



EU AI Act: Approved Text – Summary of Key Changes

4 February 2024

On 2 January 2024, the latest draft of the EU AI Act was leaked. This draft includes the proposed compromise edits to the regulation, as agreed between the European Parliament, Council of the EU and European Commission.

On 2 February 2024, the Act was [finalised](#), this development provides a clear indication of what organisations can infer from the final text. This document summarises some of the key changes that have now been agreed.

Key Changes

1. Subject matter and scope

The compromise text outlines the AI Act's primary purpose: ensuring high-level protection for health, safety, and fundamental rights, including democratic principles and environmental safeguarding. Notably, it aligns with the Council's mandate, focusing on risks to health, safety, and fundamental rights, excluding national security.

2. Definition of an AI system

The revised definition aligns with international standards, particularly the OECD's work on artificial intelligence. The compromise emphasizes that it excludes simpler traditional software systems, with guidelines to be developed by the Commission.

3. Prohibited AI practices

The compromise includes prohibitions on real-time biometric identification by law enforcement, scraping facial images, emotion recognition (limited to workplaces and educational institutions), and a nuanced ban on individual predictive policing. Notably, certain biometric and emotion recognition systems are added to Annex III with limitations.

4. Post-remote biometric identification

Law enforcement's use of post-remote biometric identification is subject to safeguards, including transparency measures, authorization requirements, and limitations on untargeted use.

5. Exceptions for law enforcement authorities

Preserving exceptions for law enforcement, the compromise maintains derogation from conformity assessment and allows real-world testing without prior authorization, with market surveillance by data protection authorities.

6. Fundamental rights impact assessment

A light version of the fundamental rights impact assessment applies to certain deployers, ensuring alignment with existing legal obligations and facilitated compliance through AI Office-developed templates.





7. Testing high-risk AI systems

The compromise retains provisions for testing high-risk AI systems outside AI regulatory sandboxes, incorporating safeguards such as market surveillance authority approval, data deletion rights, and limitations specific to law enforcement and related areas.

8. General purpose AI models

New provisions address general purpose AI models, introducing obligations, risk assessments, and reporting requirements, with industry-developed codes of practice and compliance evaluation by the AI Office.

9. Governance and enforcement

The compromise establishes the AI Office for centralized oversight of general purpose AI models, enhancing the AI Board's role and introducing a scientific panel and advisory forum for expert input and stakeholder engagement.

10. Derogation from conformity assessment

The compromise maintains derogation from conformity assessment for certain AI systems, emphasizing Commission control over the authorization process.

11. AI systems already placed on the market

Public authorities with high-risk AI systems have four years to ensure compliance, aligning with the Council's position, and GPAI models have a two-year compliance window.

12. Implementing acts and delegated acts

The compromise preserves choices from the Council's mandate regarding delegated and implementing acts, clarifying instances where only delegated acts are possible.

13. Penalties

Penalty amounts are fine-tuned, with a maximum penalty for prohibited AI practices set at 35 million EUR or 7% of annual turnover. Providers of general purpose AI models have a grace period with no fines during the first year.

14. Entry into application

The compromise establishes a 24-month entry into application period for most Regulation aspects, with varying deadlines for specific elements. Prohibitions have a 6-month deadline, and governance, general purpose AI models, confidentiality, and penalties have deadlines ranging from 12 to 36 months.

How Can We Help?

We can help you comply with the EU AI Act in one or more of the following ways:

- Providing strategic, professional and regulatory advice on the scope and application of the EU AI Act, including delivering an impact or risk assessment, which includes using our cutting-edge regulatory technology solution, [Orthrus](#).
- Helping you achieve to achieve compliance with the requirements of the EU AI Act to safeguard your AI systems for this landmark regulation.
- We also deliver regulatory, first-in-class training sessions on the EU AI Act which we would be happy to customise for your business.

We have developed an EU AI Act toolkit, setting out the ways in which we can help your business deal with AI-related business issues, regulatory or otherwise.

