

Národní knihovna České republiky

Směrnice č. 4/2025

Využívání nástrojů umělé inteligence

Obsah

Čl. I. Účel a oblast působnosti směrnice	3
Čl. II. Definice pojmů	4
Čl. III. Klasifikace umělé inteligence nástrojů podle rizik	5
Čl. IV. Povolené a zakázané vstupy	5
Čl. V. Pravidla používání veřejné umělé inteligence.....	6
Čl. VI. Interní nástroje umělé inteligence a specializované knihovní systémy	7
Čl. VII. Poskytování služeb umělé inteligence veřejnosti	8
Čl. VIII. Odpovědnost a kontrola výstupů	8
Čl. IX. Incidenty a oznamovací povinnost.....	8
Čl. X. Závěrečná ustanovení	9

Čl. I.

Účel a oblast působnosti směrnice

- 1) Účelem této směrnice je zajistit, aby využívání umělé inteligence (dále také „AI“) bylo v souladu s platnou českou a evropskou legislativou, respektovalo etické zásady a principy uvedené v Národní strategii pro umělou inteligenci České republiky 2030 a vycházelo z doporučení relevantních autorit.
- 2) Cílem je bezpečné, etické, transparentní a odpovědné používání umělé inteligence, při němž jsou chráněna práva a data jednotlivců, zajištěn lidský dohled (*human-in-the-loop*) a posilována důvěra veřejnosti.
- 3) Směrnice vychází zejména z požadavků české a evropské legislativy v oblasti práva umělé inteligence, ochrany osobních údajů, autorského práva a kybernetické bezpečnosti a zohledňuje principy stanovené v Národní strategii AI ČR 2030 a doporučení institucí, jako jsou NÚKIB, ÚOOÚ, EDPB a další.
- 4) Směrnice stanoví zásady a opatření, která mají zajistit:
 - a) odpovědné a transparentní využívání umělé inteligence v činnosti NK ČR;
 - b) dodržování zásady „bezpečné už od návrhu“ (*secure by design*) a „bezpečné v základním nastavení“ (*secure by default*) při návrhu a provozu systémů AI;
 - c) ochranu dat a zachování lidského rozhodování ve všech procesech, kde je umělá inteligence využívána;
 - d) rozvoj digitálních kompetencí a vzdělávání zaměstnanců v bezpečném a etickém používání AI.
- 5) Směrnice je závazná pro všechny útvary a zaměstnance NK ČR, kteří ke své pracovní činnosti využívají výpočetní techniku, a dále pro ty zaměstnance, kteří se podílejí na její správě.
- 6) Tato směrnice se vztahuje na veškeré využívání nástrojů umělé inteligence v činnosti NK ČR, a to jak pro interní potřeby, tak při poskytování služeb veřejnosti.
- 7) Zahrnuje zejména:
 - a) interní (vnitřní) použití – využívání nástrojů AI zaměstnanci a spolupracovníky NK ČR pro podporu odborné, provozní či administrativní činnosti;
 - b) externí (veřejné) použití – poskytování služeb využívajících umělou inteligenci směrem k uživatelům knihovny;
 - c) typy systémů, na které se směrnice vztahuje:
 - i) externí služby AI dostupné online;
 - ii) interní nástroje AI provozované na infrastruktuře NK ČR;
 - iii) specializované knihovní systémy obsahující AI funkce dodané třetími stranami;
 - iv) nástroje umělé inteligence využívané v rámci pilotních projektů, testování a výzkumu NK ČR.
- 8) Každé využití nástroje AI, které je spojeno s daty, procesy či reputací NK ČR, spadá pod tuto směrnici bez ohledu na to, zda nástroj byl oficiálně zaveden NK ČR či jde o soukromou iniciativu zaměstnance v rámci plnění jeho pracovních úkolů.
- 9) V případě pochybností o klasifikaci umělé inteligence nebo o dopadu jejího použití je třeba prostřednictvím Service Desku kontaktovat sekci DaT a postupovat v souladu s jejím stanoviskem.

Čl. II. Definice pojmů

1) Pro účely této směrnice se rozumí:

- a) Umělá inteligence (AI): automatizovaný nástroj (software či služba) vykazující schopnosti typicky spojované s inteligencí při plnění určitých úloh – zejména schopnost učit se z dat a rozhodovat či generovat obsahy samostatně. Patří sem systémy využívající strojové učení, hluboké neuronové sítě, velké jazykové modely (LLM) a další algoritmy schopné generovat text, obraz, zvuk či rozhodnutí;
- b) Externí nástroj umělé inteligence: konkrétní aplikace, systém nebo služba využívající umělou inteligenci. Může jít například o chatbota, nástroj pro generování textů či překlady, systém pro analýzu dat, prediktivní model, systém počítačového vidění např. ChatGPT, Bing Chat, AbI asistenty a překladače, kódovací asistenty jako GitHub Copilot apod. Tyto nástroje jsou provozovány externími společnostmi a NK ČR nad nimi nemá plnou kontrolu, zejména nad uložením a zpracováním vložených dat;
- c) Interní nástroj umělé inteligence: systém AI či aplikace provozovaná přímo NK ČR nebo jejím zřizovatelem v rámci interní infrastruktury (on-premise) či na vyhrazeném cloudovém úložišti splňujícím požadavky NK ČR. Interní nástroje AI jsou spravovány NK ČR a podléhají jejím bezpečnostním standardům. Patří sem mohou např. interní chatbot na intranetu, nástroj pro automatizované třídění digitálních dokumentů, překladový systém provozovaný na serverech NK ČR;
- d) Specializovaný knihovní systém umělé inteligence: konkrétní funkce AI integrované do knihovních informačních systémů a služeb. Může jít o moduly umělé inteligence dodané v rámci knihovnických softwarů (např. funkce doporučování literatury v online katalogu, automatická indexace a OCR v digitální knihovně apod.). Tyto systémy jsou zpravidla pořizovány od dodavatelů specializovaných na knihovní technologie a jsou nastaveny pro potřeby NK ČR;
- e) Osobní údaj: jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (subjektu údajů), ve smyslu čl. 4 odst. 1 nařízení (EU) 2016/679 (dále jen „GDPR“);
- f) Nařízení o AI: Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví pravidla pro umělou inteligenci;
- g) Zaměstnanec: osoba v pracovněprávním nebo obdobném vztahu k NK ČR, včetně externích spolupracovníků vykonávajících činnost pro NK ČR na základě smlouvy nebo dohody;
- h) Interní důvěrné informace: jakékoliv informace týkající se NK ČR, které nejsou veřejně známé a jejichž zveřejnění by mohlo poškodit dobré jméno NK ČR nebo negativně ovlivnit její činnost;
- i) Výstup: výstupem je myšlen jakýkoliv výsledek práce s umělou inteligencí, může se jednat o texty, obrázky, tabulky, videa apod.

Čl. III.

Klasifikace umělé inteligence nástrojů podle rizik

- 1) NK ČR zavádí klasifikaci používaných nástrojů umělé inteligence podle míry rizika, aby mohla uplatnit přiměřená opatření pro jejich využití:
 - a) Zakázané systémy AI: takové aplikace umělé inteligence, které jsou legislativou výslovně zakázány pro jejich nepřijatelný střet s hodnotami a právy. NK ČR nebude vyvíjet ani používat žádné systémy AI, které jsou v rozporu s platnými zákony. Pokud by se objevil požadavek na nasazení AI nástroje potenciálně spadajícího do této kategorie, je povinností jakéhokoli zaměstnance tuto skutečnost neprodleně nahlásit sekci DaT a daný záměr odmítnout;
 - b) Vysoce rizikové systémy umělé inteligence: systémy AI, které mohou výrazně ovlivnit bezpečnost, zdraví či základní práva osob. Vysoce rizikové systémy podléhají přísným pravidlům v souladu s Nařízením o AI. Nasazení takového systému schvaluje generální ředitel NK ČR po vyjádření sekce DaT a musí být doprovázeno analýzou rizik a dokumentací o jejich bezpečnosti a spolehlivosti;
 - c) Systémy umělé inteligence s omezeným rizikem: do této kategorie spadají nástroje AI, u nichž existují určitá rizika, ale nejsou natolik závažná, aby spadala do vysokého rizika. Při využívání těchto běžných nástrojů umělé inteligence bude NK ČR dodržovat obecná pravidla bezpečnosti a etiky, jež jsou dále v této směrnici rozvedena;
 - d) Minimální či zanedbatelné riziko: do této kategorie patří veškeré ostatní systémy AI. Zaměstnanci dbají i u této skupiny na dodržování zásad bezpečnosti, nešíření protiprávního obsahu a dodržování dalších povinností, které jim ukládají vnitřní předpisy NK ČR. Nástroje s minimálním rizikem mohou zaměstnanci používat v souladu s interními předpisy bez zvláštního povoloovacího procesu.
- 2) NK ČR průběžně hodnotí rizikovost používaných nástrojů umělé inteligence. Pokud dojde ke změně jejich funkčnosti, rozšíření použití nebo se objeví nové skutečnosti ovlivňující riziko, může být nástroj přeřazen do jiné kategorie a mohou být stanovena odpovídající opatření. Odpovědnost za správné zařazení nástroje má příslušný vedoucí pracovník ve spolupráci se sekci DaT.
- 3) Veškeré nástroje umělé inteligence používané v NK ČR musí být navrhovány a využívány tak, aby zachovávaly lidský dohled, nediskriminovaly uživatele, byly transparentní, bezpečné a spolehlivé.
- 4) Sekce DaT vede evidenci systémů umělé inteligence používaných v NK ČR, zodpovídá za jejich klasifikaci a aktualizaci. Seznam systémů AI je pravidelně revidován (nejméně 1x ročně) a dostupný všem zaměstnancům NK ČR prostřednictvím intranetu.

Čl. IV.

Povolené a zakázané vstupy

- 1) Zaměstnanci NK ČR jsou při práci s nástroji umělé inteligence povinni zvažovat, jaká data mohou do těchto systémů vkládat, s ohledem na ochranu osobních údajů, autorských práv, důvěrnosti informací a bezpečnost dat. Vyžaduje se předběžná opatrnost.
- 2) Do nástrojů umělé inteligence lze vkládat pouze takové informace, které:

- a) neohrožují práva a oprávněné zájmy třetích osob;
 - b) nejsou předmětem ochrany osobních nebo citlivých údajů, pokud k tomu není právní důvod;
 - c) neporušují právní předpisy ani interní závazky NK ČR;
 - d) nejsou označeny jako interní či důvěrné informace, pokud jejich vložení nebylo předem schváleno Sekcí DaT.
- 3) Do veřejně dostupných nástrojů AI (např. online služeb typu ChatGPT, Copilot, Gemini apod.) je výslovně zakázáno vkládat:
- a) osobní a citlivé údaje, včetně údajů o soukromí osob, zaměstnanců nebo uživatelů;
 - b) interní důvěrné informace a provozní data NK ČR;
 - c) autorsky chráněný obsah, pokud licence jeho využití v nástrojích umělé inteligence výslovně nepovoluje;
 - d) informace, které by mohly být zneužity k vytvoření nelegálního, neetického či bezpečnostně rizikového obsahu.
- 4) Do interních systémů AI je povoleno vkládat výše uvedené vstupy pouze za podmínky, že je k tomu systém určen a podle vyjádření sekce DaT je odpovídajícím způsobem zabezpečen.
- 5) Zaměstnanci jsou si vědomi, že osobní nebo jinak citlivé údaje se mohou nacházet i v metadatech, připojené e-mailové korespondenci apod., a počínají si při kopírování a vkládání větších celků obezřetně.
- 6) Vedoucí zaměstnanci mohou stanovit pro své útvary další pravidla pro využívání AI, zejména s ohledem na odůvodněnost a dokumentovatelnost využití umělé inteligence při plnění pracovních úkolů. Tato pravidla však nemohou vést k zákazu využívání umělé inteligence zaměstnanci a musí být v souladu s předpisy ohledně umělé inteligence.

Čl. V.

Pravidla používání veřejné umělé inteligence

- 1) Zaměstnanci NK ČR mohou využívat veřejně dostupné (externí) služby umělé inteligence pouze v případě, že jsou uvedeny na seznamu doporučených nebo schválených nástrojů vedeném Sekcí DaT. Pokud zaměstnanec hodlá použít jiný veřejný nástroj AI, který není na seznamu, je povinen před zahájením práce s tímto nástrojem kontaktovat Sekci DaT prostřednictvím Service Desku a požádat o jeho posouzení.
- 2) Je zakázáno využívat zjevně nedůvěryhodné nebo bezpečnostně rizikové služby AI, zejména ty, které neuvádějí způsob nakládání s vloženými daty nebo sídlí mimo jurisdikci Evropské unie bez záruk odpovídající úrovni ochrany.
- 3) Při využívání veřejně dostupných nástrojů umělé inteligence jsou zaměstnanci povinni dodržovat tyto zásady:
 - a) Minimalizace vstupů: do AI se vkládají pouze nezbytné informace potřebné k dosažení požadovaného výsledku;
 - b) Kontrola podmínek služby: před prvním použitím umělé inteligence je nutné ověřit podmínky služby, zejména způsob zpracování dat, nakládání s vloženými informacemi a místo jejich uložení;
 - c) Preference evropských služeb – zaměstnanci jsou povinni preferovat takové modely umělé inteligence, které zpracovávají data v rámci Evropské unie;

- d) Používání služeb s účtem NK ČR: tam, kde je to možné, musí být veřejné služby AI využívány prostřednictvím služebních účtů NK ČR, nikoli osobních účtů;
 - e) Zásada bezpečného přihlašování: přístup musí být chráněn silným heslem a, pokud to služba umožňuje, případně dvou faktorovým ověřením;
 - f) Transparentnost: zaměstnanec informuje svého nadřízeného nebo pracovní tým o tom, že při plnění pracovních úkolů využívá nástroj/e umělé inteligence;
 - g) Alternativní řešení: při využívání umělé inteligence by měla být zachována možnost dokončit pracovní úkol i bez zapojení AI, zejména v případě výpadku nebo ztráty služby.
- 4) Při využívání veřejných nástrojů umělé inteligence musí zaměstnanci vždy zohlednit zásady „bezpečné už od návrhu“ (secure by design) a „bezpečné v základním nastavení“ (secure by default). Znamená to předcházet rizikům úniku dat, omezit sdílení informací a využívat pouze takové nástroje, které splňují bezpečnostní standardy NK ČR.
- 5) Sekce DaT je oprávněna kdykoli aktualizovat seznam doporučených a schválených veřejných nástrojů AI, vydávat k nim metodická doporučení a pozastavit jejich používání, pokud vyhodnotí bezpečnostní nebo právní riziko.

Čl. VI.

Interní nástroje umělé inteligence a specializované knihovní systémy

- 1) Interní nástroje AI, vč. nástrojů integrovaných v knihovních aplikacích, provozované přímo NK ČR nebo dodavateli NK ČR v rámci její infrastruktury, mohou pracovat s daty NK ČR za podmínek, které zajišťují soulad s právními předpisy a bezpečnostními standardy.
- 2) Při zavádění interních nástrojů umělé inteligence je nezbytné, aby dohoda s dodavateli obsahovala:
 - a) ustanovení o ochraně dat s ohledem na platnou legislativu a zajištění kybernetické a provozní bezpečnosti;
 - b) garance dodavatele, že dodávaný model AI splňuje zákonné a etické požadavky.
- 3) Při využívání interní umělé inteligence platí tyto zásady:
 - a) zavedení každého interního systému AI podléhá schválení příslušným vedoucím zaměstnancem a sekci DaT;
 - b) interní systémy umělé inteligence musí splňovat bezpečnostní standardy NK ČR;
 - c) osobní údaje mohou být interními nástroji AI zpracovávány pouze tehdy, pokud jsou splněny všechny podmínky GDPR a interní předpisy NK ČR;
 - d) omezení interního přístupu na zaměstnance, kteří přístup k danému modelu umělé inteligence pro svou práci skutečně potřebují;
 - e) transparentnost vůči uživatelům – pokud výstup z modulu AI směřuje k veřejnosti musí být odpovídajícím způsobem označený;
 - f) Model AI nesmí být využit k obcházení přístupových práv k dokumentům;
 - g) zaměstnanec zodpovídá za kvalitu dat, které do modulu umělé inteligence vkládá.

Čl. VII.

Poskytování služeb umělé inteligence veřejnosti

- 1) Každá služba AI poskytovaná veřejnosti musí být:
 - a) transparentní – uživatel musí být jasně informován, že komunikuje s umělou inteligencí;
 - b) bezpečná a nediskriminační – systém nesmí poskytovat závadný, klamavý ani diskriminační obsah;
 - c) pod dohledem člověka – služba musí mít určenou odpovědnou osobu, která sleduje její výstupy a kvalitu;
 - d) v souladu s ochranou soukromí – zpracování osobních údajů musí mít právní titul a být technicky zabezpečeno;
 - e) označená – veřejně prezentované výstupy AI musí být zřetelně označeny jako generované umělou inteligencí.
- 2) Služby umělé inteligence mohou být poskytovány i v pilotním režimu, pokud jsou dodrženy výše uvedené zásady a zajištěn dohled sekce DaT.

Čl. VIII.

Odpovědnost a kontrola výstupů

- 1) Za konečné využití výstupů z umělé inteligence vždy odpovídá člověk.
- 2) Zaměstnanec je povinen před použitím výstupu z umělé inteligence ověřit jeho správnost, vhodnost a soulad s právními a etickými zásadami NK ČR.
- 3) Při posuzování výstupů z umělé inteligence se zaměstnanec zaměřuje zejména na:
 - a) správnost, vhodnost a legálnost výstupu;
 - b) přesnost a relevance výstupu;
 - c) uvedení zdrojů a původ informací;
 - d) vyloučení předsudků, neetického nebo nevhodného obsahu;
 - e) uvést informaci o zapojení umělé inteligence, pokud AI ovlivnila pracovní výstup.
- 4) Nasazení umělé inteligence má sloužit ke zvýšení efektivity a podpory práce, nikoli k nahrazení odborného úsudku.
- 5) Nedodržení těchto zásad bude považováno za závažné porušení interních předpisů zaměstnavatele a může mít následky v pracovněprávní oblasti.

Čl. IX.

Incidenty a oznamovací povinnost

- 1) Bezpečnostním incidentem se rozumí situace, kdy došlo ke zneužití nástroje umělé inteligence nebo prostřednictvím umělé inteligence k narušení bezpečnosti informací.
- 2) K porušení zabezpečení osobních údajů dojde při neoprávněném zpracování nebo úniku osobních údajů. Postup při porušení zabezpečení osobních údajů stanoví jiný vnitřní předpis.

- 3) Pokud služba poskytovaná za pomoci AI vydá uživateli závažně chybnou, nebo jinak závadnou informaci, která vyvolá uživateli újmu, jedná se o obsahový incident.
- 4) Interním incidentem je porušení této směrnice, ať už vědomé, nebo způsobené omylem.
- 5) Při zjištění nebo podezření na jakýkoliv incident ve spojitosti s umělou inteligencí je zaměstnanec, který se o tom dozvěděl, povinen bezodkladně nahlásit incident na Service Desk. V případě podezření na porušení zabezpečení osobních údajů též KGŘ v souladu s interním předpisem ohledně GDPR.
- 6) Po nahlášení incidentu na Service Desk vyhodnotí sekce DaT situaci a přijme nezbytná technická opatření. Pokud zjistí porušení zabezpečení osobních údajů ohlásí to bezodkladně KGŘ v souladu s jiným interním předpisem.
- 7) O každém incidentu pořídí sekce DaT záznam, v němž popíše, co se stalo, jaký byl časový postup řešení incidentu, jaká nápravná opatření byla přijata, jakou škodu incident způsobil a kdy a kam byl nhlášen. Záznam o incidentu je interním dokumentem, který v případě potřeby slouží ke komunikaci s příslušnými úřady.
- 8) Po zvládnutí akutní fáze incidentu provede NK ČR analýzu jeho příčin a přijme odpovídající opatření, aby se podobná situace v budoucnu neopakovala.
- 9) K informování veřejnosti ohledně incidentu je oprávněn výlučně Odbor komunikace, který postupuje v úzké spolupráci se sekci DaT.

Čl. X.

Závěrečná ustanovení

- 1) Vedoucí zaměstnanci NK ČR zajistí, aby s interními předpisy ohledně používání umělé inteligence byli prokazatelně seznámeni všichni jim podřízení zaměstnanci, kteří by mohli mít při plnění svých pracovních úkolů k jakýmkoliv nástrojům umělé inteligence přístup. Seznámení se prokazuje podpisem potvrzení, které je přílohou této směrnice a je připravené pro využití v RemoteSign. Podepsané potvrzení je nutno zaslat nejpozději do 30 dnů po účinnosti této směrnice ředitelce/řediteli odboru ICT prostřednictvím e-mailu.
- 2) Sekce DaT vede a průběžně aktualizuje interní seznam systémů AI používaných v NK ČR a seznam doporučených nebo schválených nástrojů umělé inteligence. Druhý jmenovaný seznam je dostupný na intranetu NK ČR.
- 3) Sekce DaT je oprávněna kdykoliv za platnosti této směrnice vydat opatření útvaru, kterým detailněji upraví otázky využívání umělé inteligence, povolování nových modelů AI, správu modelů AI a řešení bezpečnostních incidentů.
- 4) Do 30 dnů od nabytí účinnosti této směrnice předloží vedoucí všech útvarů, pokud možno prostřednictvím ředitelů odborů, sekci DaT seznam všech nástrojů umělé inteligence, které se v jejich útvech používají nebo používaly. Pokud se nástroje umělé inteligence nevyužívají, útvar tuto skutečnost písemně potvrdí.
- 5) Sekce DaT posoudí nahlášené nástroje umělé inteligence z hlediska právních, bezpečnostních a etických požadavků a rozhodne o jejich zařazení mezi doporučené nebo zakázané nástroje.
- 6) Nedílnou součástí této směrnice je příloha č. 1 – vzor potvrzení o seznámení.

- 7) Tato směrnice je závazná pro:
 - a) všechny útvary a zaměstnance NK ČR, kteří ke své pracovní činnosti využívají výpočetní techniku;
 - b) pro zaměstnance, kteří se podílejí na správě výpočetní techniky.
- 8) Tato směrnice nabývá platnosti dnem podpisu a účinnosti dnem vyvěšení na intranetu.

V Praze dne

Mgr. Tomáš Foltýn
generální ředitel
Národní knihovna České republiky

Směrnice č. 4/2025 - Využívání nástrojů umělé inteligence

Opatření generálního ředitele č. 15/2025 – Kodex odpovědného využívání umělé inteligence

Tímto potvrzuji, že jsem byl/a seznámen/a s obsahem následujících interních předpisů ohledně používání umělé inteligence v Národní knihovně České republiky:

- Směrnice č. 4/2025 - Využívání nástrojů umělé inteligence;
- Opatření generálního ředitele č. 15/2025 – Kodex odpovědného využívání umělé inteligence.

Byl/a jsem poučen/a o jejich závaznosti a o povinnosti je dodržovat.

Útvar / oddělení: _____

Ředitel odboru: _____

Jméno a příjmení	Interní elektronický podpis