Cooley

EU AI Act: Proposed 'Digital Omnibus on AI' Will Impact Businesses' AI Compliance Roadmaps

November 24, 2025

This update covers the European Commission's proposed "Digital Omnibus on AI", published 19 November 2025. Part of the European Union's simplification drive, the proposal aims to streamline the EU Artificial Intelligence (AI) Act's implementation, ease compliance burdens and adjust compliance deadlines ahead of the AI Act's full application on 2 August 2026.

The targeted amendments have important implications for businesses that place, put into service and/or use AI systems in the EU, as well as for product manufacturers that integrate AI systems into their hardware products. We've unpacked some of the key changes and simplification measures proposed by the Digital Omnibus on AI and what these might mean for businesses' AI compliance roadmaps.

For additional insights on the EU AI Act and its compliance implications, see our recent resources:

- AI Talks: Understanding the EU AI Act – What It Means for Companies Worldwide
- The EU AI Act: Key Milestones, Compliance Challenges and the Road Ahead

Key changes and simplification measures

The targeted amendments to the EU AI Act proposed by the Digital Omnibus on AI include:

1. **Extended compliance timelines for high-risk AI requirements**

Under the current EU AI Act, the rules on high-risk AI systems apply from 2 August 2026 (for Annex III use cases) or 2 August 2027 (for high-risk systems embedded into or comprising regulated products). The omnibus proposal seeks to delay the application date for these requirements, making application conditional on the readiness of applicable harmonised standards, common specifications or guidelines. A new long-stop date means that the rules on high-risk systems would apply, at the latest, from 2 December 2027 (Annex III systems) and 2 August 2028 (systems comprising or embedded into regulated products), even if standards are still lagging. The European Commission could bring the application of these requirements forward if it decides that "adequate measures in support of compliance" exist, but there's no clear test for adequacy, leaving timing uncertain. Businesses would then have six months (for Annex III use cases) or 12 months (for product/safety components) after that decision to comply.

2. **Extended grace periods for legacy AI systems**

The omnibus proposal introduces targeted grace periods for certain AI systems already on the EU market.

Providers of generative AI systems released before 2 August 2026 would have an additional six months (until 2 February 2027) to retrofit their systems to meet new transparency obligations, such as marking artificially generated or manipulated content using watermarks, metadata or other digital tags.

The Article 111 "grace period" for legacy high-risk systems placed on the market or put into service before the high-risk rules start to apply is also clarified, marking **a significant divergence from the compliance approach taken for hardware products with impacts for compliance strategies.** If at least one unit of a high-risk AI system was lawfully placed on the EU market before the new rules apply, identical units of that system can continue to be placed or used without the need to retrofit or triggering requirements for additional certification, provided the design of that high-risk AI system remains unchanged. **For most businesses, this compliance cliff will encourage the accelerated launch of products in advance of deadlines for high-risk AI compliance.** (However, if such legacy systems are intended for use by public authorities, providers must nevertheless bring them into full

compliance by 2 August 2030.)

3. **Broader application of the bias mitigation derogation for personal data processing**

The omnibus proposal would expand the current exemption allowing certain AI providers to process sensitive data to detect and correct bias. Under the new rules, all AI providers and deployers – regardless of risk level or training method – could use this exemption to reduce bias, provided they meet the same processing conditions. For high-risk systems that do not involve model training, the derogation would remain limited to dataset testing.

4. **Deletion of registration requirements for 'not high-risk' AI systems**

Currently, AI providers that demonstrate an Annex III use case is not high-risk – such as when the system is used only for preparatory tasks – must still register the system in the EU database. The omnibus proposal would remove this requirement. Providers would, however, remain obligated to document their risk assessments and make them available to regulators upon request.

5. **Codes of practice lose hard-law pathway**

The European Commission would lose its powers to adopt binding codes of practice for general-purpose AI models and the marking of artificially generated or manipulated content. Codes could still be adopted, but they would remain "soft law", limiting enforceability.

6. **Clarifications on conformity assessment procedures for embedded AI**

The omnibus proposal clarifies that when a high-risk AI system is both subject to product regulation (Annex I, Section A) and classified as a high-risk Annex III use case, the conformity assessment required under the relevant product regulation will take precedence.

7. **Increased flexibility for post-market monitoring**

Post-market monitoring remains mandatory, but businesses would no longer be required to follow a template plan previously scheduled for adoption in February 2026.

8. **New regulatory sandboxes and broader real-world testing approvals**

The omnibus proposal introduces an EU-level regulatory sandbox alongside existing national sandboxes for general-purpose AI models, creating a dual-layer structure. This will allow businesses – particularly small and medium-sized enterprises (SMEs) and small mid-caps (SMCs) – to pilot high-impact AI solutions under regulatory guidance in real-world conditions for a limited period. Beyond formal sandboxes, Article 60 of the AI Act, which permits pre-market, real-world testing of certain high-risk AI, is broadened. Providers of high-risk AI covered by product regulation (Annex I) – such as machinery, toys, radio equipment, vehicles and medical devices – would be allowed to conduct controlled live trials before full certification, subject to safeguards and oversight.

9. **Relief for SMEs and SMCs**

The AI Act already provides reduced obligations for SMEs. The omnibus proposal would extend certain SME carve outs to include SMCs – those that do not qualify as SMEs but meet the employee threshold and one of the two financial thresholds:

Number of employees	Net turnover	Balance sheet total
< 750	≤ 150 million euros	≤ 129 million euros

Under the proposal, SMCs would benefit from simplified technical documentation requirements when demonstrating compliance with high-risk AI requirements, more proportionate expectations for quality

management systems and caps on penalties for noncompliance. SMEs would themselves benefit from the further simplified quality management system requirements, currently reserved for microenterprises.

10. **Greater enforcement coordination**

The omnibus proposal centralises enforcement by granting the European Commission's new AI Office exclusive supervisory authority over certain AI systems, including those based on general-purpose AI models and systems embedded in or constituting "very large online platforms" (VLOPs) or "very large online search engines" (VLOSEs) under the Digital Services Act .

This also means that providers of systems that are high risk and subject to third-party conformity assessment could now face pre-market conformity testing by the European Commission. Meanwhile, the omnibus proposal clarifies that enforcement for high-risk AI systems embedded in regulated products listed in Annex I, Section A, would remain with the relevant national product safety regulators. Enhanced cooperation requirements for regulators should meanwhile reduce administrative burdens for business. Regulators investigating fundamental rights violations will need to make information requests to the relevant market surveillance authority rather than the business.

What's next?

The Digital Omnibus on AI is currently only a proposal. It will now proceed to the Council and Parliament, where – given the political interest – further amendments are likely, meaning trilogue negotiations are expected. With implementation targeted for 2026 – 2027, there is considerable time pressure to finalise changes to the EU AI Act before the current compliance deadline of 2 August 2026. If adopted in its current form, the Digital Omnibus on AI would enter into force three days after publication in the Official Journal of the EU.

The bundling of all amendments together and the absence of a separate "stop-the-clock" proposal raises the stakes. Failure to reach political agreement and adopt amending legislation before August 2026 would mean the existing high-risk AI requirements apply as originally drafted, possibly before the supporting standards or tools are ready. Delays in adoption risk uneven enforcement and litigation risk for companies. While retroactive "pardons" might be possible, they would face tight legal constraints and judicial scrutiny.

Practical takeaways

1. **Remap timelines:** Plan for delayed high-risk AI compliance dates, but model an early activation scenario if the European Commission deems compliance tools "adequate".
2. **Track standards:** The real trigger for high-risk AI requirements may be standards availability, common specifications or guidance – monitor development closely.
3. **Prepare for gaps:** Build contingency for an applicability gap if the omnibus proposal slips, including exposure to claims and national enforcement variance.
4. **Update data strategies:** Reassess General Data Protection Regulation lawful bases for model training and sensitive data use; ring fence model level versus system level bias processing with data protection impact assessments (DPIAs) and necessity/proportionality analyses.
5. **Anticipate labelling friction:** Expect a lag between developer tooling and user disclosure duties; document reasonable efforts and technical constraints.
6. **Maintain robust records:** Even without registration of out-of-scope high-risk AI systems, preserve self-assessment evidence and risk rationales to withstand supervisory scrutiny.
7. **Watch governance changes:** Centralised assessments and softer codes will alter how you evidence compliance – and who you engage with – pre-market.

For questions about how these developments may impact your business, please contact Cooley's EU cyber/data/privacy and international products teams.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act

or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Patrick Van Eecke **Brussels**	**pvaneecke@cooley.com** **+32 2 486 7501**
Enrique Gallego Capdevila Brussels	ecapdevila@cooley.com +32 2 486 7534
Bartholomäus Regenhardt Brussels	bregenhardt@cooley.com +32 2 486 7542
Jack Eastwood London	jeastwood@cooley.com +44 (0) 20 7556 4372
Rod Freeman London	rfreeman@cooley.com +44 (0) 20 7556 4429
Claire Temple	ctemple@cooley.com +44 (0) 20 7556 4170
Edward Turtle London	eturtle@cooley.com +32 2 486 7506

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.