

EU Commission unveils its plan to clean up the digital rulebook

Further to the [Mario Draghi report](#) last year, the European Commission (**Commission**) is working full speed to simplify the regulatory landscape. Building on the [President's Political Guidelines](#) and the Communication "[A Simpler and Faster Europe](#)", the Commission placed speed, coherence and simplification at the heart of its 2024–2029 mandate, as summed up by President von der Leyen: "less paperwork, less overlaps, less complex rules". To that end, the Commission has rolled out a series of legislative "omnibus" packages aimed at streamlining rules and cutting administrative burden. On 19 November, it released two digital omnibus proposals: one on the [simplification of the digital legislation](#) and the other on [simplification for AI rules](#) (together, the **Proposal**).

Below is a summary of the main changes proposed and their practical implications for the actors concerned.

Personal data

Relative concept of "personal data": The Proposal revisits the definition of personal data to exclude information that an entity processes without means enabling it to "reasonably likely" identify the underlying data subject. This aligns with the approach recently endorsed by the Court of Justice of the European Union (**CJEU**) in case C-413/23 P (*SRB v. EDPS*, see our [Client Alert, 11 September 2025](#)). Rather than assuming data is personal simply because someone, somewhere might identify an individual, the proposed approach focuses on what a given entity can actually determine. This does not fundamentally alter the scope of the General Data Protection Regulation (**GDPR**) but provides a more pragmatic definition aligned with recent case law.

This should encourage the use of pseudonymisation, in line with data minimisation and privacy by design principles. However, the Proposal goes on to empower the Commission to further detail the conditions under which pseudonymisation may no longer constitute personal data for certain entities. Stakeholders are likely to wait for such guidance from the Commission before relying on this new opening.

Amending rules on "special categories of data": A first draft of the Proposal that was unofficially released earlier this month contained a provision narrowing down the definition of "sensitive" data to information that would directly reveal such data. The final text abandoned that amendment and introduces new exceptions to the prohibition to process "sensitive" data, notably allowing it for the development and operation of artificial intelligence (**AI**) systems, subject to the implementation of strict safeguards.

"Codification" of legitimate interests as a legal basis for AI systems: In addition, the Proposal recognises the possibility to rely on legitimate interest as a legal basis to process data when

developing and operating AI models and systems, in line with what was foreseen by the European Data Protection Board (*EDPB*) in its [Opinion](#) of December 2024.

Businesses should not welcome this proposition as an unrestricted authorisation. Controllers will still need to perform and document a robust legitimate interest assessment. In this particular context, such an assessment will likely be under scrutiny by the regulators. The Proposal also introduces an unconditional right to object to one's use of personal data for such training. This should trigger enhanced transparency and user-friendly opt-out mechanisms that may however be difficult to implement in practice.

Integration of ePrivacy rules in the GDPR: The Proposal reduces the complexity created by the coexistence of rules governing the use of cookies and similar technologies on users' terminal equipment. This dual regime has generated legal uncertainty and higher compliance costs for controllers processing personal data obtained through such technologies.

The Proposal expands the range of situations in which cookies and comparable tools can be used without consent, including e.g. for audience measurement but only for the own use of the web owner (not for third parties). To reduce the risk of consent fatigue, the Proposal also requires controllers to set up automated and machine-readable users' preferences, in order to remember their refusals to consent for at least six months.

Streamlining data protection impact assessments (DPIAs): The Proposal requires setting up single EU-wide lists of processing operations that *do* and *do not* require a DPIA, in lieu of the current fragmented situation per Member State. These lists are due to be adopted by the Commission. Their preparation is entrusted to the EDPB which is also due to prepare a common template and a common method for conducting DPIAs going forward, subject to review every three years. This harmonisation is a welcome improvement.

Cybersecurity

A single-entry point for incident reporting under multiple legislations: The Proposal introduces a unified reporting platform to be operated by the European Union Agency for Cybersecurity (*ENISA*). This change should significantly simplify compliance with the patchwork of cybersecurity and data breach notification rules (including the GDPR, the Network and Information Security II Directive, the Digital Operational Resilience Act, the eIDAS Regulation, and the Critical Entities Resilience Directive). This "report once, share many" model is designed to reduce administrative workload for stakeholders, and therefore cut costs and enhance incident-response coordination.

Non-personal data

Consolidation into the Data Act: The Proposal consolidates most existing legislations dealing with non-personal data into the Data Act, marking a significant step towards a comprehensive EU non-personal data rulebook. This should ensure more uniformity and reduce the risk of overlaps and contradictions.

As part of this amendment, burdensome conditions like mandatory registration of data intermediation service providers becomes a voluntary regime.

Clarifying the Data Act: One of the main changes in the Data Act is the extension of the trade secret defence to refuse the sharing of data where there is a high risk that the data become

accessible in a foreign country offering a weaker trade secret protection compared to EU standards or lacking appropriate enforcement.

The Proposal also largely exempts data processing services that are custom-made for customer needs or provided by certain small-size providers from compliance, if the associated contract was concluded before or on 12 September 2025.

Artificial intelligence

While [Regulation 2024/1689](#) (the **AI Act**) is still in its early implementation phase, the Commission is already proposing targeted amendments to address anticipated implementation hurdles, reduce administrative burdens, and ensure a smoother, more innovation-friendly rollout. Key proposed changes include the following.

Flexible timelines and transitional measures: In an important shift, the application of the rules for high-risk AI systems is no longer tied to a fixed date. Instead, it is linked to the availability of harmonised standards and other compliance tools, which the Commission will confirm via a formal decision. High-risk obligations will then apply following a transition period, i.e. six months for Annex III systems (covering stand-alone high-risk use cases, such as biometrics or HR systems), 12 months for Annex I systems (covering safety components of regulated products such as machinery or medical devices), with an ultimate deadline on 2 December 2027 and 2 August 2028 respectively. In addition, a six-month grace period is introduced for generative AI transparency obligations. Providers of systems placed on the market prior to 2 August 2026 will have until 2 February 2027 to comply with “watermarking” requirements.

Centralising and strengthening supervision: According to the Proposal, supervision is due to be centralised under the AI Office, which will oversee AI systems in very large online platforms (**VLOPs**) and very large online search engines (**VLOSEs**) as defined in the Digital Services Act (**DSA**) as well as those based on a general-purpose AI model where the provider develops both model and system.

Easing the compliance burden: Key regulatory privileges benefiting small and medium enterprises (**SMEs**) are extended to small mid-caps (**SMCs**), including simplified technical documentation, streamlined quality management systems, and lower fine caps. The Proposal also removes the obligation for providers to register AI systems with potential high-risk usage when benefiting from the exceptions. Last, it softens the “AI literacy” obligation, shifting it from a direct duty on providers and deployers to the Commission and the Member States.

Streamlining conformity assessment: To prevent bottlenecks in certification, the Proposal simplifies the designation process for conformity assessment bodies. Those already designated under other EU product safety rules (e.g., medical devices) can undergo a single assessment procedure to cover AI requirements, speeding up their availability.

A pragmatic approach to bias detection: The Proposal enables the processing of special categories of personal data (in the sense of the GDPR), where strictly necessary for bias detection and correction, subject to strict safeguards.

Expanding and structuring innovation pathways: The Proposal broadens the use of regulatory sandboxes and real-world testing, including for high-risk AI systems. This should benefit European core industries and, in particular, the automotive sector.

Conclusion

The Digital Omnibus remains at the proposal stage. Once negotiations between the Parliament and the Council conclude, the final text may diverge significantly from the current version. Given the breadth of amendments put forward, discussions may prove lengthy. Some proposed grace periods could even lapse before adoption.

In addition, the Proposal represents only the first step towards optimising the application of the digital rulebook. The Commission has announced other initiatives, including a European Business Wallet to provide a secure, unified digital tool for business interactions across the EU. Meanwhile, Omnibus IV, which also addresses certain digital aspects, including extending the GDPR record-keeping obligation exception from SMEs to SMCs, is under discussion. Furthermore, the first regulation supplementing the GDPR has been recently adopted, bringing greater clarity to cross-border enforcement.

A central question is whether the Commission's initiatives to streamline the EU's digital regulatory framework will ultimately strengthen competitiveness as intended. This is clearly an outcome we wholeheartedly hope for.

KEY CONTACTS



Tanguy Van Overstraeten

Partner

tvanoverstraeten@vbb.com

+32 478 40 15 69



Gert-Jan Fraeyman

Sr. Associate

gjfraeyman@vbb.com



Dariusz Kloza

Sr. Expert

dkloza@vbb.com



Malik Aouadi

Associate

maoudi@vbb.com



Arian Birth

Associate

abirth@vbb.com



Ossama M'Rini

Associate

omrini@vbb.com