jaconsulting.pro
john@jaconsulting.pro

The EU AI Act Applies to You. Here’s What That Means.

Johnathan Aloni, Adv. | *Strategic Legal Advisor* | *Dublin / EU*

The EU AI Act is in force and its obligations are being phased in over time. If your company develops, places on the market, deploys, or uses AI systems in the European market, this regulation applies to you, regardless of whether your company is based in Europe, the US, or Asia.

Many businesses fall into one of two categories: those who believe the Act does not apply to them, and those who know it probably does but have not yet done anything about it. Both groups are taking on risk they do not need to take.

What the EU AI Act Actually Does

The EU AI Act introduces a structured risk framework for artificial intelligence systems. Where your product or system sits in that framework determines your legal obligations.

Risk Level	Description	Key Obligations
Prohibited	Banned outright	Biometric surveillance, manipulative systems, social scoring
High-Risk	Most demanding obligations	Conformity assessments, documentation, human oversight, EU database registration
Limited-Risk	Lighter requirements	Transparency obligations
Minimal-Risk	Standard operations	Voluntary codes of conduct
GPAI Models	Foundation models	Documentation, transparency, risk management

Actual classification depends on the specific functionality, intended purpose, and context of use.

A Simple Test

If you are unsure whether the EU AI Act affects your company, ask yourself three questions:

- Does your product use AI to evaluate people in a way that affects opportunities, employment, credit, education, or access to services?
- Does your AI system influence decisions made by organisations in regulated sectors such as finance, healthcare, insurance, or education?
- Could a customer reasonably rely on your AI system when making a decision that materially affects another person?

If the answer to any of these questions is YES, there is a meaningful chance your system falls into the high-risk category. At that point, guessing is no longer a strategy.

The first practical step is usually a structured classification analysis, not a full compliance programme.

The Three Mistakes Companies Are Making Right Now

Mistake 1: Treating the Deadline Picture as Settled

The European Parliament formally approved the Digital Omnibus on 15 June 2026 (423 votes in favour). The new deadlines for high-risk AI are effectively confirmed, pending Council formal adoption and Official Journal publication. What is certain for August 2026 is the Article 50 transparency layer, which did not move.

Date	What Applies
2 February 2025	Prohibited practices banned. AI literacy obligations in force.
2 August 2025	GPAI model obligations apply. Penalty regime in force. Fines of up to EUR 35 million or 7% of global turnover for prohibited practices now enforceable.

2 August 2026	Article 50 transparency obligations apply: chatbot and AI interaction disclosure, AI-generated content marking, emotion recognition disclosure, and deep fake labelling.
2 December 2026	Watermarking obligations (Article 50(2)) for AI systems already on the market before August 2026.
2 December 2027	High-risk AI standalone systems (Annex III). Subject to Council formal adoption and Official Journal publication. European Parliament approved 15 June 2026.
2 August 2028	High-risk AI embedded in regulated products (medical devices, transport safety systems). Subject to Council formal adoption and Official Journal publication. European Parliament approved 15 June 2026.

Mistake 2: Treating This as a Legal Problem Rather Than a Business Problem

AI Act compliance is not just about avoiding fines. It is increasingly about market access, investor confidence, and enterprise procurement. Sophisticated investors are already asking about AI governance during due diligence. Businesses who treat compliance purely as a cost are missing the commercial opportunity.

Mistake 3: Misclassifying Their AI System

Risk classification is not always straightforward. AI systems used for CV screening and recruitment decisions are commonly treated as high-risk under the AI Act. Credit decision tools with AI scoring fall in the same category. Even systems that appear benign can become high-risk depending on how they are used. Many companies discover this only when a large enterprise customer asks for their AI Act compliance documentation.

What Practical Readiness Looks Like

You do not need a fully built compliance framework today. You do need to understand where your company stands and have a credible plan.

- Maintain an internal inventory of AI systems used or developed by the company.
- Conduct a written classification analysis.
- Establish basic governance documentation including internal policies and oversight mechanisms.
- Understand your role in the AI value chain: provider, deployer, importer, or distributor.
- Ensure contracts with AI vendors and customers reflect relevant AI and privacy regulatory obligations.
- Assess your Article 50 transparency exposure for August 2026 regardless of the Omnibus outcome.

None of this requires a large compliance department. It requires clear thinking, the right legal framework, and a realistic understanding of how regulation interacts with product development and commercial strategy.

The Strategic Reality Most Businesses Are Missing

Many businesses outside Europe assume the EU AI Act is mainly a problem for European companies. That assumption is wrong.

European customers and procurement teams are increasingly requiring AI vendors to demonstrate regulatory readiness before entering into contracts. In practice, the Act functions as a market gatekeeper, not just a regulatory framework.

Companies that can clearly explain their AI governance and risk classification will move through procurement processes faster. Companies that cannot will struggle to sell into the European market, regardless of where they are headquartered.

For leaders and executives operating in or selling to the European market, the relevant question is no longer whether the AI Act applies. The question is whether your company understands where it sits in the framework and what that means for product design, contracts, governance, and growth strategy.

The classification analysis is the starting point. Everything else follows from it.