



Z BLOGU IUSTORIA

AI Act: co musí vědět česká firma, která používá umělou inteligenci

*EU AI Act se netýká jen vývojářů — dopadá i na firmy, které AI pouze nasa-
zují. Praktický průvodce povinnostmi.*

Nařízení Evropského parlamentu a Rady (EU) 2024/1689, známé jako AI Act, vstoupilo v platnost 1. srpna 2024. Povinnosti se zavádějí postupně — první sada od února 2025, další od srpna 2025 a plný režim od srpna 2026. Přesto většina českých firem dosud nezjistila, zda se jich vůbec týká.

Důvod je prostý: převládá představa, že AI Act reguluje pouze ty, kdo umělou inteligenci vyvíjejí. To je omyl. Nařízení se vztahuje i na tzv. nasazovatele (deployers) — tedy firmy, které AI systémy pouze používají.

Poskytovatel versus nasazovatel

AI Act rozlišuje dvě hlavní role. Poskytovatel (provider) je ten, kdo AI systém vyvíjí nebo nechá vyvinout a uvádí jej na trh pod svým jménem. Nasazovatel (deployer) je ten, kdo AI systém používá v rámci své profesní činnosti.

Pokud vaše firma používá AI nástroj pro hodnocení zaměstnanců, scoring klientů, automatizované rozhodování o úvěrech nebo třídění životopisů — jste nasazovatel. A máte povinnosti.

Důležité je pochopit, že tyto role se mohou překrývat. Firma, která vezme open-source model, dotreneuje jej na vlastních datech a nasadí interně, se může stát poskytovatelem — i když původně chtěla AI jen „používat“.

Klasifikace rizik: kam spadá váš systém

AI Act pracuje se čtyřstupňovou klasifikací rizik.

Zakázané praktiky jsou AI systémy, které nesmí existovat vůbec — sociální scoring občanů, manipulativní techniky zneužívající zranitelnost osob, biometrická identifikace v reálném čase na veřejných prostranstvích (s výjimkami pro orgány činné v trestním řízení). Zákazy platí od února 2025.

Vysoké riziko zahrnuje AI systémy používané v oblastech, kde chybné rozhodnutí má zásadní dopad na člověka. Patří sem mimo jiné: nábor a hodnocení zaměstnanců, posuzování úvěruschopnosti, přístup ke vzdělávání, kritická infrastruktura, zdravotnické prostředky. Pro vysokorizikové systémy platí nejprísnější povinnosti — včetně řízení rizik, dokumentace, lidského dohledu a transparentnosti.

Omezené riziko se týká systémů, které interagují s lidmi (chatboty, generátory obsahu). Hlavní povinností je transparentnost — uživatel musí vědět, že komunikuje s AI nebo že obsah byl AI vygenerován.

Minimální riziko zahrnuje většinu běžných AI aplikací — spamové filtry, doporučovací algoritmy v e-shopech, optimalizace logistiky. Zde AI Act neukládá specifické povinnosti, ale doporučuje dobrovolné kodexy chování.

Praktický kontrolní seznam: co udělat teď

Na základě naší praxe doporučujeme firmám pět konkrétních kroků.

Za prvé: zmapujte AI systémy ve firmě. Většina firem netuší, kolik AI nástrojů skutečně používá. Nejde jen o vlastní vývoj — jde o SaaS nástroje, cloudové služby, analytické platformy. Vytvořte inventář: co to je, kdo to dodává, k čemu to slouží, jaká data zpracovává.

Za druhé: klasifikujte riziko. Pro každý systém z inventáře určete, do které kategorie spadá. Pokud si nejste jistí, předpokládejte vyšší kategorii — důsledky podhodnocení jsou horší než náklady na nadhodnocení.

Za třetí: jmenujte odpovědnou osobu. AI Act výslovně nevyžaduje „AI compliance officera“, ale někdo ve firmě musí mít přehled o tom, jaké AI systémy firma používá a jaké povinnosti z toho plynou. V menších firmách to může být stávající compliance manažer nebo právník.

Za čtvrté: připravte dokumentaci. Pro vysokorizikové systémy vyžaduje AI Act rozsáhlou technickou dokumentaci, záznamy o fungování systému a hodnocení dopadu na základní práva. Ale i pro systémy s nižším rizikem má smysl dokumentovat, proč a jak je AI nasazena — minimálně pro případ kontroly nebo sporu.

Za páté: nastavte lidský dohled. U vysokorizikových systémů musí být zajištěn lidský dohled — tedy reálná možnost člověka zasáhnout do rozhodovacího procesu AI. Automatizované rozhodnutí, které nelze přezkoumat, je problém nejen z pohledu AI Act, ale i z pohledu GDPR.

Proč je AI Act příležitost

Rád slyším námitku, že AI Act je další regulatorní zátěž. V určitém smyslu ano. Ale podívejme se na to z druhé strany.

Firma, která má zmapované AI systémy, rozumí jejich rizikům a má dokumentaci, je firma, která rozumí svému vlastnímu fungování. V praxi vidíme, že proces přípravy na AI Act odhaluje neefektivitu, duplikace a rizika, o kterých management nevěděl.

Navíc — a to je argument, který rezonuje u firem s mezinárodními ambicemi — compliance s AI Act se stane konkurenční výhodou. Podobně jako GDPR: firmy, které ho vzaly vážně od začátku, dnes neřeší panické přizpůsobování. Ty, které čekaly, řeší problémy dosud.

AI Act má podobnou trajektorii. Povinnosti přicházejí postupně, ale přijdou. Firma, která se připraví nyní, bude mít v srpnu 2026 náskok před těmi, které začnou řešit AI Act až po první kontrole.

AI Act není regulace o umělé inteligenci v abstraktním smyslu. Je to regulace o tom, jak firmy používají technologie, které rozhodují o lidech. A to se týká většiny firem — jen o tom zatím nevědí.

Pokud si nejste jistí, zda a jak se AI Act vztahuje na vaši firmu, ozvěte se. Audit AI systémů je otázka dnů, nikoli měsíců — a důsledky ignorování nařízení mohou být nesrovnatelně nákladnější. Pokud AI Act řešíte ve spojení se smlouvami s dodavateli, podívejte se i na **Na co si dát pozor ve smlouvě** — řada povinností se propisuje do zpracovatelských doložek a smluv o dílo.

Používáte ve firmě AI nástroje a potřebujete vědět, zda a jak se na vás AI Act vztahuje? V **prevenci rizik udeláme audit vašich AI systémů a navrhne přesný roadmap do srpna 2026. **Napište nám.****

AI Act: co musí vědět česká firma, která používá umělou inteligenci

Mgr. Gabriel Kožík · Publikováno 14. 8. 2025

<https://www.iustoria.cz/blog/ai-act-co-musi-vedet-ceska-firma/>

Text je dílem chráněným autorským právem. Sdílení celého dokumentu bez úprav je vítáno; přebírání částí do jiných textů jen s uvedením zdroje. © IUSTORIA, advokátní kancelář, s.r.o.