

The EU AI Act and Israeli Tech Companies



A Rights-Based Compliance Framework

Gadi Perl

AI Regulation Advisory · Research Fellow, Hebrew University Faculty of Law

CRITICAL DEADLINE
August 2, 2026

KEY FIGURES

<p>7%</p> <p>of global annual turnover — maximum fine for prohibited AI practices</p>	<p>€35M</p> <p>absolute cap on fines, exceeding GDPR's maximum penalties</p>	<p>< 4 months</p> <p>until August 2026 full enforcement of high-risk AI obligations</p>
--	---	---

CORE ARGUMENT

THE ETHICS-WASHING RISK

Publishing an AI ethics policy or algorithmic impact statement does not satisfy the AI Act's obligations. The Act requires technically grounded, auditable compliance across the entire system lifecycle — from data governance through post-market monitoring. Regulators will look past performative transparency.

SIX THINGS ISRAELI COMPANIES MUST DO NOW

<p>1. Establish extraterritorial exposure</p> <p>If your AI output is used in the EU — by any customer, partner, or end-user — you are in scope regardless of where your company is based.</p>	<p>2. Build a lifecycle compliance map</p> <p>Compliance begins at purpose definition, not documentation. Risk assessment, data governance, and oversight mechanisms must span all stages from training to post-deployment monitoring.</p>
<p>3. Classify all AI systems by risk tier</p> <p>HR tools, credit scoring, healthcare AI, and biometrics are high-risk. Where classification is uncertain, default to high-risk — under-classification triggers the same penalties as non-compliance.</p>	<p>4. Implement layered transparency</p> <p>Traceability for auditors, verifiability for courts, intelligibility for affected individuals, and communication obligations for end users are distinct requirements — each directed at a different actor.</p>
<p>5. Appoint an EU Authorised Representative</p> <p>Providers of high-risk AI systems without EU presence must mandate an Authorised Representative in the EU before deployment. This is a legal prerequisite, not a formality.</p>	<p>6. Learn from the GDPR experience</p> <p>Israel's delayed adaptation to GDPR created years of market friction. The same risk applies to the AI Act. Compliance infrastructure cannot be built overnight — preparation time is now.</p>

COMPLIANCE TIMELINE

Feb 2025	Already in force: prohibited AI practices banned; AI literacy obligations active. Audit your full product portfolio now.
Aug 2025	Already active: GPAI obligations and penalty regime. Foundation model providers must

	comply. Fines may now be imposed.
Aug 2026	CRITICAL DEADLINE: full enforcement of Annex III high-risk obligations — hiring, credit, healthcare, biometrics. Less than 4 months away.
Aug 2027	Full scope including AI embedded in regulated products. Post-deployment monitoring obligations continue indefinitely.

TOPICS COVERED IN THIS PAPER

Extraterritorial scope · Risk classification framework · Lifecycle compliance · Algorithmic transparency layers · Data governance obligations · Human oversight requirements · GPAI model obligations · Intersection with GDPR & Israeli PPL · Penalty structure · Compliance roadmap · Ethics-washing risks · Strategic positioning

Gadi Perl · AI Regulation Advisory · Hebrew University Faculty of Law · Federmann Cybersecurity Research Center
gadi@gadiperl.com