

CHECKLIST HODNOCENÍ AI SLUŽBY

Checklist slouží k systematickému posouzení nové AI služby před jejím zavedením na úřadě. Projděte každou otázku a zaznamenejte odpověď. Služba s více než dvěma odpověďmi „Ne“ vyžaduje eskalaci na IT oddělení a DPO.

A. Bezpečnost a ochrana dat

1. Jsou data uložena a zpracovávána na území EU/EHP? Ano Ne Nejistěno
2. Jsou data šifrována při přenosu i v úložišti? Ano Ne Nejistěno
3. Poskytovatel prohlašuje, že nevyužívá vložená data pro trénování modelu? Ano Ne Nejistěno
4. Má poskytovatel certifikaci ISO 27001 nebo obdobnou? Ano Ne Nejistěno
5. Existuje definovaná doba uchovávání dat s automatickým mazáním? Ano Ne Nejistěno

B. Právní rámec

1. Nabízí poskytovatel DPA podle čl. 28 GDPR? Ano Ne Nejistěno
2. Je k dispozici seznam subprocessorů? Ano Ne Nejistěno
3. Jsou smluvní podmínky stabilní (nemění se častěji než jednou za půl roku bez upozornění)? Ano Ne Nejistěno
4. Poskytovatel má postup pro hlášení bezpečnostních incidentů? Ano Ne Nejistěno

C. Funkčnost a transparentnost

1. Je jasné, jaký model služba používá a jaké jsou jeho známé limity? Ano Ne Nejistěno
2. Poskytovatel umožňuje export nebo výmaz dat na žádost? Ano Ne Nejistěno
3. Existuje kontaktní osoba pro bezpečnostní a právní dotazy? Ano Ne Nejistěno

D. Celkové hodnocení

- Počet odpovědí „Ano“: ____
- Počet odpovědí „Ne“: ____
- Počet odpovědí „Nejistěno“: ____
- Výsledek: Nízké riziko (max. 2× Ne/Nejistěno) Vysoké riziko (3+ Ne/Nejistěno) → eskalace na IT a DPO

Aktualizace checklistu

Revidujte checklist minimálně jednou za půl roku. Sledujte změny v legislativě (AI Act, novelty GDPR), nové bezpečnostní hrozby a aktualizace podmínek poskytovatelů. Odpovědnost za aktualizaci nese IT oddělení ve spolupráci s DPO.