BEZPEČNOST AI VE FIRMĚ · CHECKLIST

AI v bezpečnostních opatřeních: 12 bodů pro povinné osoby

Pro poskytovatele regulované služby podle zákona č. 264/2025 Sb. o kybernetické bezpečnosti (NIS2), režim nižších povinností a vyhláška č. 410/2025 Sb. Ve vyšším režimu platí také, s přísnějšími požadavky vyhlášky č. 409/2025 Sb.

Zákon ani vyhlášky o bezpečnostních opatřeních umělou inteligenci nezmiňují. AI nástroje (ChatGPT, Copilot, AI v CRM, agenti) proto spadají pod stejná opatření jako jiné IT služby a dodavatelé. Odkazy v závorce jsou na zákon č. 264/2025 Sb., není-li uvedeno jinak; „písm." znamená § 14 odst. 2. Zaškrtněte, co platí.

A. EVIDENCE, RIZIKA A VEDENÍ

1. ☐ **Evidence aktiv:** jsou AI nástroje v evidenci, včetně AI funkcí ve službách, které už používáte? (§ 14 odst. 2 písm. c)
2. ☐ **Rizika:** jsou rizika AI (vložení citlivých dat, nadměrná oprávnění, prompt injection, nedostupnost služby) v hodnocení rizik? (písm. d)
3. ☐ **Vedení:** ví vrcholné vedení, které AI nástroje se používají, a je to součástí informace o stavu plnění opatření? (vyhl. 410/2025, § 4)

B. DODAVATELÉ

4. ☐ **Výběr dodavatele:** zohledňuje výběr hrozby, zranitelnosti a kvalitu bezpečnostních postupů dodavatele AI? (vyhl. 410/2025, § 3 odst. 5)
5. ☐ **Smlouva:** obsahuje požadavky bezpečnostních opatření, zejména oprávnění užívat data, řetězení dodavatelů a exit strategii? (§ 13 odst. 5; vyhl. příl. č. 2)
6. ☐ **Varování NÚKIB:** je ověřeno, že se na žádný používaný nástroj nevztahuje varování NÚKIB (např. DeepSeek, 10. 7. 2025)? (§ 72 odst. 3)

C. PŘÍSTUPY A LIDÉ

7. ☐ **Identity:** používají se AI nástroje jen s firemními účty ve správě identit a přístup se při odchodu odebírá? (písm. h)
8. ☐ **Oprávnění:** mají AI asistenti a agenti jen nezbytná oprávnění a je zkontrolované, k jakým datům se dostanou? (písm. g)
9. ☐ **Vzdělávání:** zahrnuje vzdělávání zaměstnanců a vedení práci s AI a cloudovými službami? (písm. e; vyhl. příl. č. 3)

D. PROVOZ A INCIDENTY

10. ☐ **Záznamy:** zaznamenávají se, kde to jde, události z AI nástrojů a agentů a je určeno, kdo je kontroluje? (písm. i)
11. ☐ **Incidenty:** pokrývá postup řešení incidentů i AI incidenty a prvotní hlášení NÚKIB do 24 hodin? (písm. j; § 16)
12. ☐ **Kontinuita:** je jasné, jak fungovat, když AI služba vypadne nebo ji musíte vypnout? (písm. f)

Kde začít: pokud u bodů 1 a 5 odpovíte „ne", začněte jimi. Bez evidence AI nástrojů a smluv s dodavateli se zbytek nedá doložit.

Zdroj: aiscale.cz/bezpecnost-ai/ai-a-nis2/ · Vychází ze zákona č. 264/2025 Sb. a vyhlášek č. 408, 409 a 410/2025 Sb. (zakonyprolidi.cz), stav 6. 11. 2026

Verze listopad 2026 · informativní materiál, nejde o právní poradenství