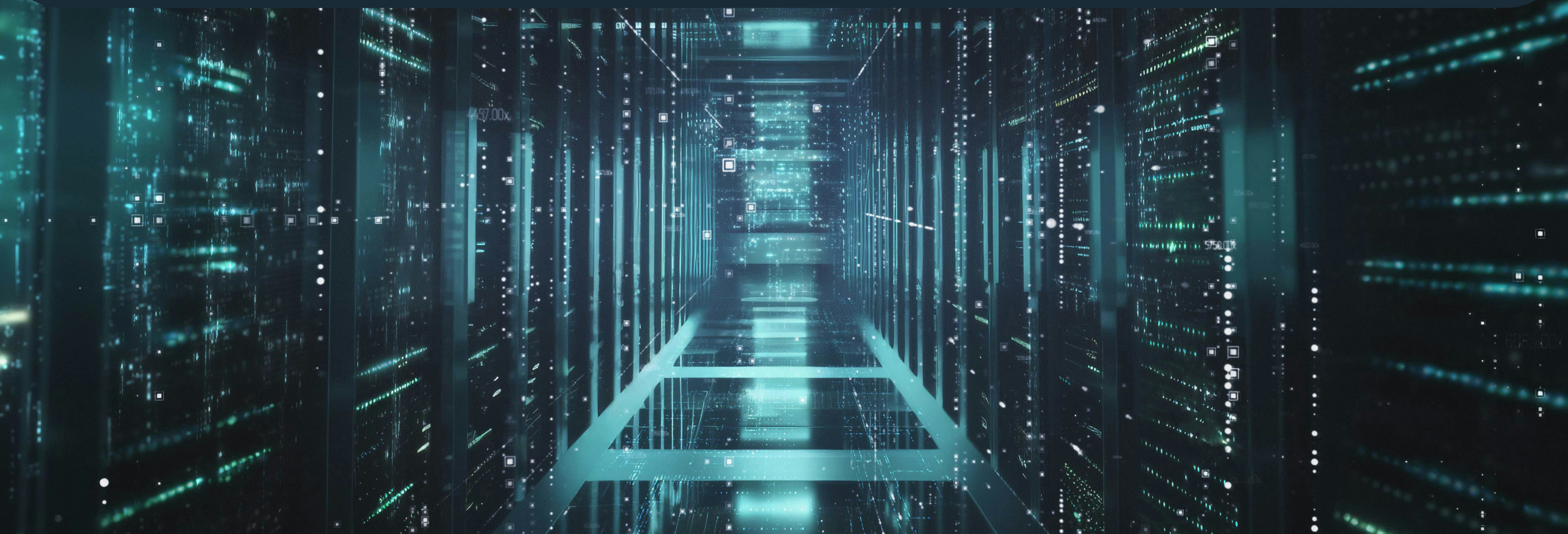
08 Issue 2026

Legance

What's at stake with the Digital Omnibus recently agreed to by EU co-legislators



On 7 May 2026, the Council of the European Union and the European Parliament reached a **provisional agreement** on the **AI Act component of the Digital Omnibus package**, following the Parliament's plenary vote of 26 March 2026. The GDPR-related component of the package, instead, remains at a considerably more contested stage of the legislative process.

On the AI Act, the most immediately consequential element of the agreement concerns the **revised application timeline for high-risk AI systems:**

- **Obligations for systems listed under Annex III** - covering for example use cases including biometrics, critical infrastructure, education, employment and law enforcement - will apply from **December 2, 2027**, rather than August 2, 2026;
- For **high-risk systems integrated into products regulated by harmonization legislation under Annex I**, the applicable date will be **August 2, 2028**;
- **Watermarking obligations for AI-generated content** will apply from **December 2, 2026**.

The agreement also introduces a significant addition to the list of forbidden AI Systems (which was already effective since February 2, 2025): systems designed for the generation of child sexual abuse material or non-consensual intimate imagery will be added to the **list of prohibited practices**, covering both their placing on the market and their use by deployers, as of the 2nd of Decembre 2026. The agreement further reinstates the **obligation for providers to register high-risk AI systems in the EU database** - including where providers consider their systems exempt from high-risk classification - and confirms the **strict necessity standard for the processing of special categories of personal data for bias detection purposes.** The agreement remains provisional and the definitive legislative text has not yet been published.

Against this background, the parallel proposal for a Regulation aiming at reviewing the GDPR remains in a stalemate. Political agreement has not been reached yet on the **amendment to Article 4(1) of the GDPR**, which goes to the heart of one of the most foundational questions in data protection law: when does a piece of information qualify as "**personal data**"?

The GDPR - read in light of **Recital 26 - requires identifiability to be assessed by taking into account not only the capabilities of the controller itself, but also the means reasonably available to any third party which, even in abstract terms, could be deemed to respond to the recipient controller.** That was, in fact, the factual background **in the Breyer judgment** (C-582/14), where **the Court established that dynamic IP addresses constitute personal data for a website operator** even when the operator itself lacks the means to identify the user directly, provided **there is a legal pathway to obtain that information from a third party** such as an internet service provider, despite the fact that to get that piece of missing information, the website operator (a government agency in the case at stake) had to go through law enforcement authorities.

The Commission's proposal would align the definition of personal data to an extensive reading of the recent Deloitte Case (C-413/23 P), by introducing a subjective, controller-specific criterion: **information would not constitute personal data for a given controller if that controller neither has nor could reasonably acquire the means to identify the individual, where the reasonability of such access to the missing piece of information is assessed from the recipient's perspective and not in general terms (i.e. Deloitte, the recipient of data from SRB, had no reasonable means to the reverse the pseudonymization/encoding carried out by the sending controller, the SRB).**
The structural implications are significant: the **same dataset could simultaneously qualify as personal data for one actor and non-personal data for another, depending on their respective capabilities.**
The joint EDPB-EDPS opinion of February 2026 expressed unambiguous opposition to this course, concluding that the proposal contradicts established case law and would **materially narrow the concept of personal data.** Council compromise texts indicate that a significant number of Member States favor deletion of the proposed amendment or its replacement with an EDPB guidelines mandate.

For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it