CLIENT ALERT | May 13, 2026

AI Act Update: EU Resolves to Change Rules and Extend Deadlines

EU lawmakers have agreed to reduce overlap of rules, introduce new prohibitions, and extend deadlines for high-risk AI systems.

On May 7, 2026, EU legislative bodies reached a political agreement on proposed amendments to the AI Act (the Agreement). This "AI Act Omnibus" forms part of the EU's broader Omnibus legislative package aimed at simplifying digital regulation. The Agreement clarifies existing AI Act requirements, extends compliance deadlines for high-risk AI systems (HRAIS), and introduces new rules on AI-generated intimate content. The European Commission (Commission) has also published guidelines and a draft Code of Practice addressing the AI Act's transparency requirements.

Although the Agreement still requires formal adoption, companies offering or using AI systems in the EU should begin aligning their compliance programs with the new framework. This Client Alert summarizes the key changes, explains other recent AI Act developments, and outlines practical steps for adapting to the new rules.

Core Changes at a Glance

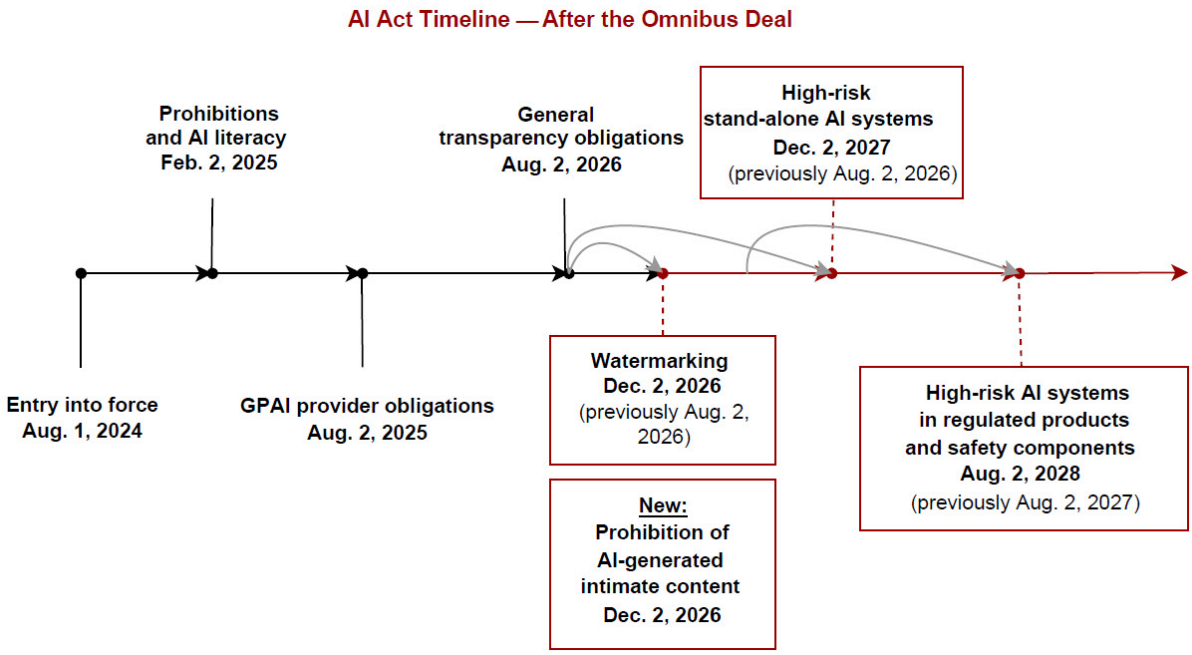
The Agreement does not change the AI Act's core architecture. It preserves the risk-based approach and the general obligations of providers and deployers. However, the Agreement proposes several updates that affect scope, practical application, and enforcement, including:

- a new prohibition targeting so-called "nudifier" applications generating potentially harmful intimate content, including child sexual abuse material (CSAM);
- extended deadlines for HRAIS obligations and watermarking transparency requirements;
- the removal of certain industrial applications from the AI Act's scope; and
- a streamlined process for bias detection.

The extension of the HRAIS compliance deadlines is a significant change in practice. Companies should use these deadlines as a basis for implementation planning.

Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Hong Kong, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practice in Japan. Latham & Watkins operates in Israel through a limited liability company, in South Korea as a Foreign Legal Consultant Office, and in Saudi Arabia through a limited liability company. © Copyright 2026 Latham & Watkins. All Rights Reserved. Under New York's Code of Professional Responsibility, portions of this communication contain attorney advertising. Prior results do not guarantee a similar outcome. Results depend upon a variety of factors unique to each representation. Please direct all inquiries regarding our conduct under New York's Disciplinary Rules to Latham & Watkins LLP, 1271 Avenue of the Americas, New York, NY 10020-1401, Phone: +1.212.906.1200.

The chart below summarizes the new deadlines for AI Act requirements across the EU.



Prohibited Practices: New Prohibition of AI-Generated Intimate Content

Certain AI practices have been prohibited under Art. 5 AI Act since **February 2, 2025**, including social scoring, subliminal manipulation, and real-time biometric remote identification in public spaces. Effective December 2, 2026, the Agreement extends these prohibitions to "nudifier" applications — AI systems that generate or manipulate sexually explicit or intimate images, video, or audio without explicit consent, or that create CSAM. Providers and deployers may not use or place on the EU market AI systems designed to create intimate deepfakes or CSAM, or that lack reasonable safeguards against such use. Violations may trigger fines of up to €35 million or 7% of annual worldwide turnover, whichever is higher.

There is also potential exposure to civil (mass) claims under EU product liability rules. To mitigate these risks, companies should anticipate potential misuse during development, implement appropriate safeguards, conduct comprehensive risk assessments, and monitor for harmful use.

HRAIS: Extended Deadlines to Comply With Comprehensive Framework

The AI Act imposes stringent requirements on HRAIS, which apply to two categories of AI system:

- stand-alone AI systems that fall within certain use cases set out in the AI Act, including systems used for recruitment and performance evaluation, credit scoring, insurance risk assessment, emotion recognition, biometric identification, and critical infrastructure applications; or
- AI systems that are products, or safety components of products, regulated by certain EU product safety laws listed in the AI Act, including medical device, vehicle, and toy safety rules.

HRAIS must comply with comprehensive obligations including risk management, data governance, technical documentation, transparency and human oversight, and accuracy, robustness, and cybersecurity. The Commission faced calls to extend the compliance deadlines for HRAIS as it has not yet issued relevant harmonized standards and guidance to enable practical implementation within the original deadlines set out in the AI Act.

The Agreement extends the compliance deadlines for stand-alone HRAIS to **December 2, 2027**. This stand-alone extension does not apply to AI systems that qualify as regulated products or safety components, for which the deadline is extended to **August 2, 2028**. Significantly, AI systems placed on the EU market before these respective dates will not be subject to the HRAIS requirements unless they undergo a substantial modification after that date.

The extension gives companies additional time to finalize risk classifications, build governance frameworks, and prepare technical documentation and monitoring systems. At the same time, companies should remember that their HRAIS may already be subject to other applicable legal obligations — particularly under the GDPR in relation to personal data (which is very broadly defined). EU data protection authorities are already actively enforcing the GDPR in the AI sector – including respective rules on data minimization, transparency, and data security requirements.

Transparency Obligations: Extended Deadline for Watermarking and New Guidelines

The Agreement does not change the scope of existing AI Act transparency obligations under Art. 50 AI Act. These requirements include:

- disclosure obligations for interactive AI systems, emotion recognition and biometric categorization systems, and deepfakes; and
- watermarking/labeling obligations for AI-generated or manipulated content.

The scope of these obligations is further specified in draft Guidelines on the implementation of the transparency obligations for certain AI systems, which the Commission recently published for consultation. These Guidelines provide non-binding interpretive guidance on Art. 50 AI Act, together with a Code of Practice on Transparency of AI-Generated Content drafted by independent experts that translates these obligations into practical compliance measures. Both guidelines are published as draft versions for stakeholders to provide comments, with final versions expected in the coming weeks, which are expected to closely follow the consultation drafts.

The obligations set out in Art. 50 AI Act apply from **August 2, 2026**. Under a grandfathering rule introduced by the Agreement, generative AI systems (i.e., AI systems specifically intended to generate synthetic content such as text, images, audio, or video) placed on the market or put into service before that date must comply with the watermarking requirements only as of **December 2, 2026**. Violations may result in fines of up to €15 million or 3% of total annual worldwide turnover, whichever is higher.

Further Adjustments: Reducing Regulatory Overlaps and Clarifying Scope and Enforcement

The Agreement further addresses a central concern raised during negotiations: the interaction between the AI Act and existing EU sectoral safety legislation governing products that incorporate AI systems.

- **Industrial AI carveout:** AI used in industrial applications and products already regulated under the Machinery Regulation is exempt from the AI Act. Other regulated industrial products and safety components — including medical devices, toys, lifts, and certain transportation applications — need only comply with applicable sectoral safety rules, rather than potentially duplicative AI Act requirements.
- **Narrower definition of "safety component":** The Agreement narrows the definition of "safety component" for HRAIS classification purposes. Relevant regulated products with AI functions that merely assist users or optimize performance will not automatically be subject to HRAIS obligations, provided that failure or malfunction does not create health or safety risks.
- **SME simplifications extended to mid-caps:** The AI Act's simplified compliance framework for small- and medium-sized enterprises will be extended to companies with up to 750 employees and €150 million in annual revenue. Benefits include simplified guidance, reduced fines, regulatory sandbox access, and standardized documentation templates.
- **Bias detection:** The amendments make it easier to use GDPR special category personal data (e.g., health information, biometric data, race, or sexual orientation) where necessary to detect and mitigate bias in AI models.

Outlook and Implications for Business

The Commission has not yet published the provisionally agreed text. The text will proceed to formal adoption by the European Parliament and the Council, which is expected by July 2026 — ahead of August 2, 2026, when HRAIS requirements would otherwise take effect.

The extended compliance deadlines provide additional time for implementation. However, given the complexity of the EU's AI regime, companies should not slow down their compliance and governance efforts. Harmonized standards and guidance needed for practical implementation may not be published until close to the new deadlines, leaving limited time to adapt.

The AI Act's prohibitions on particularly harmful AI practices (e.g., exploitation of vulnerable individuals, social scoring) are already in force. It will be supplemented by the new rules on AI-generated intimate content and CSAM as of December 2, 2026. The transparency obligations for chatbots take effect in August 2026, and the deferral for AI-generated content labeling is only four months (to December 2, 2026). These requirements may carry significant civil liability exposure and, in some cases, fines of up to €35 million or 7% of annual worldwide turnover, whichever is higher.

EU data protection authorities are already enforcing the GDPR in an AI context, having imposed fines and prohibited specific uses of AI systems and models. Companies should reflect this evolving enforcement landscape in their AI Act compliance strategies and broader AI governance programs. Practical steps include building in flexibility to accommodate forthcoming standards, guidance, and evolving market practices. Demonstrated AI Act readiness is increasingly seen as a competitive advantage and a marker of credibility in the European market.

Contacts

Sophie Goossens
sophie.goossens@lw.com
+44.20.7710.3080
London / Paris

Jean-Luc Juhan
jean-luc.juhan@lw.com
+33.1.4062.2000
Paris

Susan Kempe-Müller
susan.kempe-mueller@lw.com
+49.69.6062.6580
Frankfurt

Alfonso Lamadrid
alfonso.lamadrid@lw.com
+32.2.788.6310
Brussels

Tim Wybitul
tim.wybitul@lw.com
+49.69.6062.6560
Frankfurt / Brussels

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

James Lloyd
james.lloyd@lw.com
+44.20.7866.2668
London

Fiona M. Maclean
fiona.maclean@lw.com
+44.20.7710.1822
London

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

This publication is produced by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. See our Attorney Advertising and Terms of Use.