



RGIS

POLITIKA UMĚLÉ INTELIGENCE

RGIS

2025

© 2025 RGIS. Všechna práva vyhrazena.
RGIS_MC_0072_01

INDEX

- 2 | Představitelé CEO
- 3 | Umělá inteligence na pracovišti: proč politika umělé inteligence
- 4 | 1. Úvod
- 4 | 2. Účel
- 4 | 3. Scope
- 4 | 4. Definice
- 5 | 5. Etika umělé inteligence
- 5 | 6. Schválené nástroje ai a jejich použití
- 6 | 7. Zakázané fyzické a softwarové postupy
- 6 | 8. Přeshraniční předávání údajů a regionální soulad
- 6 | 9. Environmentální a odpovědné digitální důsledky
- 7 | 10. Odpovědnost, dodržování předpisů a monitorování
- 7 | 11. Změny politiky
- 8 | Dodatek – ChatGPT
- 10 | Dodatek – Claude
- 10 | Dodatek – Microsoft Co-Pilot

Vážený kolegové,

Vzhledem k tomu, že v RGIS využíváme transformační sílu umělé inteligence (AI), závisí náš úspěch na etickém a odpovědném využívání této technologie a na spolupráci. Umělá inteligence by měla zlepšit naši činnost a zároveň být v souladu s našimi základními hodnotami:



INTEGRITY

Umělou inteligenci používáme eticky a transparentně, přičemž dbáme na spravedlnost, odpovědnost a dodržování všech předpisů.



EXCELLENCE

Ve všech řešeních založených na umělé inteligenci se snažíme o inovace při zachování přesnosti, spolehlivosti a kvality.



RESPEKTUJTE

V aplikacích umělé inteligence upřednostňujeme lidskou důstojnost, soukromí dat a inkluzivitu a zajišťujeme spravedlnost pro naše zaměstnance, zákazníky a zúčastněné strany.



TÝMOVÁ PRÁCE

Integrujeme umělou inteligenci jako nástroj na podporu a posílení našich týmů, který podporuje spolupráci, nikoliv nahrazuje lidské odborné znalosti.



INOVACE

Využíváme umělou inteligenci ke zlepšení efektivity, rozhodování a služeb zákazníkům a zároveň průběžně vyhodnocujeme její dopad a efektivitu.

Tyto zásady tvoří základ naší politiky umělé inteligence, která určuje, jakým způsobem vyvíjíme, zavádíme a používáme umělou inteligenci v rámci celého systému RGIS. Každý člen týmu je zodpovědný za to, aby AI byla v souladu s našimi etickými standardy a obchodními cíli.

Máte-li jakékoli dotazy nebo obavy ohledně používání UI v rámci systému RGIS, obraťte se na právní oddělení (legaleurope@rgis.com). Děkujeme, že dodržíte naše hodnoty a zajišťujete odpovědné používání UI.

S pozdravem,



Asaf Cohen
Chief Executive Officer

RGIS



INTEGRITY



EXCELLENCE



RESPECT



TEAMWORK



INNOVATION

Politika Umělé Intelligence

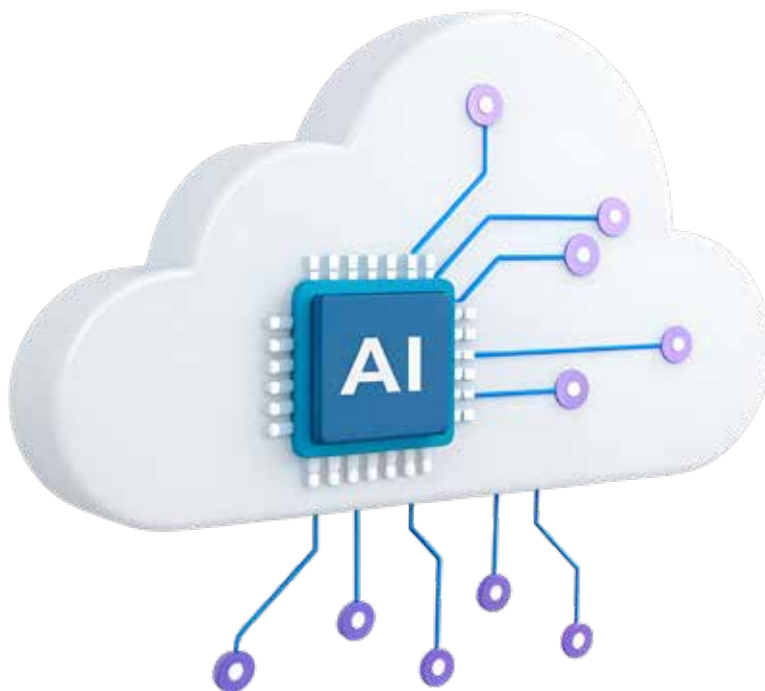
UMĚLÁ INTELIGENCE NA PRACOVÍŠTI: PROČ POLITIKA UMĚLÉ INTELIGENCE

S tím, jak se umělá inteligence neustále vyvíjí, je její potenciál pro zvýšení produktivity, zefektivnění provozu a podporu inovací nepopíratelný. S velkým potenciálem však přicházejí i neodmyslitelná rizika - od obav o bezpečnost dat a dodržování předpisů až po etické aspekty a problémy s přesností. Naše politika AI je navržena tak, aby zajistila správnou rovnováhu mezi příležitostmi a riziky a zajistila, že AI bude integrována bezpečně, strategicky a v souladu s našimi obchodními cíli.

Pod vedením ředitele pro umělou inteligenci bude integrace umělé inteligence do našich procesů pečlivě posuzována a implementována tam, kde přináší největší hodnotu, a bude zajištěno, že umělá inteligence podporuje - nikoli nahrazuje - lidské odborné znalosti. Tato politika slouží jako rámec pro zodpovědné využívání AI a zajišťuje jasnost, bezpečnost a dodržování předpisů ve všech odděleních.

Nedávná hodnocení poukazují na různou úroveň přijetí umělé inteligence v naší organizaci. Zatímco některé týmy přijaly AI pro automatizaci, analýzu a tvorbu obsahu, jiné stále váhají kvůli obavám o bezpečnost, dodržování předpisů a přesnost. Náš přístup tyto obavy zohledňuje a upřednostňuje vzdělávání, správu a bezpečnou implementaci s cílem vybudovat důvěru v roli AI v našem podniku.

Touto politikou zdůrazňujeme, že umělá inteligence není jen nástroj - je to odpovědnost. Zaměstnanci musí používat UI eticky, zamezit sdílení důvěrných údajů, zajistit přesnost výstupů a zachovat lidský dohled při rozhodování. Dodržováním těchto pokynů můžeme plně využít potenciál AI a zároveň ochránit naše operace, naše lidi a naši budoucnost.



Politika Umělé Inteligence

1. ÚVOD

Tato politika stanoví pokyny a standardy pro odpovědné používání technologií umělé inteligence (AI), včetně generativní umělé inteligence (GenAI), v rámci RGIS. Nástroje umělé inteligence jsou technologie určené k provádění úkolů, které obvykle vyžadují lidskou inteligenci, zatímco nástroje GenAI specificky generují nový, dříve nedefinovaný obsah na základě uživatelských vstupů nebo podnětů. Příkladem nástrojů GenAI jsou ChatGPT, Gemini, Microsoft Co-Pilot a další podobné platformy. Technologie AI a GenAI nabízejí transformační potenciál napříč celou společností RGIS a umožňují zefektivnit provoz, zvýšit produktivitu a podpořit kreativitu v oblastech, jako je analýza dat, tvorba obsahu a automatizace procesů.

2. ÚČEL

Umělá inteligence nabízí neuvěřitelný potenciál, ale zároveň přináší významná rizika, včetně těch, která souvisejí s bezpečností dat, důvěrností, přesností, dodržováním duševního vlastnictví a etickým používáním. Nalezení správné rovnováhy mezi využitím transformačního potenciálu AI a zmírněním rizik, která jsou jí vlastní, je zásadní pro zajištění odpovědné a efektivní implementace.

Vyžaduje proaktivní přístup, který podporuje inovace a zároveň zachovává přísná bezpečnostní opatření na ochranu dat, zajištění souladu s předpisy a dodržování etických norem. Tato politika uvádí pokyny pro interní používání, vývoj a zavádění systémů umělé inteligence (AI) v rámci systému RGIS.

Cílem je zajistit, aby naše UI používala:

- a. je v souladu s etickými normami;
- b. respektuje ochranu osobních údajů při ochraně citlivých a důvěrných informací RGIS,
- c. údaje o zákaznících
- d. dodržuje regulační rámce UI přináší významná rizika, včetně těch, která se týkají bezpečnosti dat, důvěrnosti, přesnosti, dodržování duševního vlastnictví a etického používání.

Cílem je zajistit, aby naše využívání AI bylo v souladu s etickými normami, respektovalo ochranu osobních údajů při ochraně citlivých a důvěrných informací společnosti RGIS a dodržovalo regulační rámce, včetně zákona EU o umělé inteligenci.

3. SCOPE

Tyto zásady se vztahují na všechny zaměstnance, včetně dočasných zaměstnanců a stážistů, smluvních partnerů, přidružených společností a třetích stran, kteří pracují s nástroji a systémy umělé inteligence poskytnutými nebo schválenými společností RGIS nebo s nimi interagují a přistupují k údajům společnosti RGIS. Týká se aplikací UI, nakládání s daty a požadavků na dodržování předpisů souvisejících se systémy UI používanými v rámci organizace.

4. DEFINICE

Nástroje umělé inteligence: Jakýkoli software, aplikace nebo hardware, který využívá techniky umělé inteligence (včetně strojového učení, zpracování přirozeného jazyka, rozpoznávání obrazu a generativních schopností).

Tým pro správu umělé inteligence: skupina v rámci organizace odpovědná za dohled a řízení vývoje, zavádění a etického využívání technologií umělé inteligence.

Důvěrné informace: Důvěrnými informacemi se rozumí údaje, které jsou majetkem společnosti RGIS, včetně obchodních tajemství, obchodních strategií, finančních informací a jakýchkoli jiných informací, které nejsou veřejně dostupné. Veškeré citlivé nebo neveřejné informace, mimo jiné včetně patentované technologie RM společnosti RGIS, systémů řízení zásob, řešení RFID, implementací bezdrátových technologií, údajů o zásobách klientů (včetně údajů o auditu zdravotnických zařízení), interní komunikace a provozních strategií.

Politika Umělé Inteligence

4. DEFINICE (pokračoval)

Data: označují veškeré informace shromážděné, zpracované nebo uložené systémy umělé inteligence, včetně uživatelských vstupů, výstupů systému, metadat a jakýchkoli strukturovaných nebo nestrukturovaných informací používaných pro školení, odvozování nebo rozhodování.

Etické normy: Zásady, jimiž se řídí odpovědné používání UI a které zajišťují spravedlnost, transparentnost a respektování práv jednotlivců.

Generativní umělá inteligence: Kategorie systémů umělé inteligence, které jsou navrženy tak, aby generovaly nový, dosud nedefinovaný obsah na základě uživatelských vstupů nebo podnětů. Tento obsah může zahrnovat text, obrázky, zvuk, video nebo jiné formy médií.

Proprietární systémy: RGIS: technologie RM, systémy řízení zásob, implementace RFID a bezdrátových technologií a související digitální infrastruktura.

Citlivé informace: Citlivé informace zahrnují údaje, které vyžadují ochranu vzhledem ke své povaze, včetně osobních údajů, zdravotních záznamů a všech informací, které by mohly vést ke krádeži identity nebo narušení soukromí.

Neautorizované systémy umělé inteligence: Nástroje nebo platformy AI, které nebyly výslovně přezkoumány a schváleny týmem pro správu AI.

5. ETIKA UMĚLÉ INTELIGENCE

5.1. Nediskriminace

Zavázali jsme se k poctivému vývoji a používání algoritmů umělé inteligence. Používáme kontrolní mechanismy k odhalení a minimalizaci předpojatosti v tréninkových datech a modelech umělé inteligence a zajišťujeme, aby nedocházelo k diskriminaci z hlediska věku, pohlaví, etnického původu, vyznání atd.

5.2. Transparentnost

Rozhodnutí automatizovaná našimi algoritmy jsou příslušným uživatelům vysvětlena přístupným způsobem, aby bylo zajištěno, že jim porozumí. Uživatelé tak mohou lépe pochopit logiku automatizovaných rozhodnutí, zejména pokud výsledky ovlivňují profesní nebo osobní aspekty.

5.3. Lidská kontrola

Lidé zůstávají v centru rozhodovacích procesů v provozech, které využívají technologie umělé inteligence. U každého důležitého rozhodnutí zahrnujícího UI je vždy možné odvolání člověka, které uživatelům nebo zaměstnancům umožňuje zpochybnit a objasnit výsledky vytvořené UI.

6. SCHVÁLENÉ NÁSTROJE AI A JEJICH POUŽITÍ

Zaměstnanci mohou používat nástroje umělé inteligence, které splňují jedno z následujících kritérií:

Uznávání poskytovatelé: Nástroje pocházející od známých a renomovaných dodavatelů - především ze Spojených států - nebo od dodavatelů s prokazatelnými výsledky v oblasti dodržování předpisů a zabezpečení.

Interně vyvinuté nástroje: aplikace umělé inteligence vyvinuté a udržované týmem IT RGIS.

Všechny ostatní nástroje nebo aplikace umělé inteligence musí před použitím projít formálním procesem kontroly a získat výslovné povolení od týmu pro správu umělé inteligence.

Politika Umělé Intelligence

7. ZAKÁZANÉ FYZICKÉ A SOFTWAREVÉ POSTUPY

Zaměstnanci NESMÍ:

Instalace nebo používání neautorizovaných nástrojů AI:

- Instalovat, stahovat nebo provozovat jakýkoli software nebo hardware AI na zařízeních ve vlastnictví RGIS nebo na osobních zařízeních připojených k sítím RGIS bez předchozí kontroly a výslovného písemného souhlasu týmu pro správu AI.
- Zavádět nástroje umělé inteligence, které se integrují nebo propojují s jakýmkoliv proprietárními systémy RGIS (včetně technologie RM, systémů řízení zásob, řešení RFID, implementací bezdrátových technologií, aplikací pro tablety a systémů přístrojových desek), pokud k tomu nejsou výslovně oprávněny.

Obcházení bezpečnostních nebo schvalovacích protokolů:

- Měnit, obcházet nebo vypínat jakákoli bezpečnostní opatření nebo schvalovací procesy určené ke kontrole integrace nebo používání systémů UI v rámci systému RGIS.

Integrace nástrojů AI se základními systémy:

- Připojovat nebo integrovat jakékoli nástroje AI s vlastními systémy společnosti RGIS – včetně technologie RM, systémů pro správu zásob, řešení RFID, platform bezdrátových technologií, aplikací pro tablety a řídicích panelů – bez výslovného povolení týmu pro správu AI a zabezpečení IT.

Zneužití údajů o zákaznících:

- Používání neautorizovaného softwaru, hardwaru nebo externích paměťových zařízení ke shromažďování, zpracování nebo ukládání dat zákazníků je přísně zakázáno. Všechny systémy umělé inteligence musí dodržovat bezpečnostní protokoly schválené společností, aby se zabránilo narušení bezpečnosti dat a neoprávněnému přístupu k nim.

8. PŘESHYBNÍ PŘEDÁVÁNÍ ÚDAJŮ A REGIONÁLNÍ SOULAD

Vzhledem k celosvětovému působení společnosti RGIS musí zaměstnanci:

- Zajistěte, aby každý nástroj umělé inteligence, který pracuje s daty, splňoval zákony a předpisy na ochranu dat v příslušných jurisdikcích (např. GDPR v EU, CCPA v Kalifornii, HIPAA pro zdravotnická data a další národní normy).
- Nepřenášet žádné důvěrné nebo citlivé údaje přes hranice států prostřednictvím systémů AI, pokud takové přenosy nebyly výslovně přezkoumány, zdokumentovány a schváleny týmem pro správu AI.

9. ENVIRONMENTÁLNÍ A ODPOVĚDNÉ DIGITÁLNÍ DŮSLEDKY

Snížení digitální stopy:

- Společnost RGIS používá odpovědné postupy ke snížení dopadu svých digitálních činností na životní prostředí. To zahrnuje optimalizované využívání serverů, správnou recyklaci zařízení a výběr energeticky účinných technologií.

Zodpovědné digitální povědomí:

- Podporujeme odpovědné používání digitálních technologií a propagujeme ekologické chování zaměstnanců, například omezování tisku papíru a optimalizaci využívání zdrojů IT.

RGIS

Politika Umělé Intelligence

10. ODPOVĚDNOST, DODRŽOVÁNÍ PŘEDPISŮ A MONITOROVÁNÍ

Odpovědnost za chyby generované umělou inteligencí:

- Společnost RGIS nenese odpovědnost za chyby vygenerované umělou inteligencí v inventurách, auditech nebo provozních zprávách, pokud byl nástroj umělé inteligence použit bez řádného schválení nebo mimo rámec těchto zásad. Každá taková chyba bude předmětem interního přezkumu a proti zaměstnancům, u nichž bude zjištěno porušení, mohou být přijata disciplinární opatření.

Monitorování a audit:

- Společnost RGIS si vyhrazuje právo monitorovat a kontrolovat používání nástrojů umělé inteligence na všech zařízeních ve vlastnictví společnosti nebo připojených ke společnosti RGIS. Nedodržování těchto zásad může vést k disciplinárním opatřením, a to až k ukončení pracovního poměru.

Hlášení porušení předpisů:

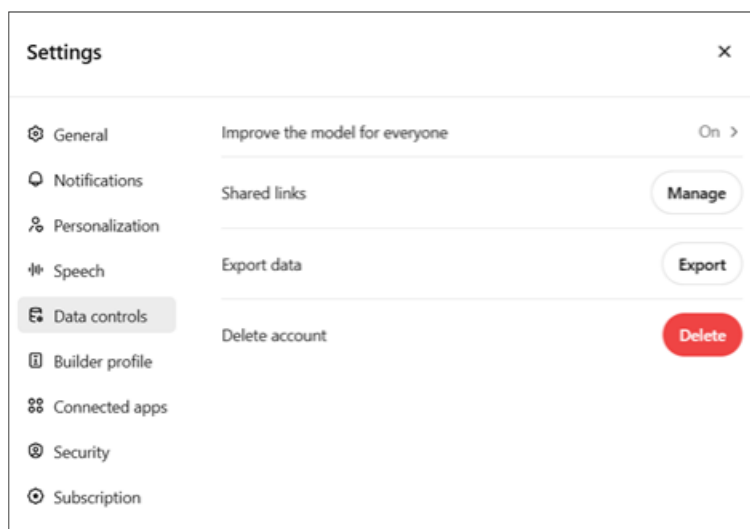
- Zaměstnanci musí jakékoli podezření na porušení těchto zásad neprodleně nahlásit svému nadřízenému, oddělení IT Security nebo týmu pro správu umělé inteligence.

11. ZMĚNY POLITIKY

Společnost RGIS si vyhrazuje právo tyto zásady kdykoli změnit nebo aktualizovat. Veškeré změny budou oznámeny oficiální cestou a vstoupí v platnost okamžitě po zveřejnění.

RGIS POLITIKA UMĚLÉ INTELIGENCE Dodatek

CHATGPT



RGIS POLITIKA UMĚLÉ INTELIGENCE Dodatek

CHATGPT

Model improvement

Improve the model for everyone

Allow your content to be used to train our models, which makes ChatGPT better for you and everyone who uses it. We take steps to protect your privacy. [Learn more](#)

Voice mode

Include your audio recordings

Include your video recordings

Include your audio and video recordings from Voice Mode to train our models. Transcripts and other files are covered by "Improve the model for everyone." [Learn more](#)

Done

Model improvement

Improve the model for everyone

Allow your content to be used to train our models, which makes ChatGPT better for you and everyone who uses it. We take steps to protect your privacy. [Learn more](#)

Voice mode

Include your audio recordings

Include your video recordings

Include your audio and video recordings from Voice Mode to train our models. Transcripts and other files are covered by "Improve the model for everyone." [Learn more](#)

Done

RGIS POLITIKA UMĚLÉ INTELIGENCE Dodatek

CLAUDE

The screenshot shows the Claude AI website interface. At the top, there is a search bar with the text "Search for articles...". Below the search bar, the article title "I would like to input sensitive data into Free Claude.ai or Claude Pro. Who can view my conversations?" is displayed. The article is dated "Updated yesterday". The main text of the article explains that by default, prompts and conversations from Free Claude.ai or Claude Pro are not used to train models. It lists two instances where data may be used: (1) if the user gives explicit permission by submitting feedback or reaching out to support, and (2) where prompts and conversations are flagged for trust and safety reviews. The article also mentions that data is used to detect and enforce [Usage Policy](#) violations, including to train trust and safety classifiers. Only a limited number of staff members have access to conversation data, and they only access this data for explicit business purposes.

MICROSOFT CO-PILOT

The screenshot shows an article titled "How does Microsoft 365 Copilot use your proprietary organizational data?". The article explains that Microsoft 365 Copilot provides value by connecting LLMs to organizational data. It can generate responses anchored in organizational data, such as user documents, emails, calendar, chats, meetings, and contacts. Microsoft 365 Copilot combines this content with the user's working context, such as the meeting a user is in now, the email exchanges the user had on a topic, or the chat conversations the user had last week. Microsoft 365 Copilot uses this combination of content and context to help provide accurate, relevant, and contextual responses.

Important

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot.

Microsoft 365 Copilot only surfaces organizational data to which individual users have at least view permissions. It's important that you're using the permission models available in Microsoft 365 services, such as SharePoint, to help ensure the right users or groups have the right access to the right content within your organization. This includes permissions you give to users outside your organization through inter-tenant collaboration solutions, such as shared channels in Microsoft Teams.

When you enter prompts using Microsoft 365 Copilot, the information contained within your prompts, the data they retrieve, and the generated responses remain within the Microsoft 365 service boundary, in keeping with our current privacy, security, and compliance commitments. Microsoft 365 Copilot uses Azure OpenAI services for processing, not OpenAI's publicly available services. Azure OpenAI doesn't cache customer content and Copilot modified prompts for Microsoft 365 Copilot. For more information, see the [Data stored about user interactions with Microsoft 365 Copilot](#) section later in this article.