Renaissance Numérique

SYNTHESIS SEPTEMBER 2026

Digital Omnibus: what implications for privacy?

Synthesis of the event

“Digital Omnibus: what implications for privacy?”

To mark the publication of its report “Rethinking the Digital Omnibus: simplification versus rights, consistency and methodology” (June 2026), Renaissance Numérique brought together representatives from business, civil society, academia and the legal profession on 24 June 2026 to discuss the issues surrounding the draft Digital Omnibus Bill on privacy.

This synthesis sets out the main points discussed during this round-table discussion, which took place at Hogan Lovells.

Participants

KEMICHE Anissa, Director of European and International Public Affairs, Numeum

MARIEZ Jean-Sébastien, Partner, Momentum Avocats

MICHAELSEN Frithjof, Institutional Relations Officer for Europe & the Digital Sector, Que choisir ensemble

ROSSI Julien, Lecturer in Information and Communication Sciences at the “Culture and Communication” Department, Université Paris 8

Moderator

DROUARD Étienne, Partner, Hogan Lovells

Rapporteures

D’ASCIA Adele, Renaissance Numérique

BHOJWANI Tasha, Renaissance Numérique

Contexte

On 19 November 2025, the European Commission introduced the “Digital Omnibus” package aimed at simplifying the EU’s digital legislative framework. This package comprised two strands: one dedicated to artificial intelligence, and the other addressing the existing digital acquis, notably the GDPR and the ePrivacy Directive.

Building on the findings of the Draghi and Letta reports on European competitiveness, this initiative reflected a broader effort to reduce administrative burdens and enhance the competitiveness of organisations operating across the Single Market.

Spring 2026 was a decisive phase for negotiations on the Digital Omnibus: following the trilogue of 7 May 2026, the Parliament and the Council reached a political agreement on the “Omnibus on AI” component. On 13 May 2026, the Member States’ representatives endorsed the compromise during Coreper, paving the way for committee vote and, subsequently, the European Parliament’s plenary vote on 16 June 2026. A few days after the roundtable organised by Renaissance Numérique, the EU Council gave its final approval on 29 June 2026. The regulation was then signed on 8 July 2026 and published in the Official Journal on 24 July, entering into force on 27 July 2026.

Within this context, Renaissance Numérique examined the extent to which this “simplification” initiative genuinely delivers on its stated objectives, particularly in terms of privacy protection and the coherence of the EU legal framework. On the occasion of the publication of its report, “Rethinking the Digital Omnibus: simplification vs. rights, coherence and method” (June 2026)[1], the think tank organised a roundtable focusing on the privacy implications of the process. At that stage, while the AI component was on the verge of final adoption, the second part of the proposal was still under discussion in the European Parliament and the Council. This left a number of questions unresolved regarding the balance between simplification, legal certainty and the safeguards, notably with respect to privacy.

The roundtable discussions therefore took place at a critical juncture: as the European Union was considering whether to lock in a series of technical amendments to the AI Act in the name of competitiveness and a more “pragmatic” approach to regulating AI systems, key choices concerning the redefinition of personal data, consent and the respective roles of different actors remained uncertain in the Omnibus component addressing the GDPR and ePrivacy acquis.

The discussions notably highlighted the fragility of the Digital Omnibus approach. While the intention to harmonize the texts (GDPR, AI Act, Data Act) and ease the burden on businesses was welcomed at first, the method used sparked some opposition. For the panelists, administrative simplification must not come at the cost of rolling back citizens’ fundamental rights, nor of undermining the case-law achievements that give the European data protection model its strength and global influence. Looking ahead, the experts agreed on the need to prioritize harmonizing the practical application of the texts rather than a hasty legislative rewrite disconnected from the technological and operational realities of the digital ecosystem.

1. This report is part of a series of work carried out by the think tank:
- November 2024, publication of the brief “EU Digital Policy: Time for Coherence Has Come”.
- May 2025: publication of the brief “For an Effective Interregulation in the Digital Sphere”.
- March 2026: response to the “Digital Fitness Check” consultation by the European Commission.

Redefining personal data: clarification or weakening of the GDPR?

The heart of the discussions that took place in this roundtable focused on the European Commission's proposal to revise Article 4 of the GDPR in order to redefine the concept of "personal data".
Indeed, the text proposes that data should only be classified as personal within the meaning of the GDPR in relation to an "entity" (which remains to be defined) that has, by itself and with the resources reasonably available to it, the means to directly or indirectly identify the individual concerned. This rewording reveals a clear misunderstanding: GDPR obligations apply to data controllers, who are defined not by their ability to access data, but by their ability to determine the means and purposes of the processing.

Anissa Kemiche (Numeum) expressed the relief felt by a large share of digital businesses at what she described as a return to pragmatism. In her view, the vagueness surrounding this definition creates systemic uncertainty. For example, a company publishing aggregated statistics for its physical stores' attendance remains subject to the interpretation of national supervisory authorities (such as the CNIL in France), which often adopt broad and divergent positions on the possibility of re-identification. For Numeum, economic actors are not calling for pure deregulation, but for "practical and precise rules" consistent with the EU's digital legislative framework. Such refocusing proposed by the European Commission would encourage innovation by offering a predictable and secure framework for data controllers according to Numeum.

In contrast, **Julien Rossi** (Université Paris 8) warned about the risk of systematic circumvention of GDPR obligations that this new wording could encourage. Limiting liability solely to the immediate means available to the data controller could pave the way for opportunistic declarations. As a result, many entities could unilaterally classify their data as "pseudonymized" or "anonymous" in an attempt to exclude themselves from the regulation's protective scope. This porousness in classification would come at the direct expense of citizens, who would lose control over the use of their information within complex subcontracting chains where re-identification remains technically possible by cross-referencing third-party databases. Exercising their rights could then become more difficult. Furthermore, data controllers would face significant legal uncertainty, since they would run the risk that partners with whom they share responsibility for processing personal data might wrongly invoke this new possibility.

This redefinition also runs up against the rapid evolution of the state of the art in technology. **Jean-Sébastien Mariez** (Momentum Avocats) noted that the dividing line between personal and non-personal data has become almost impossible to draw in a fixed way. This definition will require the adoption of guidelines from the EDPB (European Data Protection Board) in order to redefine anonymization and pseudonymization concepts. He further lamented the failure to take into account the profound evolution of technologies that strengthen privacy protection (known as "*Privacy Enhancing Technologies*")[2] since the GDPR was drafted in 2016. In his view, rather than staying confined in doctrinal debates disconnected from practice, the European regulator should rely on technical, functional and factual criteria, which have considerably evolved since the ePrivacy Directive was drafted; contemporary technologies (including new encryption techniques) are now capable of putting GDPR principles into practice.

For **Frithjof Michaelsen** all of this must be viewed through the lens of the GDPR's fundamental importance. While he believes the GDPR is not, strictly speaking, a cybersecurity text, it nonetheless remains its cradle. He therefore argued that an agreement must be reached on a definition of personal data that allows for the most secure experience possible.

2. Privacy enhancing technologies, OCDE: https://www.oecd.org/en/topics/privacy-enhancing-technologies.html

↘ Consent running out of steam

The discussion also addressed the grounds for lawful data processing, already shaken up by the growing integration of artificial intelligence. The GDPR establishes the principle of freely given, specific and informed consent.

Julien Rossi described this framework as theoretical and inadequate to modern algorithmic uses. Under Articles 5(1) and 12 of the GDPR, processing must be transparent and intelligible to the user. Yet, he asked, how can a citizen give informed consent to processing whose underlying complexity sometimes escapes even the system's own designers? He believes this inherent opacity renders the process of obtaining consent fundamentally artificial and ultimately, potentially hypocritical. In response to this challenge, the researcher advocated moving beyond mere legal injunction to spur innovation within the technology ecosystem itself, thereby developing application architectures that are natively intelligible and transparent, in line with the "*privacy by design*" principle set out in the GDPR.

On another note, **Jean-Sébastien Mariez** highlighted that he considers user consent to be an excessive focus by regulatory authorities, at the expense of the other legal bases provided for in the European text, notably legitimate interest. In his view, by excessively restricting the use of this legal basis, regulators have driven the industry toward the systematic, and often misused, deployment of cookie banners. This constant over-solicitation generates widespread cognitive fatigue among internet users, who click to dismiss cookie banners without any further consideration for the protection of their privacy.

Conversely, **Julien Rossi** pointed out that legitimate interest cannot serve as an absolute free pass for the advertising industry and behavioural targeting. In the context of online tracking, particularly on news websites, relying on the publisher's legitimate interest to politically profile an internet user remains problematic. This shifts the entire burden of protection onto the user, forced to undertake complex opt-out procedures with dozens of commercial partners whose very existence they are often unaware of.
Such technical impasse stands out within the implementation of consent signals. The ecosystem has seen a proliferation of competing protocols (Do Not Track, Global Privacy Control, the IAB's Transparency and Consent Framework, etc.). Nevertheless, as Julien Rossi explained, no text settles the question of how to prioritize these signals in the event of contradiction (for instance, between the browser and cookies). According to him, this operational uncertainty is compounded by technical anxiety among data controllers. By way of illustration, the deployment of cutting-edge technologies such as homomorphic encryption[3] or post-quantum cryptography raises deeply complex compliance questions. Practitioners/ Data controllers / Managers fear that supervisory authorities disconnected from technical realities will end up imposing ultra-specific algorithmic choices on them, turning GDPR compliance into an exercise in technological micro-management beyond the reach of mid-sized organizations. Moreover, the authorities' choices may ultimately be subject to judicial review and, subsequently, to reversal or modification by the courts. The regulator does not appear to be the best suited actor to determine which standard algorithm should be used, without taking technical, functional and security considerations into account. The vagueness of certain GDPR provisions may therefore, to some extent, constitute an advantage for innovative actors, granting them both the responsibility and the flexibility to determine how personal data should be protected in ways that are operationally feasible and responsive to technological developments.

3. Homomorphic encryption is a cryptographic technique that makes it possible to perform operations on encrypted data without it having to be decrypted. The result of these operations remains in an encrypted form and can only be decrypted by authorized recipients (that hold the decryption key). This technique thus allows participants in a computation to keep their data confidential throughout the computation. Source: https://www.cnil.fr/fr/definition/chiffrement-homomorphe

↘ Balancing between sovereignty and fragmentation: the limits of the Omnibus approach

Addressing these frictions around digital privacy at the European level brings in a multiplicity of actors, and therefore potential complications to the simplification process. For example, to remedy user fatigue with cookie banners, the Omnibus project introduces the idea of centralizing the refusal of consent at the level of browsers and operating systems.

Frithjof Michaelsen highlighted the irony and systemic danger of this proposal. He noted that the browsers and operating systems dominant in the European market are developed and controlled by the tech giants (Google, Apple, Microsoft, Meta). By entrusting the centralization of consent to these players, whose revenues depend directly on the advertising exploitation of personal data, the European Union could create a major conflict of interest. The consumer association representative fears that these companies could use this intermediary role to entrench their dominant position, to the detriment of independent press publishers and European technology alternatives.

He also raised the question of granular consent depending on the different types of processing. While this initiative seems ideal in theory, in practice it adds further complexity at the user level.

For **Anissa Kemiche**, the territorial application of digital regulation across Europe remains characterized by significant national divides, which undermine the conditions of economic fairness within the internal market. She thus pointed to the contrasting regulatory approaches adopted by two leading Member States of the European Union:

- → France, aligned with a tradition of strict protection and an independent regulator (the CNIL), advocates rigorous enforcement of the EU acquis.
- → Germany, more attentive to industrial imperatives and the competitiveness of its businesses, advocates for more flexible approaches, particularly regarding the definition of personal data and data transfers.

She believes this divergence is amplified by asymmetric institutional structures. While France relies on a single, centralized authority, Germany suffers from fragmentation with its 18 supervisory authorities.[4] For an economic actor operating on a European scale, this layered administrative structure creates chronic uncertainty.

Jean-Sébastien Mariez then reported cases of operational dead ends where, for the same data transfer agreement file (*Binding Corporate Rules* - BCR), two national authorities raised no objections while a third paralyzed the entire procedure, thereby undermining the ambition of a European one-stop shop.

In this regard, several questions and comments from the audience at this round table converged into a critique of Brussels' legislative method. One audience member drew a parallel between the European simplification projects and French simplification laws which, through the amendment process, end up making the law more complex. The lack of rigorous and transparent impact assessments was condemned by another attendee. **Anissa Kemiche** and **Frithjof Michaelsen** also deplored "empty" impact assessment documents, incapable of grasping the real compliance costs for the ecosystem and the risk of competitive distortion relative to other geographic regions.

4. Germany accounts for one federal supervisory authority plus one supervisory authority per Land (16), except for the State of Bavaria which gathers two authorities.

This divergence can also be attributed to the lack of horizontal dialogue within the European Commission itself. **Julien Rossi** pointed to the "turf wars" between the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT), primarily guided by a logic of optimizing the data market (as reflected in the concept of data holder specific to the Data Act[5]), and the DG Justice, guardian of fundamental-rights doctrine (the concept of data controller specific to the GDPR). This inconsistency reflects itself within the connected devices or smart cars regulatory impasse. By their nature, these technologies capture data within individuals' private lives. Such practices historically fall under the terminal-access framework established by the ePrivacy Directive. This framework, however, does not fully coincide with the data-protection regime established by the GDPR, which it complements.

Lastly, **Jean-Sébastien Mariez** ended this roundtable by warning against the illusion of rewriting the foundational texts. Reforming the definition of personal data to respond to a political emergency amounts to undermining years of consistent and protective case law from the Court of Justice of the European Union (notably the landmark 2016 Breyer ruling as well as the recent case law on the right of access, including the CJEU's Brillen Rottler ruling). By opening the Pandora's box of textual revision, Europe risks weakening the attractiveness of its internal market while instilling permanent legal instability.

From left to right : Julien Rossi, Anissa Kemiche, Jean-Sébastien Mariez et Frithjof Michaelsen.

5. The manufacturer of the connected product or the provider of the related service that holds the data. https://www.donneespersonnelles.fr/data-act-rgpd-differences

Renaissance Numérique
www.renaissancenumerique.org
September 2026