

STRUKTURA A OBSAH AI KODEXU

AI kodex je interní dokument, který nastavuje jednotná pravidla pro používání AI v úřadu. V praxi chrání úřad i jednotlivé zaměstnance: snižuje riziko úniku informací, nepřesných výstupů a nejasné odpovědnosti, a zároveň dává lidem jistotu, co mohou dělat bez složitého schvalování.

Kodex má být napsaný tak, aby ho koncový uživatel přečetl za 10–15 minut a hned věděl:

- jaké nástroje smí použít,
- jaká data do nich smí zadat,
- jak má kontrolovat výsledky,
- kdy má eskalovat.

Povinné části kodexu

Každý AI kodex ve veřejné správě by měl obsahovat těchto osm částí:

1. Definice a rozsah

- Co úřad považuje za generativní nástroje, asistenty a AI agenty (AI agent).
- Na koho se pravidla vztahují (zaměstnanci, externisté, dodavatelé v přístupu k systémům).

2. Zásady práce s informacemi

- Co se nesmí vkládat do AI (osobní údaje, důvěrné informace, interní dokumenty mimo schválené prostředí – podle interních směrnic).
- Zásada minimalizace: zadáváte jen to, co je nutné.
- Praktické anonymizování/pseudonymizování textů pro trénink promptu.

3. Povolené způsoby použití (typové scénáře)

- Shrnutí podkladů bez citlivých dat.
- Návrhy textů (odpovědi, pozvánky, interní sdělení) s povinným lidským schválením.
- Jazykové úpravy a zjednodušení stylu pro občany.
- Návrh struktury prezentace, podkladů pro poradů.

4. Zakázané způsoby použití

- Automatické rozhodování bez člověka tam, kde má výstup dopad na práva občanů.
- Vkládání osobních údajů do neschválených cloudových nástrojů.
- Vydávání výstupu AI za stanovisko úřadu bez ověření.



STRUKTURA A OBSAH AI KODEXU

Povinné části kodexu

5. Odpovědnosti a role

- Kdo je odpovědný za vstup (uživatel), kdo za provoz (IT), kdo za pravidla (vedení), kdo za podporu (ambasador).
- Jak funguje Eskalace a hlášení problémů (Escalation and reporting), postup kdy a komu hlásit incident.

6. Ověřování výstupů a práce s riziky

- Povinnost kontroly faktů a zdrojů (zejména kvůli halucinacím (hallucination)).
- Kontrola tónu, srozumitelnosti a přiměřenosti.
- Základní pravidla pro snížení zkreslení (bias): kontrola, zda návrh neznevýhodňuje skupiny občanů.

7. Auditovatelnost a dohledatelnost

- Co se eviduje: schválené nástroje, typové use casey, incidenty, školení.
- Kde se ukládají šablony, checklisty, reporty.

8. Schvalování a výjimky

- Jak žádat o nový nástroj / nový use case.
- Kdo může schválit výjimku a na jak dlouho.

Kodex může (a má) odkazovat na interní bezpečnostní směrnice a doporučení ÚOOÚ. Právní text v něm ale nemá převažovat nad praktickými postupy. Uživatel potřebuje návod „co udělám zítra ráno“, ne právní rozbor.

Pravidla pro práci s texty, obrázky a vizuály uveďte konkrétně:

- **U textů:** povinná kontrola jmen, čísel jednacích, termínů, odkazů na paragrafy.
- **U obrázků:** zákaz generovat nebo upravovat materiály s osobními údaji (např. fotky účastníků akce) mimo schválené prostředí.
- **U vizuálů:** jasná pravidla pro použití znaků úřadu, log a grafických manuálů (nejde-li o citaci interního manuálu, držte to na úrovni „použijte jen schválené podklady“).

