Bezpečnost AI a její zodpovědné využití ve firemním prostředí

Kód kurzu: BPZ-AI

Jednodenní kurz seznamuje posluchače s tím, jak zvýšit povědomí zaměstnanců o rizicích a správném používání AI nástrojů, ukázat bezpečné alternativy. AI nechceme zakazovat, ale naučit se ji využívat tak, aby neohrožovala důvěrnost dat, GDPR ani reputaci firmy.

Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Osnova kurzu

- Úvod do AI – jak funguje a co od ní očekávat AI jako statistický model – proč není „vševědocí systém"
- Kvalita vstupu = kvalita výstupu (zásady správného promptování)
- Kritické čtení výstupů – nutnost ověřovat fakta i bezpečnostní obsah
- Rizika a regulační rámce Typy dat: veřejné, interní, chráněné, přísně chráněné – co do AI nikdy nevkládat
- GDPR a ochrana osobních údajů ve vztahu k AI
- Ostatní legislativa (AI ACT, SK zákon – v přípravě)
- Reálné incidenty (úniky obchodních plánů, zdrojového kódu, osobních dat)
- Dopady na právní postavení a reputaci firmy
- Morální požadavky a dopady jejich nedodržení
- Porovnání AI nástrojů z pohledu bezpečnosti Geopolitický pohled na AI nástroje (USA, EU, Čína, ...)
- ChatGPT, Perplexity, Google Gemini, Microsoft Copilot – rozdíly v ochraně dat
- Enterprise AI a jejich režim práce s daty (Microsoft, Google, OpenAI Enterprise)
- On-premise / offline AI řešení – kdy a proč je nasadit jako „plán B"
- Bezpečné používání AI v praxi AI jako zdroj úniku dat
- Kde končí data
- Co je v promptě a výstupu, může vidět kdokoli
- Minimalizace a anonymizace dat při práci s AI
- Jak správně nastavit prostředí a zanechávat minimum digitálních stop
- Co si nástroj pamatuje a jak řídit uchovávání a historii dat
- Tvorba Znalostí a Knihovnic (GPT)
- Používání pouze schválených AI nástrojů a kontrola nastavení (režim ochrany dat)
- Prompt engineering. Jak formovat prompty, jaké základní parametry, specifikace, strukturu by měly mít prompty
- Praktická cvičení: bezpečné prompty, extrakce a analýza dokumentů bez rizika úniku dat
- Efektivní používání a postupy Best practices pravidla a doporučení pro zaměstnance
- Tvorba vlastních modelů, agentů
- Správa chatů
- Vztah chatu, projektu a agenta
- Využívání Knowledge a Knihovnic
- Efektivní používání – klávesové zkratky, příklady protipů
- Znalosti, jak efektivně a bezpečně využívat AI nástroje v každodenní práci
- Řízení struktury chatů
- Týmová práce a podnikové sdílení používání AI

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk