



# CANTIERE EUROPA

*THE DIGITAL OMNIBUS:  
regulatory adjustment or systemic change?*

*Alessio Caramitti, Stefano da Empoli*

## Introduction

*On 19 November 2025, the European Commission presented the awaited Digital Omnibus, a legislative package intended to streamline the European digital rulebook. The proposal includes the consolidation of legislation governing the processing and reuse of data, interventions on the collection of personal data and the rights of data subjects, the deferral of obligations for high-risk AI systems, action on the processing of sensitive data for AI model training, and the narrowing of reporting obligations for SMEs and SMCs. The proposal has sparked a variety of reactions. While there is diffuse consent on some of the measures introduced, many actors fear an excessive impact on fundamental rights, while others consider the proposal's attempt at simplification to be too modest. This document aims to encourage discussion on this topic by presenting a brief overview of the legislation affected by the Digital Omnibus, the measures that the proposal seeks to introduce and a small collection of perspectives given by different actors, to conclude with some open questions.*

- The EU has built a dense, layered digital rulebook spanning privacy and communications (ePrivacy Directive, GDPR), data mobility and reuse (Free Flow of Non-Personal Data, Open Data, Data Governance Act, Data Act), cybersecurity and resilience (NIS2, CER, DORA, CRA), and digital identity (eIDAS2 wallets), aiming to balance competitiveness, rights and resilience, generating however notable complexity, overlaps, and heavy compliance burdens.
- The EU's digital rulebook is a multi-layered regulatory architecture that builds a supranational "operating system" for the Digital Single Market. Its core strength is the creation of common standards that enable cross-border scale while embedding fundamental-rights safeguards and systemic resilience. Its main weaknesses, however, flow from the same architecture: dense, overlapping layers and shared competences produce complexity and high compliance costs, limited and fragmented enforcement, and coordination frictions, where different authorities generate uncertainty, delays, and uneven outcomes.
- The Digital Omnibus comprises three coordinated proposals (COM(2025) 835–837) under the Commission's simplification agenda. These proposals respond to calls to 'stress-test' the digital acquis by aligning the GDPR, NIS2, DORA and eIDAS2; recalibrating high-risk AI obligations and governance (including the AI Office); and consolidating the rulebook around the Data Act. In practice, it clarifies data reuse rules, modifies the definition of personal data, simplifies the ePrivacy–GDPR interface (especially regarding cookies), improves cross-domain coherence and reduces burdens for SMEs and small mid-caps through targeted exemptions.
- Given its major impact on business practices and fundamental rights, it is considered that the Digital Omnibus should be subject to full Better Regulation impact assessment to quantify social and efficiency trade-offs. On the other hand, broad support for the single incident-reporting entry point, centralised consent to reduce cookie fatigue, and renewed ePrivacy–GDPR harmonisation is registered.

# 1. Regulatory landscape: the puzzle of digital legislation

## 1.1 Mapping the European Digital Legislative Landscape

The European Union has progressively constructed a sophisticated and multi-layered digital regulatory framework that seeks to balance economic competitiveness, fundamental rights, and systemic resilience across the Digital Single Market (DSM).

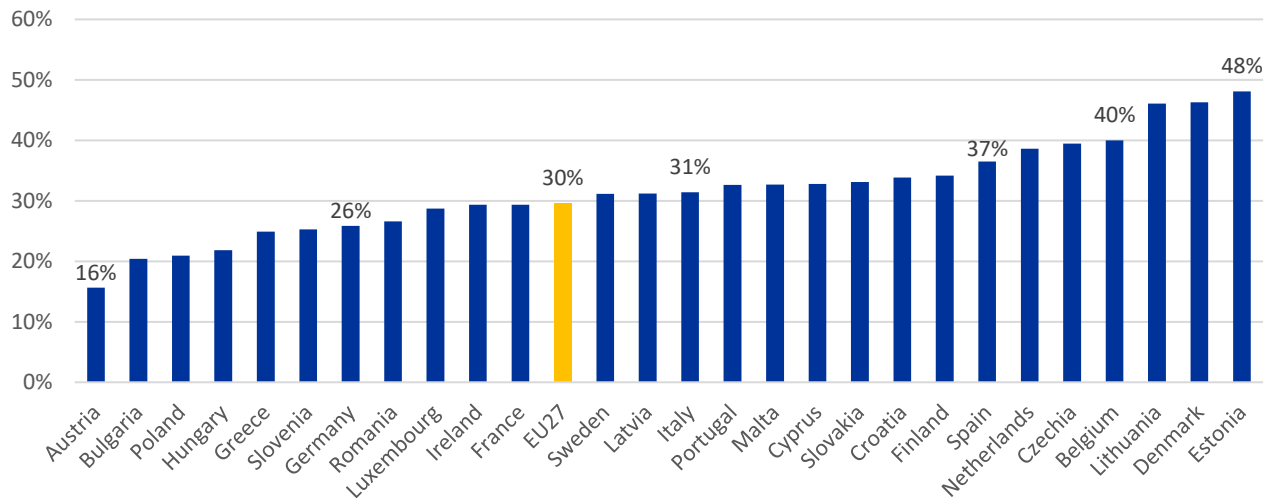
The *ePrivacy Directive* (ePD, Directive 2002/58/EC, amended 2009) is one of the most relevant elements of the European digital rulebook and continues to regulate confidentiality in electronic communications, including tracking and monitoring, and especially cookies and traffic data. Anchoring the modern architecture of the DSM is the *General Data Protection Regulation* (GDPR, Regulation 2016/679), a landmark privacy regime that harmonised personal data protection across the EU with extraterritorial effect and strong individual rights, but whose complexity and stringent compliance obligations have been criticised for imposing significant implementation burdens on organisations and creating a perception of regulatory fatigue among stakeholders. The ePD was meant to be modernized and harmonized with the GDPR through a *ePrivacy Regulation*, but the proposal was ultimately withdrawn by the Commission in 2025<sup>1</sup>. The *Free Flow of Non-Personal Data Regulation* (Regulation 2018/1807) removed localisation requirements for non-personal data, thereby reinforcing cross-border data mobility at an early stage of the EU's digital agenda, though it currently operates alongside other regimes whose overlapping scopes can create compliance complexity. The *Open Data Directive* (Directive 2019/1024) obliged public sector bodies to make high-value datasets reusable, advancing transparency and economic reuse of public information. Building on the GDPR's emphasis on data control, the *Data Governance Act* (Regulation 2022/868) established a trust-enhancing framework for voluntary data sharing and reuse across sectors, facilitating Common European Data Spaces and reducing barriers to innovation. Complementing these efforts, the *Data Act* (Regulation 2023/2854) introduced horizontal rules on fair access to and use of data – particularly data generated by connected products and services – aiming to stimulate competition and data portability while preventing monopolistic control of data; the Act's broad scope and novel obligations, however, present implementation challenges for manufacturers and service providers, particularly regarding data classification and compliance timelines.

---

<sup>1</sup> For more information on the ePrivacy Regulation, <https://www.european-eprivacy-regulation.com/> ; <https://edri.org/our-work/the-eprivacy-regulation-proposal-has-been-withdrawn-but-the-fight-for-your-privacy-is-far-from-over/>

**Fig. 1.1: Share of European SMEs that perform data analytics, 2025**

Source: Eurostat [Data analytics by size class of enterprise]



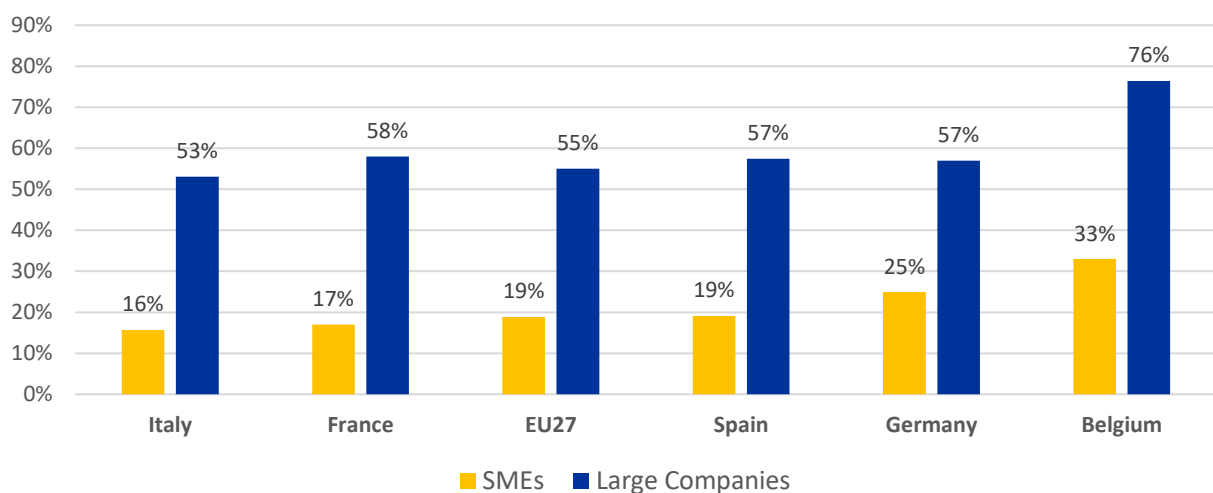
To secure digital infrastructure, the *NIS2 Directive* (Directive 2022/2555) established risk-based cybersecurity obligations for essential and important entities across multiple sectors, seeking to harmonise national responses and incident reporting, yet businesses frequently highlight the administrative overhead and heterogeneity in national transpositions of such directives. Alongside NIS2, the *Critical Entities Resilience* (CER) Directive mandated identification and resilience-building measures for organisations critical to societal functions, broadening risk management beyond cyberspace to include physical and logical threats. The *Digital Operational Resilience Act* (DORA, Regulation 2022/2554) implemented a unified operational resilience standard for the financial sector and its ICT supply chain, significantly strengthening cyber risk governance. Recent advances in digital identity, particularly *eIDAS2* (Regulation 2024/1183), aimed to deliver interoperable digital identity wallets across the EU to facilitate secure cross-border authentication. Additional horizontal instruments such as the *Cyber Resilience Act* (CRA, Regulation 2024/2847) extended baseline cybersecurity requirements to products with digital elements, though debates persist over its impact on open-source software and small suppliers.

Artificial intelligence is governed by the *AI Act* (Regulation 2024/1689), which established a comprehensive, risk-based framework. The bulk of compliance duties are allocated to providers of high-risk AI systems, while narrower obligations are imposed on professional deployers (entities that use AI in a professional capacity, as opposed to affected end users). The Act prohibits a defined set of 'unacceptable-risk' practices and regulates 'high-risk' systems that function as safety components or products subject to third-party conformity assessment under Annex I, or that fall within Annex III. There are specified carve-outs for narrowly procedural or preparatory tools, and the Commission has the possibility to recalibrate the list via delegated acts where evidence justifies it. The provider requirements for high-risk systems cover lifecycle risk management, data governance (i.e. representative, relevant and quality-controlled datasets), technical documentation, record-keeping, instructions to enable downstream compliance, transparency, human oversight enablement and ensuring appropriate accuracy, robustness and cybersecurity. These are complemented by post-market monitoring and serious incident reporting. The Act also introduces a dedicated regime for general-purpose AI (GPAI) models. All GPAI providers must

supply technical documentation and downstream information. They must also adopt a copyright-compliance policy and publish a sufficiently detailed summary of the content of their training data. 'Free and open licence' GPAI models are generally subject only to the latter two duties, unless they are deemed to be 'systemic'. In this case, additional requirements apply, such as evaluations and adversarial testing, systemic risk assessment and mitigation, and incident reporting to the AI Office and national authorities. There is also a duty to notify the Commission within two weeks if 'systemic' status is triggered, for example by training compute exceeding  $10^{25}$  FLOPs. Governance is reinforced through the establishment of an AI Office within the Commission and the introduction of codes of practice to demonstrate compliance in the absence of harmonised standards, as well as through the implementation of staged application deadlines.

**Fig. 1.2: Share of enterprises using at least one AI technology in 2025, by class size**

Source: Eurostat (isoc\_eb\_ai)



## 1.2 Efficiencies and Inefficiencies of European digital regulation

European-level digital legislation generates value by expanding national markets onto the European stage. Digital products and services greatly benefit from economies of scale and network effects, meaning that the more users use a service, the more the profits they generate will exceed the costs of delivering the service. Moreover, for digital products such as social networks, the more users engage with the platform, the more value is generated for each user (e.g. the greater the variety of content available), and the more likely it is that the community will thrive and expand. The establishment of common supranational standards, rules and practices serves to construct the Digital Single Market, a globally relevant stage in which European businesses, users and activities alike can operate (in theory) seamlessly across borders.

The imposing legislative approach pursued in the past by the European Institutions – together with the relevance of the market itself – has sparked the so-called “Bruxelles Effects”, effectively setting standards and shaping regulations around the world in various sectors, with GDPR being amongst the most prominent examples (Bradford, 2019). Nevertheless, this regulatory

constellation is often considered complex to navigate and burdensome for the economy due to its overlapping obligations and risk-averse approach, which, according to some analysts, hampers innovation at its earliest stages. However, other analysts have noted that this strict and burdensome regulation has only recently been introduced, suggesting that factors other than regulation, such as the incomplete implementation of the DSM, are hindering innovation and putting the EU at a disadvantage compared to other competitors.

While drafting the digital rulebook, the European Union pursued specific objectives, such as the protection of fundamental rights and the prevention of the excessive exploitation of personal information by companies for commercial purposes, or by hostile actors for the perpetration of interference and destabilisation<sup>2</sup>. Similar to how it cannot be expected to generate the same revenues from fishing after the implementation of marine protection laws, the protection of personal data, and other rights and values, comes at a cost. Indeed, as Mario Draghi explained that *“one of the clearest demands is for a radical simplification of GDPR,”* which has *“raised the cost of data by about 20 percent for EU firms compared with US peers”* (Draghi 2025), the GDPR deliberately embeds higher data-related costs through its design, notably via the principle of data minimisation, which obliges controllers to limit processing to what is strictly necessary for specified purposes.

The GDPR surely carries inefficiencies, resulting in total annual compliance costs estimated to up to €500,000 for small and medium-sized enterprises (SMEs) and up to €10 million for large organisations (Draghi, 2024). However, it is complex to untangle the costs related to inefficiency to the intrinsic costs that data protection practices carry – and the broad benefits that data protection can generate.

The current European digital rulebook presents inefficiencies that are objectively recognisable and others aspect that can be seen either as inefficiencies or strengths, based on the perspective of the stakeholder analysing them. For example, **data subjects’ rights**, such as access to personal data, on the one hand represent a democratic approach to data collection and treatment, effectively empowering citizens to exercise control over information that concerns them. On the other hand, however, the exercise of this right represents a cost for companies and data holders, which are required a precise management of their databases by the GDPR, especially when handling large datasets or highly sensitive data. These processes involve significant fixed costs, which confer a comparative advantage on larger firms, for whom the relative cost of compliance is lower than for SMEs due to economies of scale (Marino, 2025).

Moving forward, the **notification of cyber incidents** surely falls under the category of clear inefficiencies. Indeed, a single cyber incident can trigger parallel notification duties under multiple EU legal acts – GDPR, NIS2, DORA and CRA – despite being based on the same underlying facts. For example, incidents involving both service disruption and personal data breaches must be reported simultaneously to Data Protection Authorities, Computer Security Incident Response Teams (CSIRTs), national competent authorities, and in some cases ENISA, while also requiring communication to affected data subjects, service recipients, or clients. These obligations differ markedly in terms of scope, thresholds, recipients, timelines and reporting formats: GDPR imposes a 72-hour deadline focused on risks to individuals’ rights and freedoms; NIS2 introduces a three-

---

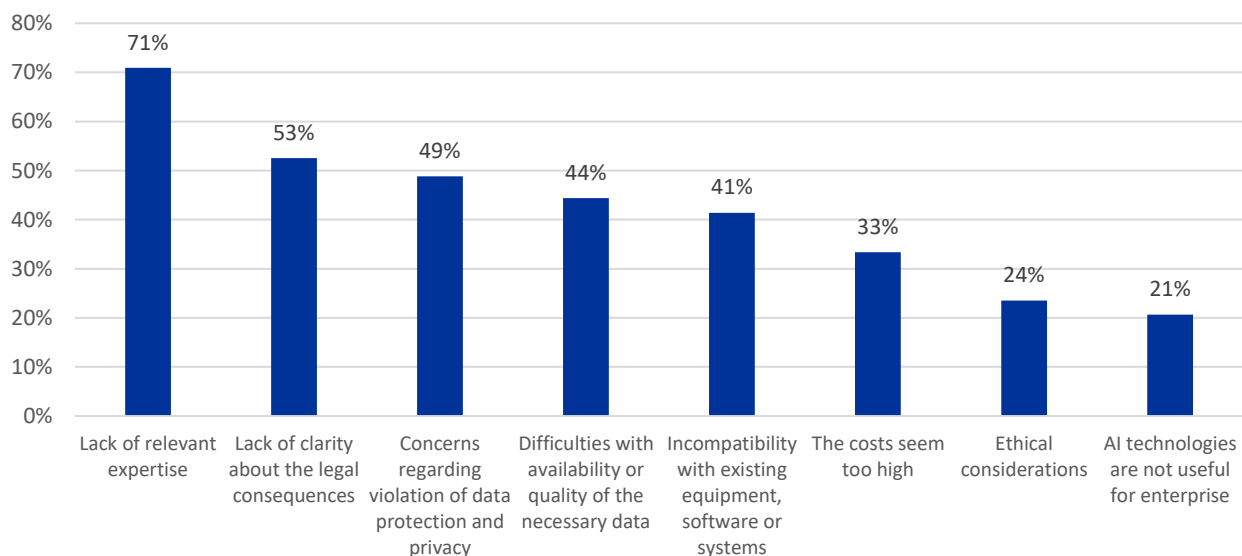
<sup>2</sup> The information leaked by Edward Snowden and the Cambridge Analytical scandal are two concrete examples of exploitation of data harvest against democratic rules.

phase reporting model starting within 24 hours and centred on service continuity; DORA establishes sector-specific, harmonised reporting to financial supervisors with phased notifications; and the CRA adds further layers of early warnings and vulnerability disclosures for manufacturers of products with digital elements. The lack of alignment between these regimes obliges organisations to run multiple reporting processes simultaneously, often under severe time pressure and before full technical clarity is available, increasing the risk of inconsistent disclosures and regulatory scrutiny. This fragmentation is further exacerbated by national-level add-ons, such as law-enforcement notification requirements linked to insurance coverage, and by the possibility of cumulative sanctions under different legal instruments for the same incident (FERMA, 2024).

Subsequently, the regulatory framework governing **tracking technologies** is currently marked by fragmentation and operational inefficiencies, largely stemming from the simultaneous application of the ePrivacy Directive and the GDPR. The ePD regulates the storage of and access to information on users' terminal equipment, such as cookies, while the GDPR applies to the subsequent processing of that information insofar as it qualifies as personal data. This dual-layered regime has generated overlaps, uncertainty, inconsistent enforcement practices, and a significant compliance burden for regulated entities. From the users' perspective, the requirement to provide consent on a site-by-site basis has resulted in widespread "cookie consent fatigue", encouraging routine acceptance of choices that are often poorly understood. This dynamic has been systematically exploited through the deployment of unlawful and manipulative consent architectures, frequently leading to consent that is neither fully informed nor genuinely voluntary. For businesses, persistent legal uncertainty acts as a deterrent to legitimate technological innovation and constrains the deployment of non-intrusive, data-driven analytics, particularly in areas such as website performance measurement, service optimisation, and user experience improvement (Euroconsumers, 2025; noyb, 2024).

**Fig. 1.2: Enterprises that have ever considered using any of the AI technologies by reason for not using, EU, 2025. (% of the enterprises that have ever considered using any of the AI technologies)**

Source: Eurostat (isoc\_eb\_ai)



Furthermore, it is widely recognised that the **enforcement** of data protection rules is one of the digital acquis's weakest spots. The persistent lack of effective GDPR enforcement, particularly in cross-border contexts, reflects deep and systematic shortcomings in the regulation's enforcement model, in addition to inadequate actions by individual supervisory authorities<sup>3</sup>. As argued by Gentile and Lynskey (2022), the GDPR relies on complex composite administrative procedures – such as the one-stop-shop, cooperation, and consistency mechanisms – which combine national and EU-level decision-making without sufficiently harmonised procedural rules or clear lines of accountability. This architecture has generated significant procedural ambiguity, delays, and fragmentation, as key concepts such as “draft decision”, “without undue delay”, and the scope of investigations are interpreted differently across Member States. In practice, the system confers a structurally dominant role on lead supervisory authorities, enabling them to shape the scope, pace, and outcome of investigations, while relegating other concerned authorities to a largely reactive position. This imbalance undermines the principle of equal application of EU law and allows national enforcement cultures, priorities, and resource constraints to decisively influence outcomes in cases with EU-wide impact.

These issues of enforcement and compliance are supported by a survey conducted by noyb (GDPR: a culture of non-compliance?, 2024), which targeted data protection professionals. In this survey, 74.4% of respondents agreed (53.1% strongly agreed and 21.3% somewhat agreed) that “*If a DPA would walk into the door of an average controller tomorrow, they would surely find relevant GDPR violations.*”, while almost 70% (47.0% strongly agreed and 22.9% somewhat agreed) agreed that better enforcement was needed to improve user privacy in practice. Nevertheless, slightly more than half of respondents (51.4%; 19.7% strongly agree, 31.4% somehow agree) agreed with the statement that “Independent of the paperwork, the GDPR has significantly improved how organizations process personal data”.

At the same time, procedural fairness<sup>4</sup> deficits further weaken enforcement. Data subjects are largely excluded from meaningful participation in cross-border proceedings and face substantial obstacles in accessing effective judicial remedies, particularly where decisions are taken by foreign authorities acting as lead supervisors. The interaction between national procedural autonomy and limited EU-level safeguards has resulted in lengthy proceedings, inconsistent sanctions, and, in some cases, strategic under-enforcement, especially where large multinational companies concentrate their EU operations in jurisdictions perceived as more lenient or resource-constrained. These dynamics diminish deterrence and increase risk of forum shopping, unequal

---

<sup>3</sup> For example, as reported in Gentile and Lynskey (2022): 2020/2789(RSP), ‘European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (‘Schrems II’), Case C-311/18’. The Parliament criticised the Irish Data Protection Commission (DPC), expressing ‘deep concern that several complaints against breaches of the GDPR filed on 25 May 2018, the day the GDPR became applicable, and other complaints from privacy organisations and consumer groups, have not yet been decided by the DPC, which is the lead authority for these cases.’

<sup>4</sup> “In its general meaning, procedural fairness the framework through which public decision-making can be structured in such a way that key values such as factual and legal accuracy, transparency, the balancing of all (public) interests involved and the consultation of all relevant parties are considered.” From Van Cleynenbreugel and Grozdanovski (2025)

More information on the concept of procedural fairness in Europe: <https://academic.oup.com/book/7683/chapter-abstract/152747587>

levels of fundamental rights protection, and erosion of trust in the GDPR framework (Gentile and Lynskey, 2022).

## 2. The Digital Omnibus

### 2.1 Context, Scope and Covered Areas

The Digital Omnibus is structured as a legislative package built around three proposals (COM(2025) 835, 836 and 837), intended to operationalise the Data Union Strategy through targeted, technical amendments to core instruments of the EU digital acquis, coupled with repeals of rules deemed outdated or of residual relevance. The proposal is explicitly framed as part of the Commission’s wider “implementation and simplification” agenda (COM(2025) 47 final) and responds to repeated calls from the European Council (March, June and October 2025) and the European Parliament (resolution of 11 September 2025) to “stress-test” and streamline the EU acquis in support of competitiveness, while maintaining high standards of fundamental-rights protection.

These three pieces of legislation aim, firstly, to coordinate the GDPR, NIS2, DORA and eIDAS2. Secondly, the proposals intervene on the obligations for high-risk AI systems, by delaying their entry into force, strengthen the AI Office and better connect the AI Act with the GDPR. Finally, the Digital Omnibus proposes to consolidate the digital rulebook under the Data Act. The reform is meant to clarify the rules governing data processing and reuse, simplify the cookie regime and streamline the interaction between the GDPR and the ePrivacy framework, ensure closer coordination between rules on artificial intelligence, data governance and cybersecurity, and provide targeted support to SMEs and small mid-caps through exemptions or lighter regulatory regimes.

In more detail, one of the main and most controversial reforms introduced by the Digital Omnibus, as it will be illustrated in the final chapter, is a new definition of '**personal data**'. The concept of identifiability shifts from being an abstract, objective property of information to being a concept according to which information relating to a natural person is not necessarily personal data for every other person or entity “merely because another entity can identify that natural person”. Information is not personal to a given entity if that entity cannot identify the person in question, taking into account the means 'reasonably likely to be used' by that entity. Furthermore, it does not become personal to that entity merely because a subsequent recipient may have means reasonably likely to identify the person in question. This change follows the European Court of Justice's (ECJ) interpretation of personal data<sup>5</sup>. The proposal also anticipates implementation support: the Commission, together with the European Data Protection Board, will support

---

<sup>5</sup> *EDPS v SRB* C-413/23 P. However, it has been argued that alignment with the ECJ has been conducted selectively and without a systematic engagement with the Court’s broader case law on data protection, surveillance, and algorithmic decision-making.

controllers by stipulating technical criteria in an implementing act to operationalise the updated approach in practice.

Moreover, **data subject rights** are impacted. Indeed, the subject's right to access data can be denied when considered as abusive or for purposes different from the protection of their data. The explanatory text provides concrete illustrations of abusive patterns, such as strategic requests designed to trigger refusal and then leverage compensation claims; excessive requests made with the intent of causing harm; or requests offered to be withdrawn in exchange for a benefit. In operational terms, the GDPR's fee/refusal mechanism for manifestly unfounded or excessive requests is expressly extended to include situations where, for Article 15 on access requests, the data subject abuses the right for non-protective purposes. Transparency obligations are also derogated when the processing is not likely to result in a high-risk application or where it is assumed that the data subject already has the information about the controller's identity and contact details and the processing purposes. The explanatory memorandum illustrates the intended scope through examples such as craftsman–client relationships and sports clubs where processing is confined to membership management and communications, while explicitly excluding data-intensive contexts (for example, employment). The derogation is also bounded: it does not apply, inter alia, where the controller transmits data to other recipients/categories, transfers data to a third country, carries out automated decision-making (including profiling), or indeed where the processing is likely to result in high risk.

Emphasis has also been placed on the so-called “**cookie fatigue**”, arising from the ePrivacy Directive first and the GDPR after, which set the “privacy by default” standard, requiring the explicit consent by the user to store and process identifying trackers (cookies, digital fingerprints and similar). The proposal aims to harmonise the interactions between the two legislations by shifting the legal treatment of personal data for natural persons in relation to terminal equipment entirely under the GDPR (continuing however to apply the requirements from the ePrivacy Directive for non-personal data), and to introduce a new consent mechanism. In particular, consent will be centrally managed at the level of the terminal equipment of the user (implemented through the browser), rather than through a cookie banner for each website. Media services are excluded from this centralized mechanism: they are allowed to ignore users' browser signals and initiate their own consent request.

The newly introduced article 88a GDPR, which governs the lawfulness of stored or accessed information, also provides a list of low-risk purposes for which consent is not required. The proposed exemptions under the new article are narrowly defined and confined to specific activities: the transmission of communications; the provision of services explicitly requested by the data subject; the generation of aggregated audience measurement for the provider's own online service; and the maintenance or restoration of the security of a service offered by the controller or of the terminal equipment used for that service. In addition, Article 88a(4) further strengthens consent requirements by mandating a “one-click refusal” option, prohibiting repeated consent requests while consent remains valid, and introducing a six-month cooling-off period following a refusal for the same purpose.

The Digital Omnibus also tackles **data breach notification obligations**. Firstly, in case of a data breach, a notification is required only if the breach is likely to result in a high risk to the rights and freedoms of the data subjects. The notification period is also extended from 72 to 96 hours.

Secondly, a single-entry point for incident reporting will be implemented and will cover reporting obligations under NIS2, GDPR, DORA, Digital Identity Regulation, and CER.

As already mentioned, the Digital Omnibus proposes a **consolidation of the data acquis**. Indeed, the Data Governance Act, the Free Flow of Non-Personal Data Regulation and the Open Data Directive are set to be merged under the Data Act. Simultaneously, key terms such as “data user”, “data holder” and “public emergency” are harmonised and further clarified. Moreover, data owners are allowed to refuse the disclosure of data if it may lead to the transfer of sensitive information to third countries lacking an adequate level of protection or may otherwise jeopardise the Union’s essential security interests, therefore strengthening the protection of trade secrets. Finally, Article 35 GDPR is amended to streamline and consolidate the data protection impact assessments (DPIAs), which are required when processing personal data is likely to result in a high risk to the rights and freedoms of individuals. The proposal replaces existing national lists of processing operations subject to DPIA with a list at EU level, provided by the European Data Protection Board, which should also introduce common methodologies. However, there is no clarity on how the new list will correlate with the existing ones and how it should apply to existing products.

Regarding **artificial intelligence**, the Digital Omnibus intervenes under both the GDPR and the AI Act. The proposed amendments to the GDPR aim to provide legal certainty for the development and operation of AI systems while preserving a high level of data protection. The introduction of point (k) under Article 9(2) would allow the processing of sensitive data for AI-related purposes with robust safeguards and the removal of sensitive data where identified. At the same time, the new Article 88c would clarify the use of legitimate interests as a possible legal basis for AI development and operation, with appropriate safeguards and within the meaning of Article 6(1)(f) GDPR<sup>6</sup>. However, it adds the caveat that this does not apply where other EU or national laws explicitly require consent. The latter passage has been deemed problematic for the DSM since AI providers/deployers might have to comply with up to 27 different cases where consent is explicitly required.

Furthermore, the draft proposal recalibrates key obligations under the AI Act by combining regulatory simplification with more gradual and differentiated implementation. It removes the binding requirement for providers and deployers to ensure AI literacy within the company, replacing it with a non-binding encouragement by the Commission and Member States. Obligations for high-risk AI systems are substantially deferred and linked to the availability of compliance-supporting instruments, such as harmonised standards and Commission guidance, with differentiated application dates and final backstop deadlines of August 2028, or August 2030 for systems intended for public authorities.

The proposal further clarifies and expands grace periods for high-risk systems and extends transitional periods for certain transparency obligations applicable to generative AI and general-purpose AI (GPAI) models. Procedural burdens are reduced through the elimination of registration

---

<sup>6</sup> “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

requirements for non-high-risk systems, streamlined and “once-only” conformity assessments, and closer integration with existing sectoral product conformity regimes.

At the same time, the framework expands Union-level and national AI sandboxes, broadens the scope for real-world testing, enhances the AI Office’s supervisory and enforcement powers – particularly in relation to GPAI models and very large online platforms (VLOP); a measure that some actors consider as the introduction of a single point of failure and potential bottlenecks for high-risk systems – and extends the possibility to process sensitive data for bias detection. Finally, the proposal introduces additional facilitations and reduced sanctions for SMEs and mid-cap enterprises.

### 3. Risks and Opportunities

The reform of the digital rulebook proposed by the Commission through the Digital Omnibus has sparked several and contrasting reactions, expressed through responses to the public consultation, reports, open letters and speeches. The following section presents and summarizes some of the feedback received by the Commission for the 16 September 2025 - 14 October 2025 Call for Evidence<sup>7</sup> as well as responses to the second feedback call (currently undergoing, 21 November 2025 - 13 March 2026) and external material published after the diffusion of the proposal.

#### 3.1 Stakeholders’ perspectives and opinions from the civil society

- **BEUC** (the European Consumer Organisation) expressed<sup>8</sup> a strongly critical position towards the Digital Omnibus proposal, framing it not as simplification but as de facto deregulation. BEUC argues that the proposal goes far beyond the Commission’s stated intention of “targeted modifications” and instead amount to a substantial reopening of both the GDPR and the AI Act, without sufficient justification, evidence, or impact assessment. From BEUC’s perspective, this approach directly contradicts recent Commission assurances that simplification would not weaken existing protections. The position highlights a series of specific legal risks for consumers. BEUC criticises proposed amendments to Article 4 GDPR, which would allow controllers to determine whether data are personal, and Article 88c GDPR, which would permit training AI models on personal data based on legitimate interest and without consent. These changes are presented as particularly problematic when combined with delays in the application of AI Act obligations, creating what BEUC characterises as a regulatory gap that weakens data protection precisely when AI-related risks are increasing. With respect to the AI Act, BEUC objects to the proposed “stop-the-clock” approach, the rollback of AI literacy obligations,

---

<sup>7</sup> The referred Call for Evidence alone (available here: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus_en)) contains more than 500 feedbacks, a selection of arguably positive and negative opinions has been conducted.

<sup>8</sup> [https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-116\\_Digital\\_Omnibus\\_proposals\\_keep\\_protections\\_under\\_GDPR\\_and\\_uphold\\_the\\_AI\\_Act.pdf](https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-116_Digital_Omnibus_proposals_keep_protections_under_GDPR_and_uphold_the_AI_Act.pdf)

the introduction of a broad new Article 4a allowing “exceptional” processing of sensitive data for bias detection, and the expansion of exemptions (including for certain high-risk systems and mid-cap companies). According to BEUC, these measures would reduce transparency, accountability, and enforcement, ultimately harming consumers and undermining European competitiveness by disproportionately benefiting non-European Big Tech companies. BEUC concludes that the Digital Omnibus, as proposed, risks weakening consumer protection and digital sovereignty rather than enhancing them.

- **DIGITALEUROPE** advances<sup>9</sup> a strongly pro-simplification and competitiveness-driven interpretation of the Digital Omnibus, framing regulatory complexity as the primary structural barrier to Europe’s ability to scale innovation, commercialise technology, and remain geopolitically relevant. The central thesis is that Europe’s weakness in critical technologies (AI, semiconductors, quantum) does not stem from lack of talent or market size, but from overlapping, fragmented, and prescriptive regulation. The Digital Omnibus is therefore presented as a “low-hanging, high-impact” opportunity to reduce administrative burdens across data, AI, and cybersecurity while preserving core policy objectives. DIGITALEUROPE does not call for reopening the GDPR’s foundations, which it explicitly recognises as a global benchmark, but proposes a shift towards *voluntary-by-default* data sharing under the Data Act, deletion of overlapping international transfer regimes, and targeted clarifications allowing broader reliance on legitimate interest (including for AI model development and security). A recurring concern is that current rules “criminalise data markets before they develop”, imposing obligations irrespective of actual market failure. On artificial intelligence, their document accepts the AI Act’s protective goals but argues that its horizontal design, governance structure, and compliance machinery risk undermining competitiveness. DIGITALEUROPE calls for expanding the legacy clause, eliminating registrations and fundamental rights impact assessments, and sharply limiting authorities’ access to source code and agrees with delaying obligations until harmonised standards are available. It also proposes institutional reform, notably transforming the AI Office into an independent supervisory body and embedding structured industry input. Across cybersecurity, the submission advocates for unified reporting thresholds, templates, timelines, and a single reporting entry point. Overall, the Digital Omnibus is framed as a corrective instrument to rebalance EU digital law away from procedural accumulation and towards risk-based, innovation-compatible governance.
- The **European Machinery and Equipment Manufacturing Industry** (VDMA) adopts a supportive yet fundamentally dissatisfied stance towards the Digital Omnibus<sup>10</sup>. While it welcomes the Commission’s initiative as a first, limited step towards simplification, it argues that the package falls short of the scale of reform required to restore Europe’s competitiveness and digital sovereignty. From VDMA’s perspective, regulatory

---

<sup>9</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33103770\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33103770_en)

<sup>10</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33365801\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus/F33365801_en)

accumulation now outweighs the benefits of legal certainty, especially for a SME- and mid-cap-dominated industrial sector that cannot amortise compliance costs at scale. On AI regulation, VDMA identifies the ambiguous classification of “high-risk AI” as the central structural problem. It argues that the interaction between the AI Act and sectoral product legislation (notably the Machinery Regulation, 2023/1230) creates double regulation of low-risk industrial AI, undermining legal certainty without improving safety. While VDMA supports targeted simplifications – such as proportional obligations for SMEs/SMCs, reduced registration requirements, and alignment of compliance timelines with standardisation – it maintains its core demand for the deletion of Article 6(1) and Annex I(A) of the AI Act<sup>11</sup>, which it sees as the root cause of unnecessary burden for industrial and physical AI systems. Regarding the Data Act, VDMA is largely critical of the Digital Omnibus amendments, describing them as technical and insufficient to deliver meaningful relief<sup>12</sup>. It calls for stronger protection of trade secrets, clearer definitions (especially of “data holder”), and greater entrepreneurial freedom, including the exclusion of Business-to-Business (B2B) contractual arrangements from mandatory data-sharing obligations. By contrast, VDMA is openly supportive of the proposed amendments on the GDPR, particularly those clarifying when data is not personal, reducing information obligations in low-risk contexts, extending breach notification timelines, and harmonising data protection impact assessment requirements. Overall, the paper frames GDPR simplification as the most tangible and positive element of the Digital Omnibus, while urging a broader and more ambitious revision, especially in AI and cybersecurity, to reach a “critical threshold” of simplification.

- Lastly, the joint Opinion adopted by the **European Data Protection Board** (EDPB) and the **European Data Protection Supervisor** (EDPS) takes<sup>13</sup> a conditionally supportive but rights-protective approach to the Digital Omnibus on AI. The EDPB and EDPS welcome the objective of addressing implementation challenges of the AI Act and reducing administrative burdens but repeatedly stress that simplification must not lower the level of protection of fundamental rights, in particular data protection. The document frames the proposal as acceptable only insofar as it preserves accountability, transparency, and effective supervision in a rapidly evolving AI landscape. In principle, the Opinion supports extending the legal basis for processing special categories of personal data for bias detection and correction, but only under strictly circumscribed conditions, with a reinstatement of the “strict necessity” standard and clear limitation to cases involving serious risks of discrimination or harm. The EDPB and EDPS also strongly oppose the proposed removal of registration obligations for certain Annex III AI systems deemed “not high-risk” by providers, arguing that registration is essential for public transparency, accountability, and timely intervention by authorities, and that the proposed savings are

---

<sup>11</sup> Article 6(1) AI Act defines an AI system as “high-risk” when it is a safety component of a product, or itself a product under EU harmonisation laws (Annex I) and that product (or the AI system as a product) must undergo third-party conformity assessment before being placed on the market or put into service.

<sup>12</sup> “The proposed amendments in the Digital Omnibus are rather disappointing. Instead of the necessary changes to certain obligations, it only contains technicalities.” page 6.

<sup>13</sup> [https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-12026-proposal\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-12026-proposal_en)

negligible compared to the risks. On governance, the Opinion welcomes EU-level AI regulatory sandboxes and enhanced cooperation with the AI Office, but insists on systematic involvement of Data Protection Authorities, clarification of competences, and an observer role for the EDPB in the European Artificial Intelligence Board. Regarding enforcement, the EDPB and EDPS accept a degree of centralisation for GPAI-based systems but warn against over-broad exclusive competence of the AI Office without safeguards for national authorities and DPAs. Finally, they express serious concern over the proposed postponement of high-risk AI obligations, urging legislators to maintain existing timelines where feasible (to ensure transparency) or to minimise delays to avoid undermining fundamental rights.

## Open questions

- *Which would be the main effects of the proposed Digital Omnibus?*
- *Is the impact of the proposal on fundamental right significant? Does the Digital Omnibus exceed the general characteristics and limitations of an omnibus, which should be limited to purely technical or procedural clarifications? Or is the simplification effort too weak and should go further in the future?*
- *Will the delaying of obligations for 'high-risk' systems be effective in reducing burdens and uncertainty for providers? Or does it risk to become a factor of uncertainty itself?*
- *What changes to the EC proposal coming from the Council and the Parliament can we expect to see?*