden. Under the AI Act, the GDPR, the NIS2 Directive, and multiple other legal frameworks, businesses and other institutions may face separate duties to report the same incident in differing ways.

C. 'The smooth application of the AI Act rules'

The rush to regulate artificial intelligence in the EU—combined with last-minute changes to the legislative proposals made in response to ChatGPT's emerging market success—resulted in legislation (the AI Act) that may significantly hamper the EU's adoption of these pivotal technologies. As we

noted in our work on tech startups, compliance with the AI Act may divert significant resources from startups and stifle their development.[2]

It is thus important to ensure that the AI Act's provisions are enforced proportionately. This must include a careful evaluation of any guidelines and other documents meant to implement the law. AI Act implementation efforts to date, including drafting of the General Purpose AI Code of Practice, have not treated AI's potential to improve European economic welfare with sufficient seriousness.

III. GDPR Simplification

In the communication on "A Simpler and Faster Europe", the Commission refers to "the broader assessment, during the first year of the mandate, of whether the expanded digital *acquis* adequately reflects the needs and constraints of businesses such as SMEs and small midcaps, going beyond necessary guidance and standards that facilitate compliance".[3] While the Commission listed the GDPR among the digital *acquis* that would be subject to assessment, the Digital Omnibus proposal's published outline does not include any improvements to the GDPR.

This omission represents a critical missed opportunity. While the GDPR's substantive provisions aren't necessarily the core problem—as the regulation was intended to protect personal data while acknowledging the need to balance privacy with other fundamental rights and societal goals—the law's enforcement structure has produced a disproportionate, absolutist interpretation of privacy law. The real challenge facing European businesses is not merely this administrative burden but fundamental uncertainty about compliance boundaries, driven by an enforcement framework that systematically privileges privacy over all other objectives of EU law.

The current regime empowers DPAs as both prosecutor and judge, wielding enormous power to impose crippling fines in service of a privacy-maximalist agenda. DPAs appear driven by the belief that their sole responsibility is to maximize privacy and data protection, requiring regulated businesses to demonstrate—against an extremely high standard of proof—that any other interests might justify deviating from the most privacy-focused approach. While regulators acknowledge GDPR's Recital 4, which explicitly addresses proportionality and the non-absolute nature of privacy rights, this principle remains subordinated to enforcement practices that treat privacy as supreme.

The recent EDPB Opinion on AI models exemplifies this structural failure: It provides a lengthy list of compliance measures, while offering no guarantees that following such measures will satisfy

---

[2] Dir Auer & Lazar Radic, *A Europe Fit for the Age of Startups: Rhetoric and Reality in the EU's Digital Package*, INT'L CTR. L & ECON. (August 2025), https://laweconcenter.org/resources/a-europe-fit-for-the-age-of-startups-rhetoric-and-reality-in-the-eus-digital-package.

[3] European Commission, *A Simpler and Faster Europe: Communication on Implementation and Simplification* (1 February 2025), *available at* https://commission.europa.eu/document/download/8556fc33-48a3-4a96-94e8-8ecacef1ea18_en?filename=250201_Simplification_Communication_en.pdf.

enforcement authorities. It therefore effectively grants regulators near-limitless discretion, while providing minimal practical guidance to those trying to innovate responsibly.[4]

This fundamental disconnect from economic realities means EU businesses cannot rely on any consistent interpretation of compliance—even those ostensibly tested in enforcement proceedings. Even the *threat* of discretionary regulatory enforcement, combined with the risk of heavy fines, can chill investment decisions significantly, as well as innovation at the margins.

The approach adopted by CNIL, the French DPA, in its guidance on AI and the GDPR contrasts favourably with the EDPB document.[5] While CNIL demonstrated that proportionate and pragmatic guidance is possible under the GDPR is possible, it is clear that the EDPB is currently institutionally incapable of following CNIL's lead.

The enforcement framework's institutional bias toward privacy absolutism contradicts not only the GDPR's text but also the EU's broader ambitions, as outlined in the Draghi report and the Commission's stated goals. This model fails to adequately represent the non-privacy rights and interests of individuals—particularly vital interests like economic security that fall within the purview of political authorities whose involvement is currently seen as anathema under the interpretation of DPA "independence".

The Commission's proposed GDPR Procedural Regulation fails to address these fundamental issues, merely tinkering at the margins while leaving the privacy-absolutist enforcement structure intact. Rather than focusing on recordkeeping requirements for SMEs—a performative exercise that would waste this opportunity—Europe needs a proportionate data-protection framework that avoids absolutist zealotry and recognizes privacy as one vital interest among many, including economic security and freedom of expression.

Without credible guarantees that the GDPR will be interpreted through the lens of proportionality and in harmony with the full spectrum of EU law objectives—from the Digital Single Market to fundamental freedoms—any simplification efforts will remain superficial. The Commission should recognize that meaningful GDPR simplification requires addressing this structural imbalance in enforcement.

How can this be addressed?

First, the main text of the GDPR could be amended with explicit references to the principle of proportionality, the risk-based approach, and the need to balance privacy and data protection with

---

[4] European Data Protection Board, *Opinion 28/2024 on Certain Data Protection Aspects* (Art. 64) (2024), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

[5] Commission Nationale de l'Informatique et des Libertés (CNIL), *IA et RGPD : la CNIL Publie ses Nouvelles Recommandations Pour Accompagner une Innovation Responsable* (7 February 2025), *available at* https://www.cnil.fr/fr/ia-et-rgpd-la-cnil-publie-ses-nouvelles-recommandations-pour-accompagner-une-innovation-responsable.

other rights and values (*e.g.*, amending and moving the content of Recital 4). This would constitute an important declaration but would likely be insufficient, given the DPAs' entrenched attitudes.

Second, the principle of proportionality could be embedded *institutionally*, ensuring that data protection serves its intended purpose without undermining Europe's economic competitiveness and other fundamental values. One way to move in this direction would be to involve an independent, multidisciplinary tribunal to decide on enforcement actions and guidance documents—a body not stacked with privacy lawyers but that would include economists, business experts, and generalist judges who could weigh privacy alongside other fundamental rights and Europe's need for innovation and growth.[6] Such a tribunal's legal framework could require it to articulate how each decision balances data protection against other fundamental rights and economic realities, ensuring that privacy isn't automatically placed above freedoms such as conducting business, research, or expression.

IV. How to Identify Simplification Goals: Significant Indirect Effects

Given our mission to apply law & economics analysis, we also wish to comment on the methodology for identifying simplification priorities. We will do so in this section using the example of the importance of taking impacts on *business users* seriously in policy choices. By focusing on removing some administrative barriers *directly* imposed on some businesses, the Commission may lose sight of more serious barriers created by imposing restrictions on suppliers (*e.g.*, online marketplaces, platforms) upon which EU SMEs and mid-caps rely. This example demonstrates that the current process of impact assessment and policy design risks failing to notice some of the very significant barriers to innovation and economic growth posed by EU law.

In the already-cited communication on "A Simpler and Faster Europe", the Commission highlighted that "improving how we make rules" will be a priority, and that this will include "reinforced SME and competitiveness checks".[7]

In that spirit, we stress that legal restrictions on digital-business activities are likely to constitute more significant barriers for EU businesses than mere "red tape" obligations. Moreover, such significant barriers can arise from legal duties imposed on *other* businesses. Impact assessments of the kind currently conducted by the Commission can easily overlook this reality.

To illustrate, consider how EU businesses and other organisations that rely on large online platforms to reach their audiences are under risk from legal restrictions imposed on those platforms.

---

[6] *See* Mikołaj Barczentewicz, *A Serious Target for Improving EU Regulation: GDPR Enforcement*, EUTECHREG (27 February 2025) https://eutechreg.com/p/a-serious-target-for-improving-eu.

[7] European Commission, *supra* note 3.

EU data-protection authorities have demonstrated growing hostility to personalised advertising, refusing to recognise the economic nature of the relationship among online platforms, their users, and business users (advertisers).

This regulatory hostility has tended to lack serious reflection on how restrictions on ad targeting will affect business users. Many EU businesses—particularly SMEs—simply could not function without cost-effective ways to target relatively niche audiences. A niche artisanal producer or a startup launching an innovative product will often depend on the ability to reach specific audiences without the massive budgets required for broad brand advertising.

In its DMA-enforcement decision against Meta, the Commission acknowledged that Meta's advertising platform provides unparalleled scale and personalisation capabilities. Yet the Commission's approach would be to degrade these tools without any analysis of the collateral damage to Meta's business users. This is an example of enforcement practice that dangerously disregards the consequences for EU businesses other than the direct addressee of the decision.

Ironically, this kind of regulatory assault on personalised advertising may prevent the emergence of the very EU digital champions that policymakers claim to want. Consider that TikTok—one of the biggest challengers to established online platforms in recent years—was to a considerable extent promoted through effective advertising on existing platforms like Facebook and Instagram. If we hope for future EU challengers to emerge and scale, closing off the most effective ways to reach EU audiences will be profoundly counterproductive.

New entrants and challengers depend on targeted advertising both to acquire users cost-effectively and to generate revenue. By making personalised advertising increasingly difficult or impossible, EU regulations risk creating a moat around incumbent positions—the opposite of the stated goal of promoting contestability.

Analogous downstream consequences of regulations that target platforms are already visible in the political-advertising sphere. Google, Meta, and Microsoft have turned off political advertising in the EU rather than risk falling afoul of unclear rules around political ads.[8] As reported in the press, this has significant implications for political and issue messaging in the EU, limiting the ability of political parties, civil-society organisations, and advocacy groups to reach citizens effectively. This shutdown should serve as a cautionary tale. If personalised advertising is significantly restricted for standard commercial ads, the impact on EU businesses would be far more disruptive.

[8] Ellen O'Regan & Eliza Gkritsi, *EU Political-Ad Rules Kick In for Google, Meta, Microsoft*, POLITICO (May 2025), https://www.politico.eu/article/eu-political-ad-rules-google-meta-microsoft-big-tech-kick-in.

Another example of the consequences of ignoring business-user impacts is the DMA's demonstrated effect on hotels. When the DMA was enforced against Google's hotel-search features, European hotels experienced a 30% drop in direct booking traffic and a 36% decline in direct bookings.[9]

Moreover, among the primary beneficiaries were large American online travel agencies like Booking.com and Expedia, which captured the market share that EU hotels lost. HOTREC, representing more than two million European hospitality businesses, described this outcome as "paradoxical": an EU law intended to promote competition that ended up harming EU small businesses, while benefiting large U.S. corporations.[10]

The lesson from this example is that the EU digital *acquis*—including the GDPR, but also asymmetric regulations like the DMA and the DSA—need to be subjected to careful analysis of their negative indirect effects. The impact assessment behind the DMA can serve as a case study of poor analysis of indirect effects, where positive indirect effects were assumed without robust analysis, while negative indirect effects were ignored.

[9] Javier Delgado, *DMA Implementation Sinks 30% of Clicks and Bookings on Google Hotel Ads*, Mirai Blog (7 May 2024), https://www.mirai.com/blog/dma-implementation-sinks-30-of-clicks-and-bookings-on-google-hotel-ads.

[10] HOTREC, *Joint Industry Statement on Google Search and Article 6.5 of the Digital Markets Act* (6 March 2024), https://www.hotrec.eu/en/policies/joint_industry_statement_on_google_search_and_article_6-5_of_the_digital_markets_act.html.