EU Digital Omnibus Package: Proposed rule simplifications and postponements

Published 11-Feb-2026 by
Tim Hitchcock

After unveiling an omnibus package in early 2025 to simplify, align and in some cases delay EU sustainability rules, the European Commission closed last year with a "Digital Omnibus Package" targeting data, resilience and AI laws. Like its sustainability counterpart, it aims to boost international competitiveness but could have a greater effect on businesses.

The package unveiled on November 19 contains two measures. A digital omnibus regulation would amend several measures. Some are embedded, like the General Data Protection Regulation (GDPR) and the 2002 e-Privacy Directive, which was to be replaced by a regulation until proposals were dropped in 2025. Others are new: the Data Act only took effect last September and member states have until July 17 to identify critical entities like financial market infrastructures under the Critical Entities Resilience Directive (CER).

The second part of the package is a "digital omnibus on AI" regulation that would revise provisions and timings in the EU AI Act. Many of its provisions covering high-risk systems will only take effect on August 2. Proposing changes and delays this late on is a significant step for the commission and could pose problems and uncertainty for businesses.

The context for the whole digital omnibus package is the 2024 Draghi report, which criticised "inconsistent and restrictive regulations" for holding back innovation in Europe. The commission estimates it would save businesses 5 billion euros in costs. Henna Virkkunen, commission vice-president, said the package responds to complaints about complicated and overlapping data rules and reporting requirements, and would also facilitate the use of high-quality data sets to train and develop AI systems.

"Many businesses feel they are under a lot of red tape they don't face in other markets, which is making the EU less competitive," said Tim Hickman, head of the data, privacy and cybersecurity practice at the law firm White & Case, based in London.

"The commission is under pressure to improve portions of the EU's digital legislation that are having an adverse effect and adding costs without providing much benefit."

Pseudonymised information

One key change in the general regulation concerns the issue of when an individual is identifiable from pseudonymised information, making that information "personal data" and subject to GDPR processing restrictions. Complications arose from the Court of Justice of the EU (CJEU) case of Breyer, which ruled that pseudonymised information must be treated as personal data if a data controller could access additional information that would identify the data subject.

That broad interpretation meant firms had to treat large quantities of information as personal data, restricting its use. In EDPS v SRB last September, the CJEU took a more subjective approach towards identifiability, with "personal data" status depending on whether a data recipient could identify its subject using "the means reasonably likely to be used."

The proposed general regulation puts that test into an addition to GDPR Article 4. This would replace a recital that requires "all" reasonably likely means to be considered, therefore leaning further towards pseudonymised information being personal data.

"The commission is effectively codifying the CJEU's SRB judgment," Hickman said.

"As a result, data would not be "personal data" in the hands of an entity if that entity cannot (taking into account "the means reasonably likely to be used") identify the individual to whom it relates. If this change is implemented, it will mean that some businesses will have stronger arguments that the data they process is not personal data, and their processing activities are therefore not subject to the GDPR."

Data breach reporting

Another proposal in the general regulation would extend the deadline for notifying the competent supervisory authority of a data breach from 72 to 96 hours.

"Rolling back the GDPR data breach reporting deadline from 72 to 96 hours is welcome, but in practice will make very little difference for most companies," Hickman said.

"Initial reports will still be very high-level of necessity. It takes businesses some time to pull together detailed information and send it to the relevant authority or authorities, so the existing approach of a high-level data breach notification followed by a more detailed investigation and report will remain the norm."

Similarly, firms may welcome a proposed single-entry point for reporting data breaches and cybersecurity incidents, and the resulting simplifications. A new body, to be developed by the EU cybersecurity agency ENISA, would receive and forward reports under a "report once, share many" principle. This arrangement would cover various regimes, including GDPR, CER, and the Digital Operational Resilience Act (DORA), but reporting could remain complex in practice.

"A single-entry point for incident reporting is a positive development, but it is likely to have limited impact because many businesses face parallel reporting obligations under multiple EU laws in relation to a single incident, not all of which will fall within the single-entry point," Hickman said.

"In addition, once a notification is filed, many businesses are at risk of parallel enforcement proceedings on the same facts, by regulators in different EU member states."

Special categories of data

The package makes several clarifications of requirements affecting non-high-risk AI systems. It also proposed replacing AI Act Article 10(5) with a new Article 4a. This would allow firms to make greater use of special types of personal data that GDPR Article 9 puts under extra safeguards.

"A major change involves permitting greater use of special categories of data (SCD) to test and develop AI systems," Hickman said.

"Limited processing of SCD would be permitted on the basis that 'bias detection and correction constitute a substantial public interest.' AI companies have broadly welcomed this change because none of the other grounds for processing SCD in Article 9 GDPR are viable in the context of testing AI systems."

Proposed delays to enforcement

Probably the commission's most challenging AI Act proposal is to postpone the application of those rules, which are due to apply from August. This is due to delays producing the necessary standards, specifications and guidelines, but is embarrassing to say the least, given the commission's earlier refusal to grant a postponement. Furthermore, although EU leaders are to hold a February summit on competitiveness and making regulation more conducive to innovation, not everyone wants to see digital regulation weakened or delayed.

"In mid-2025, in response to requests from business to delay implementation of the AI Act, the commission bluntly stated that it would not do so," Hickman said.

"However, the Omnibus package published in November 2025 proposes phased delays to enforcement of the rules on high-risk AI systems. It remains to be seen whether the commission will be able to make these changes before the scheduled start of enforcement on August 2."

"This has left many businesses in limbo, uncertain of when enforcement will begin. In addition, civil liberties groups and other interested parties have opposed a postponement."

(Tim Hitchcock, for CUBE Regulatory Intelligence)

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 12-Feb-2026