Regulatory Updates since Toolkit v1.1

Issued 2 September 2026 by the ICT4Peace Foundation · Version 1.1 · Covers developments to 31 August 2026

Status of this document

This addendum supplements the twelve tools of the Toolkit for Responsible Technology Use by Private (Cyber) Security Companies, version 1.1, published June 2026. It records regulatory developments confirmed after that publication date.

Where this addendum and a v1.1 tool document differ on a date, an obligation or an enforcement position, this addendum states the current position and prevails. Tool documents will be revised at the next quarterly content review.

It is maintained by the ICT4Peace Foundation as part of the Toolkit's standing governance process: monthly regulatory monitoring, quarterly content review. Each month's confirmed developments are appended here.

Key dates at a glance

Obligation	Applies from	Who it affects
EU AI Act — Article 50 transparency duties	2 August 2026 (in force and enforced)	Deployers and providers of AI systems, including private security companies using emotion recognition, biometric categorisation or generative AI
EU AI Act — Article 50 marking for systems already on the market	2 December 2026	Providers of generative AI systems placed on the market before 2 August 2026
EU Platform Work Directive — national transposition	2 December 2026	EU member states; national laws will reach platform-mediated security staffing
EU AI Act — Annex III standalone high-risk obligations	2 December 2027 (postponed from 2 August 2026)	Providers and deployers of high-risk AI, including biometrics, employment, critical infrastructure, law enforcement
CSDDD — member state transposition	26 July 2028	EU member states must have written the directive into national law
CSDDD — obligations apply to companies	26 July 2029	A single application date for all in-scope companies: EU companies with more than 5,000 employees and net worldwide turnover above EUR 1.5 billion; non-EU companies with more than EUR 1.5 billion of turnover generated in the EU
EU AI Act — Annex I product-embedded high-risk obligations	2 August 2028 (postponed from 2 August 2027)	Providers of AI embedded in regulated products

1. EU AI Act transparency duties are now in force and being enforced

Since 2 August 2026 the European Commission's AI Office and national market surveillance authorities have been enforcing the EU AI Act, and the transparency obligations in Article 50 apply directly.

Under Article 50, a company deploying an emotion recognition system or a biometric categorisation system must inform the people exposed to it that the system is in operation. This is a duty on the deployer, not only on the provider — so a private security company operating behavioural-analytics CCTV, aggression or distress detection, or biometric sorting of individuals carries the obligation itself, whoever built the system.

Also under Article 50, deepfake images, audio and video must be labelled as artificially generated or manipulated, and AI-generated text published to inform the public on matters of public interest must be disclosed as such. Providers of generative AI systems must mark synthetic outputs in a machine-readable format. Generative systems placed on the market before 2 August 2026 have until 2 December 2026 to meet the marking and detection requirements.

Penalties for breach of the transparency obligations reach EUR 15 million or 3% of total worldwide annual turnover, whichever is higher. Penalties for engaging in a prohibited AI practice reach EUR 35 million or 7% of worldwide turnover.

Affects Tools 1, 6, 7, 8 and 10. Tool 6 (Surveillance and Monitoring) is the most directly engaged: this is the first hard, enforceable European obligation bearing on the surveillance technologies most commonly deployed in private security.

> **Source:** *European Commission, "Commission starts enforcing AI Act rules and new transparency requirements on 2 August", 31 July 2026; "Enforcement framework of the AI Act", updated 24 August 2026; "Quick facts: transparency rules for AI systems", 29 July 2026. https://digital-strategy.ec.europa.eu/en/policies/enforcement-ai-act*

2. The high-risk obligations have been postponed to December 2027

Regulation (EU) 2026/1744, the Digital Omnibus on AI, was adopted on 8 July 2026 and entered into force on 27 July 2026. It defers the obligations for standalone high-risk AI systems listed in Annex III of the EU AI Act from 2 August 2026 to 2 December 2027. High-risk AI embedded in regulated products under Annex I moves from 2 August 2027 to 2 August 2028.

This is a correction of substance for the Toolkit. Annex III covers most of the AI applications relevant to private security: remote biometric identification, biometric categorisation, emotion inference, AI used in recruitment and worker management, and AI used in the protection of critical infrastructure. Where a v1.1 tool document states that high-risk duties — risk management systems, data governance, logging, human oversight, fundamental rights impact assessment, conformity assessment — apply from August 2026, that statement is no longer correct.

Companies should treat the period to 2 December 2027 as a preparation window rather than a compliance holiday. Two things are unaffected by the postponement and are enforceable now: the prohibited practices in Article 5, and the Article 50 transparency duties described in section 1 above.

> **Source:** *Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 (Digital Omnibus on AI), in force 27 July 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202601744 · European Commission, guidelines on high-risk AI systems. https://digital-strategy.ec.europa.eu/en/policies/guidelines-ai-high-risk-systems*

3. Which authority supervises which deployment

The enforcement architecture of the EU AI Act became operational on 2 August 2026 and can now be stated with certainty.

- The AI Office within the European Commission supervises providers of general-purpose AI models, and AI systems built on general-purpose models by the same provider.
- National market surveillance authorities supervise all other AI systems in their member state. A private security company deploying AI is almost always a deployer, and therefore answers to the market surveillance authority of the country in which it operates — not to the AI Office.
- The European Data Protection Supervisor supervises the use of AI by EU institutions, bodies and agencies.

The Commission may also enforce directly against prohibited AI practices, which include manipulation, exploitation of vulnerabilities, and predictive policing that assesses the risk of an individual committing an offence on the basis of profiling alone. The last of these bears directly on any risk-scoring or threat-prediction service offered by a private security company in relation to identified individuals.

Affects Tool 9 (Accountability and Transparency), which in v1.1 could not name a competent enforcer, and Tools 1, 6 and 7.

Source: *European Commission, "The enforcement framework of the AI Act", updated 24 August 2026. https://digital-strategy.ec.europa.eu/en/policies/enforcement-ai-act*

4. Developments to watch — not yet obligations

The following are confirmed developments that do not yet change what companies must do, but are expected to affect the Toolkit's guidance.

- The United Nations Working Group on the use of mercenaries is preparing a thematic report on the use of technology by mercenaries, mercenary-related actors and private military and security companies, for presentation to the Human Rights Council at its 63rd session (7 September to 7 October 2026). It examines AI and machine learning, biometric and behavioural surveillance, commercial satellite and geospatial intelligence, cyber intrusion capabilities, cloud services and data brokerage, synthetic media, drones, and crypto-asset financing. It is expected to become the authoritative United Nations reference on private security technology use.
- The European Data Protection Board adopted draft guidelines on anonymisation and on web scraping for generative AI on 8 July 2026, open for public consultation until 30 October 2026. The three-part anonymisation test — no singling out, no linkability, no inference — will bear on what a security company may treat as anonymised footage or logs.
- The International Labour Organization adopted the Decent Work in the Platform Economy Convention, 2026 (No. 193) in June 2026 — the first global standard addressing algorithmic management and workers' personal data. No ratifications are confirmed to date.
- The Corporate Sustainability Due Diligence Directive, as amended by Omnibus I, must be transposed by member states by 26 July 2028 and applies to in-scope companies from 26 July 2029 — a single application date replacing the staggered timeline in the original directive. Scope is now EU companies with more than 5,000 employees and net worldwide turnover above EUR 1.5 billion, and non-EU companies with more than EUR 1.5 billion of turnover generated in the EU. First reporting covers financial years beginning on or after 1 January 2030. Affects Tools 9 and 12.
- The EU Platform Work Directive (EU) 2024/2831 must be transposed by member states by 2 December 2026, covering transparency of automated monitoring and decision-making, restrictions on processing workers' personal data, and human oversight of algorithmic decisions.

Maintenance

This addendum is updated monthly from the Toolkit's regulatory monitoring briefings, and its contents are folded into the tool documents at each quarterly content review. Version 1.1, 2 September 2026 — revised the same day to distinguish the CSDDD transposition deadline (member states, 26 July 2028) from the date the obligations apply to companies (26 July 2029). Next review: December 2026.