CO NIKDY NEVKLÁDAT DO AI

Základní pravidlo

Do žádného externího AI nástroje nevkládejte údaje, nad kterými byste po odeslání ztratili kontrolu. Platí to pro bezplatné i placené verze — u neplacených verzí bývá běžné, že poskytovatel může vložené údaje využít k tréninku svých modelů, ale ani placená verze tuto možnost nemusí automaticky vylučovat.

Kontrolní seznam "Nevložil jsem do AI"

☐ **Osobní údaje**

např. jména, adresy, rodná čísla, čísla dokladů, e-mailové adresy občanů i zaměstnanců.

☐ **Citlivé údaje**

např. zdravotní stav, trestní záznamy, politická příslušnost, etnický původ, biometrické údaje.

☐ **Interní dokumenty**

např. rozpracované analýzy, strategické materiály, zápisy z neveřejných jednání, personální hodnocení.

☐ **Interní dokumenty**

např. dokumenty označené stupněm utajení podle zákona o ochraně utajovaných informací.

Proč je to důležité

Jakmile data opustí interní prostředí úřadu a dostanou se na servery poskytovatele AI, úřad nad nimi ztrácí faktickou kontrolu. Hrozí jejich použití k trénování modelu, únik při bezpečnostním incidentu nebo přenos do jurisdikce mimo EU. Každý takový případ představuje potenciální porušení GDPR s rizikem sankce od ÚOOÚ.