AI ACT (NAŘÍZENÍ (EU) 2024/1689) · KATEGORIZACE RIZIK

Čtyři úrovně rizika AI a co z nich plyne pro firmu, která AI používá

AIscale

AI Act netřídí nástroje, ale konkrétní použití AI: stejný nástroj může být na e-maily v jedné úrovni a na hodnocení uchazečů v jiné. Tabulka je psaná pro zavádějící subjekt (firma, úřad, škola, která AI používá); poskytovatelé mají povinností výrazně víc.

ÚROVEŇ	CO TAM PATŘÍ	CO MUSÍ FIRMA, KTERÁ AI POUŽÍVÁ	OD KDY	PODROBNOSTI
Nepřijatelné riziko zakázané praktiky, čl. 5	Devět zakázaných postupů: manipulace a klamání, zneužívání zranitelnosti, sociální bodování, předvídání trestné činnosti z profilu, necílené stahování tváří, rozpoznávání emocí na pracovišti a ve škole, biometrická kategorizace podle citlivých znaků, biometrická identifikace v reálném čase pro policii, tvorba nekonsensuálního intimního obsahu.	**Nepoužívat.** Zákaz platí i pro firmu, která si nástroj jen předplatila. Prověřit HR, call-centrové a kamerové nástroje (funkce emotion, sentiment, engagement, stress) a výsledek zapsat. Pokuta až 35 mil. EUR nebo 7 % obratu.	2. 2. 2025 doplněné položky 2. 12. 2026	aiscale.cz/ai-act/zakazane-praktiky/
Vysoké riziko čl. 6, přílohy I a III	Oblasti přílohy III: zaměstnanost a řízení pracovníků (např. třídění životopisů), přístup k základním službám (např. úvěrové hodnocení), vzdělávání (např. bodování zkoušek), biometrie, kritická infrastruktura, prosazování práva, migrace, justice. A AI jako bezpečnostní součást výrobků (příloha I).	**Povinnosti podle čl. 26:** používat podle pokynů poskytovatele, lidský dohled, hlídat vstupní data, logy alespoň 6 měsíců, informovat zaměstnance a dotčené osoby, hlásit incidenty. Chtít od dodavatele písemné zařazení systému.	2. 12. 2027 (příloha III) 2. 8. 2028 (příloha I)	aiscale.cz/ai-act/vysoce-rizikove-systemy/
Riziko transparentnosti čl. 50	Chatboti, generativní AI, deepfakes (fotorealistická AI tvář, hlas, video) a AI text zveřejňovaný k informování veřejnosti o věcech veřejného zájmu.	**Chatbot dá najevo, že je AI.** Deepfake se viditelně označí. AI text o věcech veřejného zájmu se označí, pokud neprošel redakční kontrolou člověka. Běžný marketingový text, popis produktu ani interní dokument se neoznačují.	2. 8. 2026	aiscale.cz/ai-act/oznacovani-ai-obsahu/
Minimální nebo žádné riziko	Převážná většina AI systémů, které se dnes v EU používají, např. spamové filtry nebo videohry s AI. Běžné použití ChatGPT, Copilotu či překladače na texty, e-maily a analýzy.	**AI Act žádná zvláštní pravidla nezavádí.** Zůstává průřezová povinnost přijímat opatření k AI gramotnosti (čl. 4) a vědět, jaké nástroje a k čemu používáte (registr AI nástrojů).	čl. 4 od 2. 2. 2025	aiscale.cz/ai-act/registr-ai-nastroju/
Mimo úrovně: obecné modely AI (GPAI)	Modely, na kterých stojí ChatGPT, Gemini, Copilot a další nástroje. Pravidla míří na jejich poskytovatele: transparentnost, autorské právo, u modelů se systémovým rizikem posouzení a zmírnění rizik.	**Přímo nic.** Nepřímo: dodavatel musí mít dokumentaci, kterou po něm můžete chtít. Kdo si nad obecným modelem postaví vlastní vysoce rizikový nástroj, stává se poskytovatelem (čl. 25).	2. 8. 2025	aiscale.cz/ai-act/terminy/

Jak zařadit nástroj, který používáte: 1. Dělá něco ze zakázaných praktik? → nepřijatelné · 2. Rozhoduje o lidech v oblasti přílohy III (nábor, hodnocení zaměstnanců, úvěry, pojištění, vzdělávání, biometrie)? → vysoké · 3. Komunikuje s lidmi nebo tvoří obsah, který zveřejňujete? → transparentnost · 4. Nic z toho → minimální. Vždy: AI gramotnost (čl. 4) a záznam v registru; kategorie se odvíjí od účelu, ne od nástroje.