BEZPEČNĚ A ZODPOVĚDNĚ S AI

Vzdělávací cíle (Learning Objectives)

Cílem vzdělávacího kurzu je:

- Vysvětlit právní a bezpečnostní požadavky pro použití generativní umělé inteligence ve veřejné správě, včetně GDPR, role správce a zpracovatele a základních ustanovení AI Act.
- Představit jasné kategorie pravidel: co nikdy nevkládat do AI (osobní údaje, citlivé údaje, interní/utajované informace) s praktickými příklady a odůvodněním.
- Seznámit s postupy anonymizace a minimalizace dat (anonymization, pseudonymization, data minimization) a dostupnými nástroji a kroky pro jejich aplikaci.
- Popsat postupy pro vyhodnocení a výběr AI služeb z hlediska bezpečnosti, včetně kontrolních otázek pro dodavatele, kritérií rizikovosti a šablony pro DPA.
- Diskutovat principy lidské kontroly a odpovědnosti v rozhodovacích procesech a poskytnout vzory dokumentace (auditní stopa, záznam o použití AI).
- Analyzovat příklady pochybení a navrhnout nápravná opatření, včetně praktických cvičení: anonymizace ukázkového souboru a rozhodovací scénář.

Výsledky učení (Learning Outcomes)

Po absolvování kurzu bude student schopen:

- Identifikovat a vysvětlit konkrétní právní závazky (GDPR, role správce/zpracovatele, AI Act) při plánování použití generativní umělé inteligence v konkrétní agendě.
- Aplikovat postup anonymizace a minimalizace (anonymization, pseudonymization, data minimization) na ukázkovém souboru a doložit kroky do záznamu o použití AI.
- Provést hodnocení rizikovosti konkrétní AI služby podle předloženého checklistu a sestavit návrh DPA položky pro vybranou službu.
- Navrhnout a zdokumentovat rozhodovací bod pro lidskou kontrolu v daném procesu a formulovat postup dokumentace (auditní stopa, záznam o použití AI) pro spisovou službu.
- Posoudit případovou studii pochybení, identifikovat příčiny a navrhnout konkrétní nápravná opatření včetně kroků komunikace s dotčenými stranami.
- Vypracovat bezpečnostní a compliance část plánu pilotního nasazení AI v oddělení: DPA, pravidla pro data, dokumentační povinnosti, role DPO a IT.