BEZPEČNOST AI VE FIRMĚ · CHECKLIST

Bezpečnostní minimum pro AI ve firmě: 8 bodů

Pro firmu, která AI používá a nevyvíjí. Osm opatření, která pokryjí většinu rizik: únik dat, osobní účty, přístupová práva, prompt injection, AI agenty, chybné výstupy a dodavatele.

Zaškrtněte, co už máte. U každého bodu je napsáno, které riziko řeší a čím to doložíte. Co nemáte, zapište s termínem a odpovědnou osobou.

A. PŘEHLED A SMLOUVY

1. ☐ **Seznam používaných AI nástrojů** s dodavatelem a typem účtu (firemní, nebo osobní).
   Řeší: osobní účty a nástroje, o kterých firma neví. Doklad: registr AI nástrojů s datem poslední revize.

2. ☐ **Firemní verze** tam, kde se pracuje s daty zákazníků nebo zaměstnanců, se zpracovatelskou smlouvou.
   Řeší: únik dat bez právního rámce. Doklad: zpracovatelská smlouva (DPA) založená u každého takového nástroje.

3. ☐ **Pravidlo pro data**: co do AI smí, co jen do firemní verze a co nikdy.
   Řeší: únik dat přes vstupy. Doklad: semafor dat ve směrnici pro používání AI, lidé ho znají.

B. PŘÍSTUPY A OPRÁVNĚNÍ

4. ☐ **Přihlašování firemním účtem** s vícefaktorovým ověřením a zrušení přístupu při odchodu zaměstnance.
   Řeší: zneužití účtů a odchod dat s člověkem. Doklad: postup při nástupu a odchodu (checklist IT).

5. ☐ **Revize sdílení** dokumentů před nasazením AI asistenta napojeného na firemní data.
   Řeší: AI vidí víc, než by měla. Doklad: záznam o kontrole sdílení s celou firmou, seznam citlivých webů a týmů.

6. ☐ **Omezená oprávnění a lidské schválení** u agentů a automatizací, které mohou jednat.
   Řeší: prompt injection a příliš velká oprávnění agentů. Doklad: seznam agentů s rozsahem oprávnění a kroky, které vyžadují schválení člověkem.

C. VÝSTUPY A INCIDENTY

7. ☐ **Kontrola výstupů** před tím, než jdou ven nebo do systémů.
   Řeší: chybné výstupy a slepá důvěra. Doklad: pravidlo „kdo AI výstup posílá, ručí za něj“ ve směrnici, checklist revize.

8. ☐ **Postup při incidentu**: komu hlásit, že se něco nepovedlo, a jak rychle. U osobních údajů běží lhůta 72 hodin pro ohlášení ÚOOÚ.
   Řeší: pozdní reakce na únik. Doklad: jednostránkový postup a vzor záznamu o incidentu.

Stop pravidlo: pokud u bodů 2 a 3 odpovíte „ne“ a lidé pracují s daty zákazníků, řešte je jako první. Zbytek počká, únik dat ne.

Souvislost s AI Actem: body 3, 7 a školení k nim jsou zároveň opatřeními k AI gramotnosti podle čl. 4 nařízení (EU) 2024/1689. Kdo zavede a zdokumentuje bezpečnostní minimum, má velkou část souladu hotovou.

Zdroj: aiscale.cz/bezpecnost-ai/rizika-ai-ve-firme/ · Vychází z OWASP Top 10 for LLM Applications 2025, dokumentace Microsoft Learn a varování NÚKIB, stav 6. 11. 2026

Verze listopad 2026 · informativní materiál, nejde o právní poradenství