Bezpečné užívání nástrojů AI

Doporučení vedení Univerzity Karlovy k bezpečnému užívání nástrojů generativní umělé inteligence

Vedení Univerzity Karlovy upozorňuje akademickou obec na bezpečnostní hrozby, které byly identifikovány v některých nástrojích generativní umělé inteligence. V této souvislosti nedoporučujeme nasazení a užívání nástroje DeepSeek pro pracovní a akademické účely.

Doporučujeme při užívání zejména volně, bezplatně dostupných aplikací, nejen pro služby generativní umělé inteligence, mít na paměti doporučení Národního úřadu pro kybernetickou bezpečnost (NÚKIB), více viz

Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB doporučuje obezřetnost v používání náhle populárních aplikací .

Přestože se zatím Národní úřad pro kybernetickou bezpečnost přímo nevyjádřil k užívání nástroje DeepSeek, doporučujeme celé akademické obci, aby ho pro plnění pracovních a studijních úkolů nepoužívala.

Vysoká obezřetnost platí i pro další chatboty od čínských výrobců, jako např. Qwen od Alibaba. Použití nástrojů vyvinutých a spravovaných subjekty pod jurisdikcí států s omezenou akademickou svobodou může představovat institucionální riziko v podobě potenciálního nelegitimního ovlivňování akademické činnosti.

Ohrožená jsou osobní data registrovaných uživatelů systému, o čemž svědčí i rezervovaný přístup a obezřetnost členských států vyjádřená na posledním zasedání Evropského sboru pro ochranu osobních údajů dne 11. 2. 2025. Nástroj DeepSeek by měl být podroben důkladnému přezkumu a sledován na evropské platformě zabývající se umělou inteligencí. Nelze vyloučit zneužití vložených dokumentů a vstupů včetně přihlašovacích údajů, ohroženy jsou i výsledky duševní práce výzkumnic, výzkumníků i studujících.

Doporučujeme užívání nástrojů, které mají bezpečnostní rizika smluvně i technicky ošetřena, pro nejširší užití na Univerzitě je vhodný nástroj Microsoft Copilot for Education **, dostupný všem zaměstnancům a studentům Univerzity Karlovy ve** webovém prohlížeči.

Pro pokročilé užití doporučujeme pořízení zaměstnanecké licence Microsoft 365 Copilot, které je integrováno do online aplikací (např. Excel, word, outlook, ...).

Postupně budovaný seznam doporučených a prověřených nástrojů je dostupný zde.

Pokud hodláte pro práci, výzkum nebo studium použít jiný nástroj a nejste si jistí jeho bezpečností, ozvěte se týmu pro AI do Centra pro podporu e-learningu - elearning@cuni.cz.

Vedení Univerzity Karlovy vyzývá odborníky v oblasti generativní AI ke spolupráci nejen na postupném rozšiřování tohoto seznamu zdrojů, ale i zapojení do Pracovní skupiny Generativní AI na UK.

Univerzita Karlova vítá všechny vzdělávací aktivity, které jsou pořádány rektorátem i fakultami a výzkumnými týmy a jsou zaměřeny na bezpečné a užitečné užívání nástrojů generativní AI, informace o nich se snažíme kumulovat na stránce https://ai.cuni.cz a šířit prostřednictvím speciálního newsletteru.

Pro první seznámení zaměstnanců s principy práce s nástroji generativní AI doporučujeme absolvování e-kurzu připraveného Fakultou humanitních studií Úvod do generativní AI .