



Cybersecurity And Technology Law

The EU Launches First AI-Act Inquiries

October 23, 2026

The EU Launches First AI-Act Inquiries against AI Developers

BY IRENE KYRIAKIDES, NATALIA SOULIA, NIKOLAOS TILEMACHOS VELLIOS

In October 2026, the European Commission's AI Office launched its first enforcement inquiries under the EU AI Act. According to publicly available reports, the inquiries followed alleged incidents in which AI models undergoing cybersecurity evaluations gained unauthorized access to external systems. In particular, frontier AI developers' reports indicate that certain agents breached intended containment measures during cybersecurity testing and compromised external infrastructure.

As confirmed by Henna Virkkunen, European Commission Executive Vice-President for Tech Sovereignty, Security and Democracy, on October 14, 2026, the AI Office exercised its formal enforcement powers (which have applied since August 2026) by issuing Requests for Information to the developers concerned, following voluntary disclosures that were considered insufficient.

Does the AI Act Apply to Pre-Market Development Activities?

- ▶ **The Statutory Carve-Out:** Article 2(8) of the AI Act expressly excludes pre-market research, testing and development activities from the scope of the Regulation. Industry counsel argues that an unintended breach by an evaluation agent during internal sandbox testing does not readily fit the definition of placing an AI system on the market.
- ▶ **The EU's Interpretation:** Although purely internal testing is exempt, recent developments raise the question whether and in what circumstances the research-and-development exemption could cease to apply once a model escapes its testing environment and affects the EU market. On this interpretation, disruption of the EU market would evidence a failure to comply with mandatory risk-mitigation measures, thereby triggering the application and enforcement of the AI Act.

Scientific Panel's Warnings

The AI Office's independent advisory panel identified two interrelated concerns:

1. **Cybersecurity safeguards:** Risks posed by internal models during development require stronger governance, together with enhanced cybersecurity capabilities to detect and investigate incidents of containment breaches.
2. **Model behavior and oversight:** High-capability models may deviate from intended objectives and mislead evaluators, warranting closer scrutiny of training techniques and architectures that may limit model monitorability.

Key Legal Takeaways

- ▶ **Constructive placing on the market:** It remains contested whether an autonomous external breach by an AI model can constitute a constructive "*placing on the market*" within the meaning of Article 3 of the AI Act, therefore establishing the EU's jurisdiction.
- ▶ **A precedent for containment as a compliance obligation?** While the AI Act does not require any specific architecture, the security of evaluation environments is likely to be assessed under the cybersecurity and risk-reduction obligations. Insufficient robust sandbox security could therefore potentially establish the Commission's jurisdiction, irrespective of whether the AI system has formally been placed on the market.
- ▶ **Escalation and financial exposure:** If the responses to the Requests for Information fail to satisfy the AI Office, the Commission may escalate the matter from an administrative inquiry to formal non-compliance proceedings, potentially exposing developers to fines of up to 3% of their total worldwide annual turnover.

Contact Us



Irene Kyriakides

PARTNER

i.kyriakides@kglawfirm.gr



Natalia Soulia

COUNSEL

n.soulia@kglawfirm.gr



Follow Us

ATHENS OFFICE

28, Dimitriou Soutsou Str.,
115 21 Athens

T +30 210 817 1500
E kg.law@kglawfirm.gr

THESSALONIKI OFFICE

31, Politechniou Str.,
551 34 Thessaloniki

T +30 2310 441 552
E kg.law@kglawfirm.gr

www.kglawfirm.gr

Disclaimer: This newsletter contains general information only and is not intended to provide specific legal, or other professional advice or services, nor is it suitable for such professional advice, and should not be used as a basis for any decision or action that may affect you or your business. Before making any decision or taking any action that may affect you or your business, you should consult a qualified professional advisor. We remain at your disposal should you require any further information or clarification in this regard.

©Kyriakides Georgopoulos, 2026