



FROM THE IUSTORIA BLOG

AI Act: What Czech Companies Need to Know About Using Artificial Intelligence

The EU AI Act doesn't just apply to developers — it covers businesses that merely deploy AI. A practical guide.

MGR. GABRIEL KOŽÍK

14 August 2025 · 6 min read

Regulation (EU) 2024/1689 of the European Parliament and of the Council — widely known as the AI Act — entered into force on 1 August 2024. Obligations are being phased in: the first set applied from February 2025, the next from August 2025, and the full regime takes effect in August 2026. Yet the majority of Czech businesses have not determined whether the regulation applies to them at all.

The reason is straightforward: a widespread assumption that the AI Act only regulates those who develop artificial intelligence. That assumption is wrong. The regulation also covers so-called deployers — businesses that merely use AI systems in the course of their professional activity.

Provider versus deployer

The AI Act distinguishes two primary roles. A provider is an entity that develops an AI system (or has it developed) and places it on the market under its own name. A deployer is an entity that uses an AI system within its professional capacity.

If your company uses an AI tool to evaluate employees, score clients, automate credit decisions, or screen CVs — you are a deployer. And you have obligations.

Critically, these roles can overlap. A company that takes an open-source model, fine-tunes it on proprietary data, and deploys it internally may become a provider — even if the original intent was simply to "use" AI.

Risk classification: where your system falls

The AI Act operates on a four-tier risk framework.

Prohibited practices are AI systems that must not exist at all — social scoring of citizens, manipulative techniques exploiting vulnerabilities, real-time biometric identification in public spaces (with narrow exceptions for law enforcement). These prohibitions apply from February 2025.

High risk encompasses AI systems used in areas where an incorrect decision significantly impacts a person. This includes, among others: recruitment and employee evaluation, creditworthiness assessment, access to education, critical infrastructure, and medical devices. High-risk systems face the strictest obligations — risk management, documentation, human oversight, and transparency requirements.

Limited risk applies to systems that interact with people (chatbots, content generators). The primary obligation is transparency — users must know they are communicating with AI or that content was AI-generated.

Minimal risk covers most common AI applications — spam filters, e-commerce recommendation engines, logistics optimisation. The AI Act imposes no specific obligations here, though it encourages voluntary codes of conduct.

A practical checklist: what to do now

Based on our advisory practice, we recommend five concrete steps.

First: map the AI systems in your organisation. Most companies have no idea how many AI tools they actually use. This goes beyond in-house development — think SaaS tools, cloud services, analytical platforms. Create an inventory: what each system is, who supplies it, what it does, and what data it processes.

Second: classify the risk. For every system in your inventory, determine which category it falls into. If you are uncertain, assume the higher category — the consequences of underestimation outweigh the costs of overestimation.

Third: appoint a responsible person. The AI Act does not explicitly require an "AI compliance officer," but someone in the organisation must have oversight of which AI systems are in use and what obligations follow. In smaller firms, this can be the existing compliance manager or in-house counsel.

Fourth: prepare documentation. For high-risk systems, the AI Act requires extensive technical documentation, operational logs, and fundamental rights impact assessments. But even for lower-risk systems, it makes sense to document why and how AI is deployed — at minimum for potential audits or disputes.

Fifth: establish human oversight. For high-risk systems, meaningful human oversight must be in place — a genuine ability for a person to intervene in the AI's decision-making process. Automated decisions that cannot be reviewed are problematic not only under the AI Act but also under the GDPR.

Why the AI Act is an opportunity

I hear the objection often: the AI Act is yet another regulatory burden. In a sense, that is true. But consider the other side.

A company that has mapped its AI systems, understands their risks, and maintains proper documentation is a company that understands its own operations. In practice, we find that the process of preparing for the AI Act reveals inefficiencies, redundancies, and risks that management was unaware of.

Furthermore — and this argument resonates with internationally minded businesses — AI Act compliance is becoming a competitive advantage. The parallel with GDPR is instructive: companies that took it seriously from day one are not scrambling today. Those that waited are still dealing with the consequences.

The AI Act follows a similar trajectory. Obligations are arriving gradually, but they are arriving. A company that prepares now will be ahead of those that start addressing the AI Act only after the first regulatory inspection.

The AI Act is not regulation about artificial intelligence in the abstract. It is regulation about how businesses use technologies that make decisions about people. That concerns most companies — they simply do not know it yet.

If you are unsure whether or how the AI Act applies to your business, get in touch. An AI systems audit takes days, not months — and the cost of ignoring the regulation can be disproportionately higher. If your AI Act work touches supplier contracts, see also [Contract mistakes — five errors we see most often](#) — many obligations end up in processor clauses and works-and-services agreements.

Using AI tools in your business and need to know whether and how the AI Act applies? In our [risk prevention practice](#) we audit your AI systems and design a precise roadmap to August 2026. [Get in touch](#).

AI Act: What Czech Companies Need to Know About Using Artificial Intelligence

Mgr. Gabriel Kožík · Published 14 August 2025

<https://www.iustoria.cz/en/blog/ai-act-what-czech-companies-need-to-know/>

This text is protected by copyright. Sharing the document whole and unaltered is welcome; reuse of parts in other texts requires attribution. © IUSTORIA, advokátní kancelář, s.r.o.