

Bezpečné, etické a smysluplné využívání služeb umělé inteligence (AI) na VŠE v Praze

Anotace:

Tato směrnice s celoškolskou působností stanovuje pravidla provozu a používání služeb umělé inteligence (AI služeb) a veškerých ICT technologií zaměřených na automatizovanou práci s daty a informacemi na Vysoké škole ekonomické v Praze. Konkrétní podmínky využívání AI služeb v rámci výuky, průběžného hodnocení a kvalifikačních prací mohou být dále upraveny fakultami, garanty předmětů nebo vedoucími kvalifikačních prací.

Směrnice vychází z principů odpovědné a důvěryhodné umělé inteligence, v souladu s platnými právními předpisy EU, zejména s GDPR a kybernetickou bezpečností.

	Zpracovatel:	Schválil:
Jméno:	Ing. Milan Nidl, MBA	doc. Ing. Petr Dvořák, Ph.D.
Útvar / funkce:	prorektor pro informatiku a digitalizaci	rektor
Podpis:		
Platnost od:	dnem podpisu	do odvolání
Účinnost od:	dnem podpisu	do odvolání

Vymezení pojmů

1. KC-AI: Kompetenční centrum AI – je tým na provoz a rozvoj AI, jehož základem je oddělení KC AI, které je součástí Centra informatiky. Součástí týmu KC AI jsou i externí členové v roli AI mentorů
2. AI služba: digitální systém využívající metody strojového učení nebo jiné techniky umělé inteligence ke vytváření či zpracování obsahu, dat či informací, od interaktivních chatbotů po autonomní vykonávání úkolů.
3. Chráněné informace označuje následující skupiny informací:
 - a) Osobní údaje dle GDPR,
 - b) Neveřejné a důvěrné informace VŠE,
 - c) Informace, při jejichž zpracování pomocí AI služby by mohlo dojít k porušení autorského zákona, obchodního zákoníku či jiných zákonů.
4. Posuzování rizikového přístupu v užívání AI služeb probíhá v následující škále:
 - a) Zakázané
 - b) Rizikové
 - c) Povolené

Článek I

Účel a působnost

1. Tato směrnice stanovuje základní principy, pravidla, pravomoci a odpovědnosti pro používání služeb umělé inteligence (dále jen „AI“) na Vysoké škole ekonomické v Praze (dále jen „VŠE“) pro zajištění efektivní, smysluplné, bezpečné, etické, odpovědné a udržitelné využití AI služeb.
2. Směrnice má celoškolní působnost a vztahuje se na oprávněné uživatele podle čl. 2 odst. I, které v souvislosti s prací nebo jinou obdobnou činností vykonávají následující činnosti:
 - a) Závislou práci vykonávanou v pracovněprávním vztahu
 - b) Službu
 - c) Dobrovolnickou činnost
 - d) Odbornou praxi nebo stáž
 - e) Studium

Článek 2

Governance AI služeb – role a pravomoci a odpovědnosti

- I. AI služby mohou využívat pouze oprávnění uživatelé (dále též uživatelé).
 - a) Oprávnění uživatelé používají AI služby zodpovědně, eticky a bezpečně.
 - b) Oprávněnými uživateli se rozumí:
 - i. **zaměstnanci** Vysoké školy ekonomické v Praze v rozsahu potřebném k plnění pedagogických, vědeckých a dalších pracovních povinností vyplývajících z jejich pracovní náplně na Vysoké škole ekonomické v Praze,

- ii. **studenti** Vysoké školy ekonomické v Praze v rozsahu potřebném k plnění studijních a dalších povinností vyplývajících ze studijního poměru na Vysoké škole ekonomické v Praze,
 - iii. **jiné osoby**, kterým bylo na základě smluvního ujednání vydáno povolení k užívání AI služeb (zpravidla formou přidělení uživatelského jména a licence k AI službě).
2. Pro schválení užívání AI služby v prostředí VŠE rozhoduje „datový režim poskytovatele AI služby“ a právní rámec ČR takto:
- a) je uzavřena smlouva mezi VŠE a poskytovatelem AI služby.
 - b) ze strany VŠE je akceptována smlouva o zpracování osobních údajů (DPA), která zaručuje, že poskytovatel AI služby nakládá s daty v souladu s GDPR, tj. nezneužije a neprotrénuje na nich své modely, pokud VŠE do AI služby vkládá klientská či univerzitní data.
 - c) jsou zakázány veškeré (free/spotřebitelské) AI služby bez institucionální smlouvy a bez prověřené smlouvy o zpracování osobních údajů (DPA).
3. Vedoucí zaměstnanci zajišťují, aby používání AI služeb jimi a jejich podřízenými bylo v souladu s touto směrnicí.
4. Univerzitou pověřené osoby k dobrovolnickým nebo ke smluvním činnostem zajišťují, že osoby, které pro ně vystupují na VŠE, popřípadě vykonávají svou činnost dobrovolnickou, jsou seznámeni s touto směrnicí a ve sjednaných činnostech jednají v souladu s touto směrnicí.
5. Vedení VŠE:
- a) Podporuje rozvoj kompetencí v oblasti AI, zejména v kontextu managementu, ekonomiky a rozhodování.
 - b) Schvaluje pravidla etiky a bezpečnosti AI služeb.
 - c) Odpovídá za nastavení AI governance k plnění právního rámce ČR pro rozvoj a provoz AI služeb.
 - d) Odpovídá za soulad AI strategie se Strategickým záměrem VŠE.
6. Kompetenční centrum AI (KC AI) je kontrolní a operativní orgán pro AI na VŠE zejména koordinuje:
- a) Efektivní, smysluplné, bezpečné a etické využití AI.
 - b) Návrhy a změny jednotných pravidel, standardů, metodik.
 - c) Aktivní podporu transferu know-how a nejlepších praktik.
 - d) Rozvoj AI gramotnosti a podporovat vzdělávání uživatelů AI služeb v oblasti možností, limitů, rizik, bezpečnosti a odpovědného používání AI.
 - e) Selektivní nebo úplnou implementaci AI služeb v rámci životního cyklu zavádění AI služeb.
 - f) Mapování AI iniciativ.

Článek 3

Základní principy používání AI služeb na VŠE

- I. Používání AI služeb na VŠE se řídí zejména těmito principy:

- a) Efektivita – AI služba je využívána tak, aby podporovala produktivitu, kvalitu a minimalizovala finanční náklady.
- b) Smysluplnost – AI služby jsou využívány tehdy, pokud prokazatelně přispívají ke kvalitě výuky, studia, výzkumu nebo řízení univerzity.
- c) Bezpečnost – Při používání AI služby uživatel zajišťuje ochranu informací, dat a know-how VŠE i autorských práv třetích stran. Uživatelé si jsou vědomi osobní odpovědnosti za informace vkládané do AI služeb.
- d) Etika a integrita – používání AI služeb nesmí narušovat akademickou integritu, poctivost a odpovědnost jednotlivce. Uživatelé AI služeb si jsou vědomi omezení AI služeb a své osobní odpovědnosti za publikované výsledky vzniklé použitím AI služeb.
- e) Transparentnost – používání AI služeb je dokumentovatelné a zdroje pro výstupní tvrzení z AI jsou dohledatelné. Uživatelé AI služeb si jsou vědomi omezení AI služeb a své osobní odpovědnosti za výsledky použití AI služeb. Za splnění transparentnosti je považováno, že výstup z AI je jasně označen.
- f) Rizikově orientovaný přístup – při používání AI služeb musí být zohledněna povaha a míra rizika konkrétního využití AI, zejména pokud může mít dopad na práva, povinnosti, hodnocení nebo postavení studentů, zaměstnanců nebo dalších osob.
- g) Lidský dohled a kritické ověřování – výstupy AI služeb musí být vždy přiměřeně ověřeny člověkem, zejména pokud mohou mít dopad na rozhodování, hodnocení, výzkum nebo práva a povinnosti dalších osob.
- h) Nediskriminace a férovost – při používání AI služeb je třeba přiměřeně zohledňovat riziko zkreslení, diskriminace nebo neobjektivních výstupů.
- i) Proporcionalita – pravidla a omezení při používání AI služeb musí odpovídat povaze konkrétního použití, míře rizika a možným dopadům na dotčené osoby a akademické prostředí.

Článek 4

Etika používání AI služeb

AI služby a jejich výstupy musí být užívány v souladu s obecnými etickými principy a zásadami obsaženými v Etickém kodexu Vysoké školy ekonomické. Minimálně musí být splněny následující etické zásady:

- g) AI služba by měla sloužit jako nástroj na podporu rozhodování, nikoliv jako jeho náhrada.
- h) Za výstupy práce vždy nese odpovědnost konkrétní uživatel AI služby.
- i) Vždy by mělo být jasně označeno, pokud je text, obrázek či kód vytvořen pomocí AI služby.
- j) Do veřejně dostupných AI služeb nesmí být bez odpovídajícího právního titulu nebo schválení Kompetenčním centrem AI vkládány neveřejné osobní údaje, důvěrné informace, obchodní tajemství nebo autorsky chráněný obsah, pokud by mohlo dojít k jejich dalšímu využití poskytovatelem AI služby.
- k) Rozhodnutí AI služby s významným dopadem na práva, povinnosti nebo postavení studentů, zaměstnanců či dalších osob nesmí být činěna výhradně automatizovaně bez odpovídajícího lidského posouzení.

Článek 5

Transparentnost používání AI služeb

2. Uživatelé informačních služeb VŠE musí být informováni, pokud komunikují s AI systémem nebo službou.
3. Generovaný obsah AI službou používaný ve výuce, administrativě nebo komunikaci musí být označen.
4. Generovaný deepfake obsah a syntetická média musí být jednoznačně označena.
5. Pokud je výstup AI služby použit jako podklad pro rozhodnutí nebo hodnocení konkrétní osoby, musí být na žádost umožněno přiměřené vysvětlení způsobu použití AI a lidský přezkum výsledku.
6. Výstupy nástrojů pro detekci obsahu vytvořeného AI nesmí být samy o sobě považovány za důkaz porušení studijních nebo pracovních povinností a musí být vždy podrobeny individuálnímu lidskému posouzení.

Článek 6

Povolené a doporučené způsoby využití AI služeb

- I. Doporučené způsoby využití AI služeb na VŠE jsou:
 - a) Vysvětlování pojmů či postupů nebo brainstorming nápadů.
 - b) Konzultace postupů pro práci s daty.
 - c) Příprava studijních podkladů.
 - d) Strukturování textů.
 - e) Shrnutí informací.
 - f) Návrhy variant řešení.
 - g) Rešerše a vyhledávání odborných zdrojů a orientační shrnutí literatury.
 - h) Kontrola pravopisu, gramatiky, úprava citačního aparátu, úprava formátu a stylistiky textu, tabulek a grafů, pokud nedochází ke změně významu sdělení.
 - i) Použití ke strojovému překladu textu, který je součástí odevzdané práce. Rozsah přeloženého textu nesmí zasahovat do autorského přínosu práce. Pokud jde o cizí text (pasáž z knihy), pak musí být text i označen v souladu s citačními pravidly.
2. Použití AI služby jako jazykové, technické nebo podpůrné asistence není samo o sobě porušením akademické integrity, pokud nedochází k nahrazení vlastního odborného, analytického nebo tvůrčího přínosu autora.
3. Povolené způsoby využití AI služby pro agentní chování, automatizaci či jednorázové akce lze realizovat jen, pokud:
 - a) Nedochází k změně a mazání chráněných informací.
 - b) Nedochází k negativnímu ovlivňování provozu informačních systémů VŠE.
4. Rozsah povinnosti uvést použití AI služby by měl odpovídat míře jejího vlivu na výsledný výstup.
5. Použití AI služeb nesmí vést k rezignaci na vlastní odborný úsudek, kritické myšlení nebo odpovědnost za výsledný výstup.

Článek 7

Zakázané a rizikové způsoby využití AI služby

- I. Je zakázáno:
 - a) Používat Kompetenčním centrem AI neevidované, neschválené a zakázané AI služby.

- b) Používat pro pracovní činnost s neveřejnými nebo interními informacemi osobní soukromé účty u veřejných AI služeb.
- c) Vkládat do AI služeb osobní údaje, citlivá data nebo neveřejné informace v rozporu s GDPR a interními předpisy VŠE, viz článek 4.
- d) Vydávat výstupy AI služeb za vlastní odbornou nebo tvůrčí práci bez odpovídajícího přiznání použití AI, viz článek 4.
- e) Používat AI služby k obcházení studijních povinností, hodnocení nebo kontrolních mechanismů, viz článek 4.
- f) Jakékoliv jiné využití AI služby směřující k neoprávněnému nebo k nezaslouženému osobnímu zisku (jak finanční, tak nefinanční osobní výhody), např. viz článek 3 odst. 1, písm. d.
- g) Neoprávněně využívat AI služby k porušování práv duševního vlastnictví.

2. Rizikové použití AI služby:

- a) Musí být vždy konzultováno s nadřízeným, v případě nejasností z kontextu nebo právního rámce zamýšleného užití AI služby, pak s alespoň s jedním z následně uvedených: Kompetenčním centrem AI, garantem předmětu, řešitelem výzkumného grantu.
- b) Je považováno vydávání generovaných výstupů z AI služby za vlastní originální práci, tj. neuvedení využití služby AI formou citace nebo prohlášení, pokud se nejedná o povolené využití AI bez povinnosti uvedení.
- c) Je považováno v konfiguraci jako autonomní agenty k vytěžování dat a informací z informačních systémů VŠE bez schválení Kompetenčním centrem AI.

3. Za rizikové použití AI služeb se považuje zejména:

- a) Použití AI při hodnocení studentů.
- b) Použití AI při personálním rozhodování.
- c) Profilování osob.
- d) Automatizované doporučování nebo klasifikace osob.
- e) Zpracování citlivých nebo neveřejných údajů.
- f) Použití AI v disciplinárních nebo kontrolních řízeních.

4. Porušení pravidel použití AI služeb se řeší dle příslušných zákonů a vnitřních předpisů. V případě porušení pravidel používání AI v této směrnici:

- a) V oblasti výuky řeší pochybení fyzické osoby studenta Disciplinární komise příslušné fakulty.
- b) V oblasti pracovně právního vztahu řeší pochybení fyzické osoby Děkan, případně Etická komise či Interní kontrolor.
- c) V oblasti obchodně právního vztahu řeší pochybení fyzické osoby Právní oddělení.
- d) V oblastech jiných než výše uvedených nebo do stavu určení fyzické osoby řeší pochybení fyzické osoby Kompetenční centrum AI, případně Interní kontrolor.

Článek 8 Evidence AI služeb

- I. Centrum informatiky vede centrální evidenci AI služeb využívaných v:
 - a) Administrativě.
 - b) Výuce.
 - c) Výzkumu.
 - d) Infrastruktuře.
 - e) Informačních systémech.
2. Evidence AI služby obsahuje:
 - a) Název AI služby.
 - b) Použitý AI model a poskytovatel a datový režim AI služby (zero-data-retention, formulovaný rozsah zpracování dat).
 - c) Rozsah potřebných oprávnění k systémům VŠE a způsob ovládání AI služby (desktop nástroj, WWW klient, REST API rozhraní).
 - d) Forma chování AI služby (agentní, neagentní).
 - e) Účel použití AI služby na VŠE.
 - f) Očekávaný přínos zvolení konkrétního řešení AI služby.
 - g) Uvedení Garanta AI služby.
 - h) Typ zpracovávaných dat.
 - i) Popis financování.
3. Evidování AI služby musí být zajištěno před zahájením využívání.
4. Povinnost evidence AI služeb se vztahuje na AI služby, které ovlivňují zákonné povinnosti VŠE, zejména:
 - a) Používané systémově.
 - b) Integrované do systémů VŠE.
 - c) Využívané ke zpracování neveřejných, citlivých nebo významných institucionálních dat.
5. Používání neevidovaných AI služeb formulovaných v odst. 4 je zakázáno.

Článek 9

Bezpečnost AI služeb

- I. Je zaměřena na plnění zákonných požadavků univerzity, tj.:
 - a) Zpracování a ochranu osobních informací vkládaných do zpracování AI služeb v internetu nebo Cloud prostředí v kontextu GDPR.
 - b) Zpracování a ochranu dat z výzkumu a vědy v kontextu dle zákona č. 328/2025 Sb., Zákon o výzkumu, vývoji, inovacích a transferu znalostí.
 - c) Ochranu informací a kybernetické bezpečnosti dle zákona č. 264/2025 Sb., o kybernetické bezpečnosti.
 - d) Ochranu autorských práv dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).
2. Je zaměřena na minimalizaci případné škody či na jiné negativní důsledky způsobené provozem AI služeb na VŠE.

Uživatelé AI služeb:

- a) Smí používat jen povolené a schválené standardy AI služeb uvedené v článku 11 odst. 1.
 - b) Smí používat AI služby povoleným způsobem uvedeným v článku 4 a 6.
 - c) Odpovídají za důsledné ověřování spolehlivosti výstupů z AI služeb: jejich správnosti, aktuálnosti, pravdivosti, ale i nezávadnosti.
 - d) Nesmí používat agentní AI služby proti univerzitním informačním systémům z důvodů negativního vlivu na dostupnost informačních systémů a zkreslování detekce anomálních projevů uživatelů k odlišení legitimního a nelegitimního chování, viz článek 7, odst. 1.
3. AI služby provozované na VŠE musí umožňovat auditovatelné logování činností.
 4. Logování AI služeb musí zahrnovat zejména:
 - a) Identifikaci uživatele.
 - b) Čas použití.
 - c) Použitý AI model.
 - d) Vstupy a výstupy AI.
 - e) Metadata rozhodování.
 - f) Informace o automatizovaných akcích.
 5. Log záznamy AI služeb musí být:
 - a) Automaticky generované.
 - b) Chráněné proti neoprávněné změně.
 - c) Uchovávané minimálně 6 měsíců.
 - d) Dostupné pro audit a bezpečnostní analýzu.
 6. Bezpečnost AI služeb monitoruje Kompetenční centrum AI.

Článek 10

Bezpečnostní incidenty v AI službách

1. Za bezpečnostní incident v AI službách se považuje zejména:
 - a) Únik dat prostřednictvím AI služby.
 - b) Neautorizované použití AI služby.
 - c) Manipulace výstupů AI služby.
 - d) Halucinování AI služby s dopadem na provoz interního workflow nebo univerzitní agendy.
 - e) Kompromitace AI služby.
 - f) Neoprávněné agentní chování AI služby.
2. Bezpečnostní incidenty v AI službách musí být neprodleně hlášeny Centru informatiky – Manažer KB.
3. Manažer KB vede evidenci bezpečnostní incidenty v AI službách a provádí jejich vyhodnocování.

Článek 11

Standardy AI služeb pro provoz, administrativu, tvůrčí činnost a vzdělávání

- I. Povolené standardy AI služeb VŠE jsou:
 - a) Schvalovány Vedením VŠE v souladu s koncepcí Kompetenčního centra AI na VŠE.
 - b) Evidovány Kompetenčním centrem AI.
 - c) Uvedeny na webové stránce Centra informatiky.
2. Z nařízení NÚKIB je zakázán AI nástroj DeepSeek. Jeho používání je monitorováno bezpečnostními nástroji Centra informatiky. Pozitivní nález používání DeepSeek je považován za bezpečnostní incident a porušení tohoto zákazu může být posuzováno jako porušení interních bezpečnostních pravidel.

Článek 12

Závěrečná ustanovení

1. Tato směrnice nabývá účinnosti dnem podpisu rektorem.
2. Směrnice bude pravidelně přezkoumávána a aktualizována zejména s ohledem na technologický vývoj, regulační změny, bezpečnostní rizika a zkušenosti z praktického používání AI služeb na VŠE.
3. Tato směrnice je závazná pro všechny součásti VŠE.