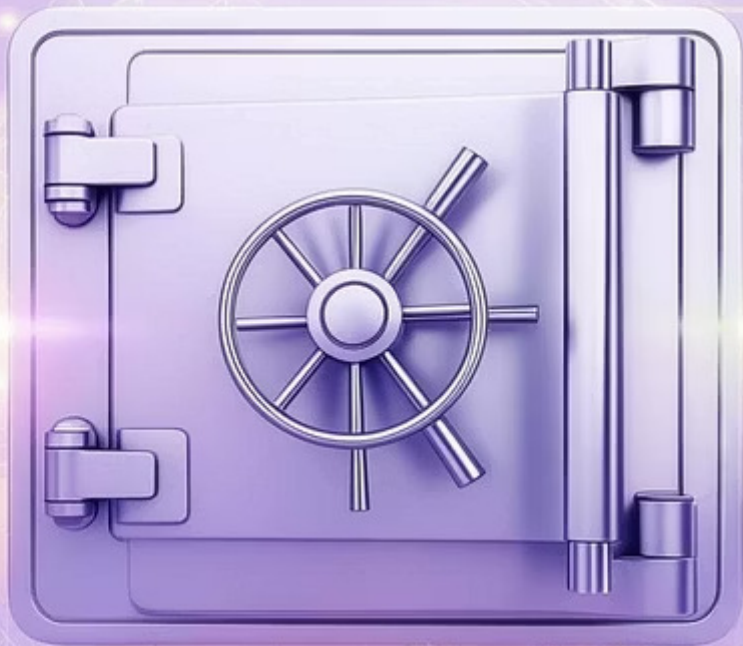




AI v MoyaKybeon: Kompletní přehled

verze 7.11.2025

1. Úvod

Proč jsme AI do MoyaKybeon přidali

Umělá inteligence je dnes všude – a je snadné v ní vidět buď zázrak, nebo hrozbu. My v MoyaKybeon ji vnímáme jinak: jako **praktického asistenta**, který pomáhá s rutinními úkoly, ale nikdy nepřebírá kontrolu.

Naším cílem bylo vytvořit **AI, která slouží lidem**, ne naopak.

Proto jsme ji zahrnuli do MoyaKybeon tak, aby její využití bylo bezpečné a v souladu se zákonnými i etickými principy.

Tento přehled shrnuje všechny důležité otázky, které o AI v MoyaKybeon zazněly – společně s odpověďmi, které vám pomohou pochopit, **co AI dělá, co nikdy dělat nebude, a jak chrání vaše data**.

Kapitola 2

Jak AI v MoyaKybeon funguje



Jaký je hlavní účel AI v aplikaci?

Hlavním účelem je urychlit vám práci. Pečlivě jsme vybrali scénáře, kde použití dává smysl.

Pro každý scénář jsme předdefinovali a odladili dotaz. Uživatel nikde nemá možnost pokládat své vlastní dotazy.

Seznam všech AI scénářů, ze kterého je jasně patrný účel každého dotazu, je uveden v nápovědě.



Bude AI rozhodovat sama, nebo jen poskytovat návrhy?

Jak je zajištěno, že uživatel může kdykoli přepsat nebo obejít doporučení AI?

Princip návrhu

V aplikaci je důsledně dodržen princip, že **AI pouze navrhuje možný obsah** a je na uživateli, aby návrh posoudil a dle svého úsudku upravil.

Žádná automatická změna

Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.

Fyzicky je to provedeno například tak, že je na přání uživatele pomocí AI předvyplněn obsah datových položek, které může uživatel ve formuláři dále libovolně editovat. Tato pole jsou po vyplnění pomocí AI barevně zvýrazněna, aby měl uživatel přehled, která pole neupravoval.

Jak v aplikaci vizuálně odlišíte "doporučení AI" od "finální hodnoty schválené uživatelem"?

Grafické odlišení

Doporučení vytvořená pomocí AI jsou ve formuláři graficky odlišená, dokud je uživatel neuloží nebo nezmění:

- seznamy a textová pole jsou **modře orámovány**
- ostatní položky jsou zvýrazněné **modrým fontem**

Ochrana existujících dat

Pokud už formulář obsahuje uživatelem zadané vstupy, nedochází k jejich přepsání doporučeními AI.

Hlídáte anomálie?

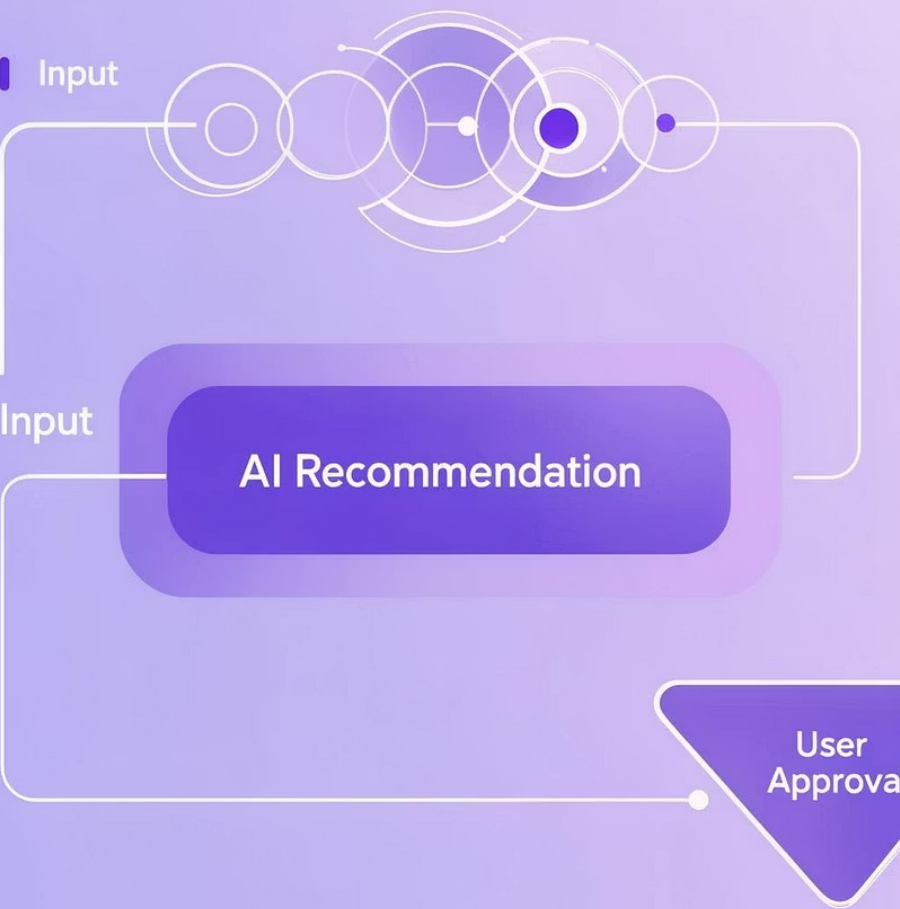
(např. že AI vyplňuje všechno na "nízký dopad")

Nehlídáme.

V aplikaci je důsledně dodržen princip, že AI pouze navrhuje možný obsah a je na uživateli, aby návrh posoudil a dle svého úsudku upravil.

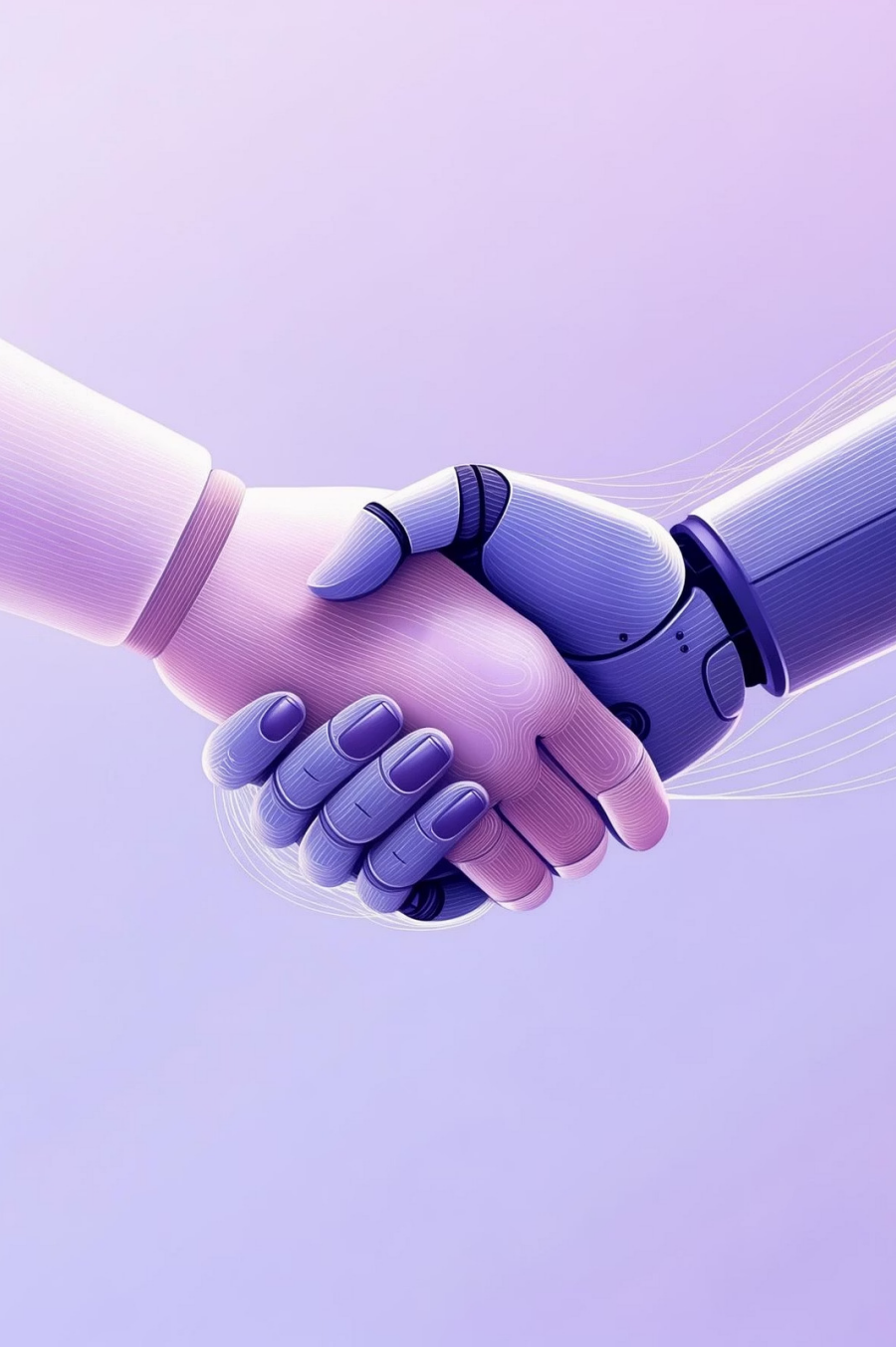
Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.





Lze exportovat report, který ukáže vstup → doporučení → schválení?

- i Nelze. V aplikaci je důsledně dodržen princip, že AI pouze navrhuje možný obsah a je na uživateli, aby návrh posoudil a dle svého úsudku upravil. Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.



Umožňuje aplikace doložit, že doporučení dala AI a nikoli živý uživatel?

Neumožňuje.

- ❑ V aplikaci je důsledně dodržen princip, že AI pouze navrhuje možný obsah a je na uživateli, aby návrh posoudil a dle svého úsudku upravil.

Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.

Jak bude AI fungovat v on-premise prostředí?

Pokud se organizace rozhodne využívat ve svém on-premise prostředí AI služby, bude nutné, aby nastavila síťovou komunikaci tak, aby bylo možné komunikovat se sadou služeb Microsoft Azure, které jsou pro API komunikaci s AI službami potřebné.





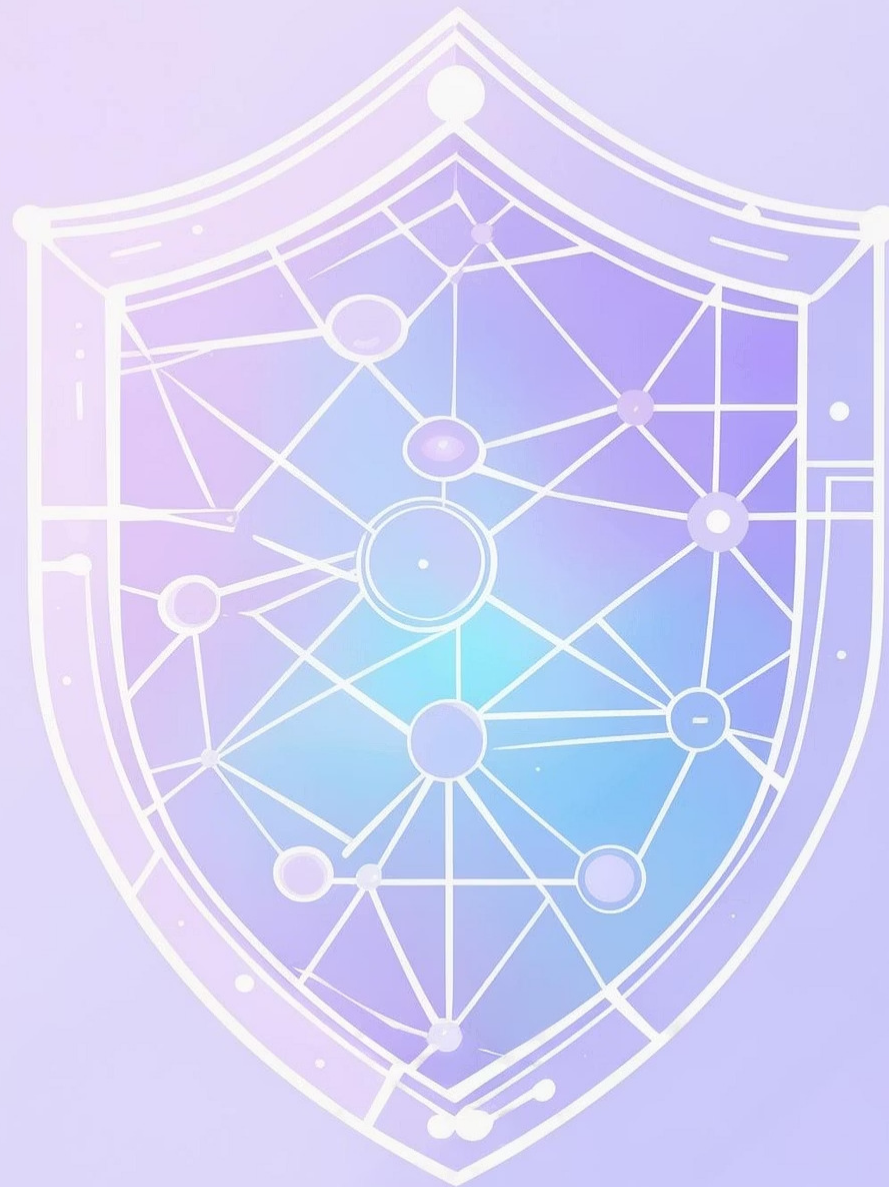
Můžeme mít MoyaKybeon bez AI?

Samozřejmě

Stačí nepovolovat (nebo kdykoliv později zakázat) příslušnou volbu **"Povolit AI asistenci"** v Zákaznické zóně - to je v kompetenci administrátora organizace.

Kapitola 3

Bezpečnosť a ochrana dát



Jaká data odchází do AI?

AI předáváme **nejmenší potřebné množství dat**, které je důležité pro kvalitní odpovědi.

01	02	03
Název zpracovávané položky	Kontext organizace	Potenciálně citlivé informace
odesíláme vždy	odesíláme pouze pokud je vyplněn. Předpokládáme, že se jedná o veřejně dostupné informace. Je na administrátorovi organizace, jaké informace vyplní.	(seznam primárních aktiv, seznam typových podpůrných aktiv, seznam základních podpůrných aktiv a seznam byznys procesů) tyto informace se odesílají pouze u některý dotazů a musí to být explicitně dovoleno administrátorem organizace.

Jinými slovy, v MoyaKybeon můžete používat umělou inteligenci bez toho, aby potenciálně citlivá data opustila MoyaKybeon a byla předána dál.

Kde data leží a o jaká data se jedná?

Uložení dat

Uložení dat předaných AI se řídí podmínkami společnosti OpenAI.

- [Podmínky používání pro EU | OpenAI](#)
- [Zásady ochrany osobních údajů | OpenAI](#)

Data v MoyaKybeon jsou uložena na MS Azure v rámci EU.

Ochrana citlivých dat

AI nepředáváme žádné citlivé osobní údaje a předání ostatních citlivých informací musí být explicitně povoleno.

Nikdy nejsou odesílána nejcitlivější data (například vlastní hodnocení hrozeb, zranitelností, aktiv, rizik, atp.) ani citlivá data o uživateli (například kdo je garantem nebo gestorem, osobní údaje, atp.)

 Data v MoyaKybeon jsou uložena na MS Azure fyzicky umístěném na území EU.

Může se k datům posílaným do AI dostat někdo jiný?

Jak jsou data chráněna před únikem, zneužitím nebo neautorizovaným přístupem?

Šifrování

Data jsou šifrována při přenosu (TLS) i při uložení (AES-256).

Přístupová kontrola

Přístup k datům mají pouze autorizovaní zaměstnanci za přísných podmínek.

Auditní logy

Systém zaznamenává přístupy a změny pro účely bezpečnostních auditů.

Anonymizace

U některých služeb (např. ChatGPT Enterprise) je obsah promptů anonymizován a **nepoužívá se pro trénink modelů**.

Detailní informace jsou k dispozici přímo od poskytovatelů:

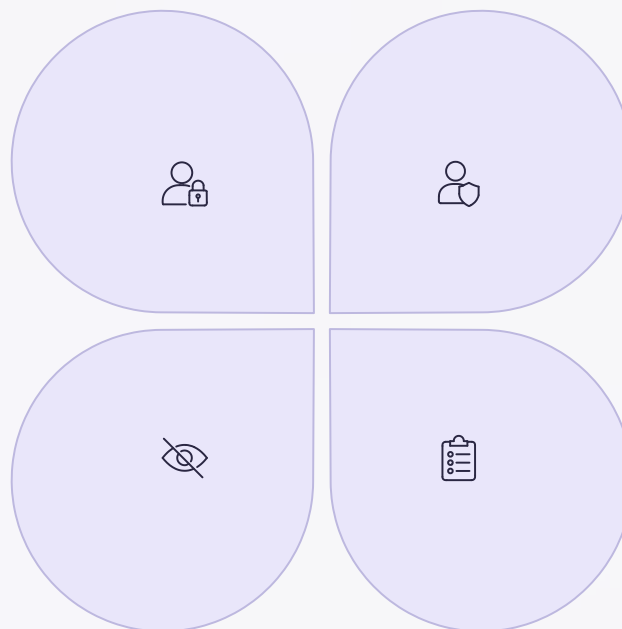
- Popis služby: [Azure OpenAI Service produktová stránka](#)
- Obchodní podmínky / smlouva o službě: [OpenAI Services Agreement](#)
- [Podmínky používání pro EU | OpenAI](#)
- [Zásady ochrany osobních údajů | OpenAI](#)

Jaká jsou opatření proti únikům?

Může AI odhalit citlivé údaje jiného uživatele?

Šifrování

Data jsou šifrována při přenosu (TLS) i při uložení (AES-256).



Přístupová kontrola

Přístup k datům mají pouze autorizovaní zaměstnanci za přísných podmínek.

Anonymizace

U některých služeb (např. ChatGPT Enterprise) je obsah promptů anonymizován a **nepoužívá se pro trénink modelů**.

Auditní logy

Systém zaznamenává přístupy a změny pro účely bezpečnostních auditů.

Detailní informace jsou k dispozici na webu OpenAI:

[Podmínky používání pro EU | OpenAI](#)

[Zásady ochrany osobních údajů | OpenAI](#)

Data, která jsou používána pro dotazy, jsou trojího typu:

- **předdefinovaná formulace dotazu** - sama osobě neobsahuje žádná důvěrná data
- **obecně známé informace**, které se o své společnosti rozhodne organizace sama zveřejnit
- **potenciálně citlivá data** jako jsou například názvy položek jednotlivých katalogů (například seznamy aktiv, hrozeb, zranitelností atp.) nebo číselníků.
Každá organizace se může rozhodnout, zda takováto data umožní odesílat.

Nikdy nejsou odesílána nejcitlivější data (například vlastní hodnocení hrozeb, zranitelností, aktiv, rizik, atp.) ani citlivá data o uživateli (například kdo je garantem nebo gestorem, osobní údaje, atp.).

Jsou data při přenosu a ukládání šifrována?

Ano

OpenAI zajišťuje ochranu dat z promptů pomocí:

- **Šifrování:** Data jsou šifrována při přenosu (TLS) i při uložení (AES-256).
- **Přístupová kontrola:** Přístup k datům mají pouze autorizovaní zaměstnanci za přísných podmínek.
- **Auditní logy:** Systém zaznamenává přístupy a změny pro účely bezpečnostních auditů.
- **Anonymizace:** U některých služeb (např. ChatGPT Enterprise) je obsah promptů anonymizován a nepoužívá se pro trénink modelů.

Detailní informace jsou k dispozici:

- Popis služby / co služba nabízí: [Azure OpenAI Service – produktová stránka](https://azure.microsoft.com/en-gb/products/openai/) (azure.microsoft.com)
- Obchodní podmínky / smlouva o službě (platí obecně pro OpenAI API, nutné ověřit přímo u Azure): [OpenAI Services Agreement](https://openai.com/policies/terms-of-use) (openai.com)
- [Podmínky používání pro EU | OpenAI](#)
- [Zásady ochrany osobních údajů | OpenAI](#)

Jak dlouho jsou doporučení AI uchovávána v logu nebo databázi?

Doporučení AI

Doporučení AI jako taková **neuchováváme**.

- Pokud je uživatel přepíše, hned zmizí
- Pokud je uživatel akceptuje, ukládají se jako běžné hodnoty zadané uživatelem

Auditní log

V auditním logu uživatelských aktivit je informace, že uživatel použil AI (**bez hodnot**).



Jak je vše zabezpečeno, pokud AI nepoužijeme (a API už tam je)?

Aplikace neposkytuje žádné API pro externí volání AI funkcí.

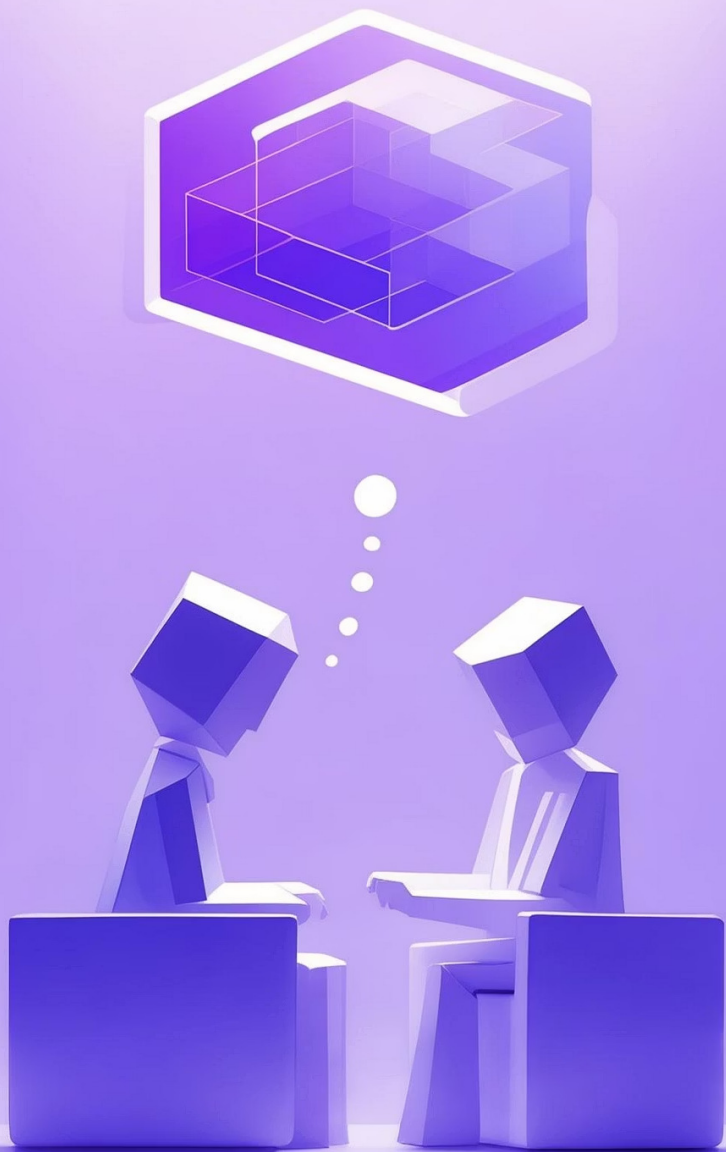
Naopak MoyaKybeon volá API MS Azure Services a teprve v rámci tohoto volání poskytuje data obsažená v promptu.



Kdy se poprvé odešlou data a jaká?

Data se odesílají pouze jako součást promptu, tj. **kdykoliv uživatel použije AI funkci.**

Detailně je pro každý dotaz popsáno v nápovědě, jaká data se odesílají. Samotnou aktivací AI funkcionality nedochází k odeslání dat.



Může se stát, že v jednom vlákně konverzují dva zákazníci?

Podle dokumentace poskytovatele služby Azure OpenAI Service, společnosti Microsoft, je to **vyloučené**.

Jaké kontexty se odesílají, pokud je uživatel ve více organizacích?

Je úplně jedno, jestli má uživatel přístup k jednomu nebo více prostředím. Odesílá se jen takový kontext, který odpovídá prostředí, ve kterém uživatel právě pracuje. A pouze, pokud je kontext vyplněn.



Jsou data použita k učení?

Nejsou

Kapitola 4

Prostředí, kde AI běží



Jaké nástroje AI třetích stran využíváte?

Používáme pouze nástroje třetích stran, a to výhradně ty, které jsou k dispozici prostřednictvím služeb v prostředí **Microsoft Azure (Azure AI Services)**:

Azure OpenAI Service

přístup k modelům jako GPT-4 a DALL·E

Azure AI Document Intelligence

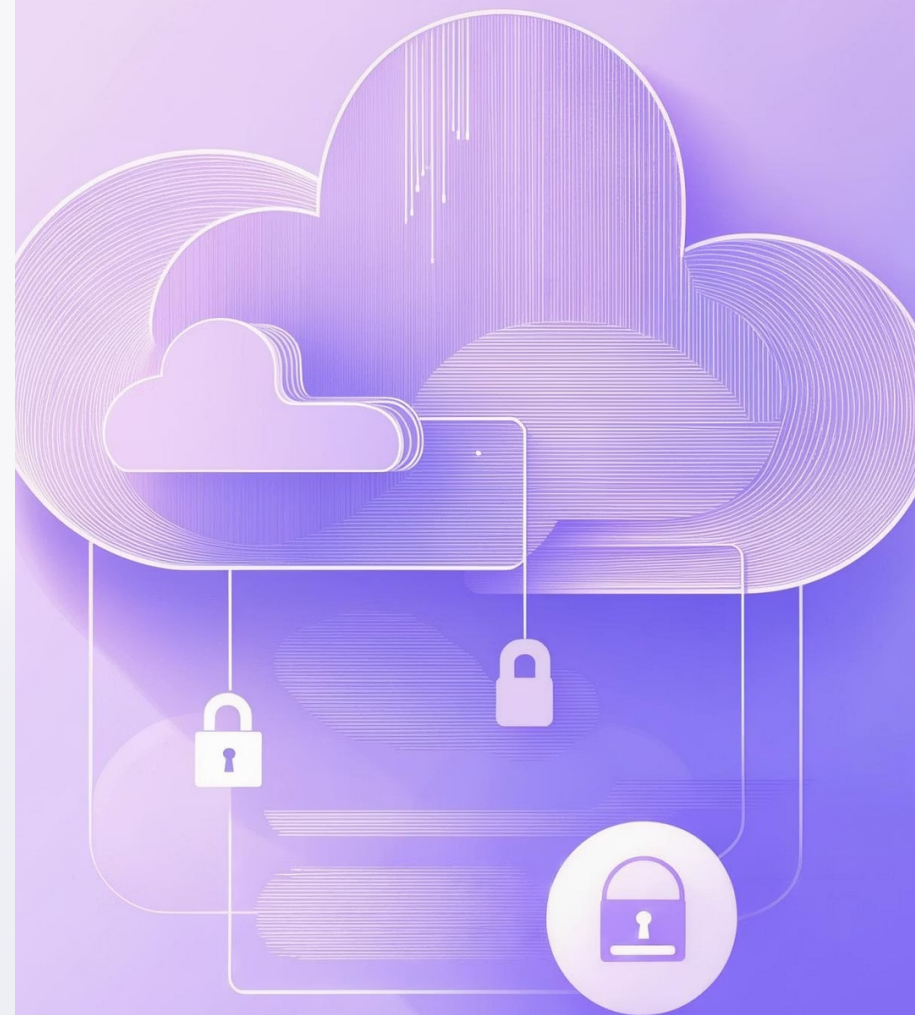
extrakce dat z dokumentů (formuláře, tabulky)

Zde jsou důležité odkazy k službě Azure OpenAI Service od Microsoft:

- Popis služby / co služba nabízí: [Azure OpenAI Service produktová stránka](#)
- Obchodní podmínky / smlouva o službě (platí obecně pro OpenAI API, nutné ověřit přímo u Azure): OpenAI Services Agreement

Jak zajišťujete, že AI bude průběžně aktualizovaná a bezpečná?

Používáme pouze služby [Azure AI Services](#), které jsou spravovány a prověřovány společností Microsoft, která zajišťuje jejich bezpečnost.



Kapitola 5

Používané modely a jejich vlastnosti



Na jakých datech byla AI trénována?

Používáme tyto modely:

- GPT-4o mini
- GPT-4.1

Základní údaje o trénování modelů:

Model	Znalostní cutoff	Typ dat	Bezpečnostní opatření
GPT-4o mini	Říjen 2023	Veřejná + licencovaná data	Filtrace, RLHF, expertní testy
GPT-4.1	Červen 2024	Veřejná + licencovaná data	Optimalizace pro praktické úlohy

Další informace:

- <https://openai.com/index/gpt-4o-mini-advancing-cost-efficient-intelligence/>
- <https://openai.com/index/gpt-4-1>

V případě, že zařadíme nový model, bude tato informace aktualizována.

Jak AI trénujete?

(provádíte vlastní trénink nebo používáte hotové modely?)

Neprovádíme žádné specifické trénování. Používáme již natrénované ověřené modely třetích stran.

Používáme tyto modely:

- GPT-4o mini
- GPT-4.1

Základní údaje o trénování modelů:

Model	Znalostní cutoff	Typ dat	Bezpečnostní opatření
GPT-4o mini	Říjen 2023	Veřejná + licencovaná data	Filtrace, RLHF, expertní testy
GPT-4.1	Červen 2024	Veřejná + licencovaná data	Optimalizace pro praktické úlohy

Další informace:

- <https://openai.com/index/gpt-4o-mini-advancing-cost-efficient-intelligence/>
- <https://openai.com/index/gpt-4-1>

V případě, že zařadíme nový model, bude tato informace aktualizována.



Jak často aktualizujete znalosti modelu v návaznosti na nové hrozby?

Model nespravujeme, tedy ani netrénujeme - používáme ho tak, jak je k dispozici.

Jak AI hodnotí hrozby a zranitelnosti – má napojení na externí databáze (ENISA, NÚKIB, CVE)?

Na základě svých "znalostí" a na základě vstupů poskytnutých v rámci promptu.
Aktivní propojení na tyto databáze jsme nebudovali.



Jak testujete, že AI není zaujatá?

Používáme pouze modely GPT-4o mini a GPT-4.1. Testování nezájatosti je prováděno jejich tvůrcem - společností Open AI. Detaily na webu <https://openai.com/>

Jak byla AI testovaná před nasazením?

(funkčnost, bezpečnost, red-teaming)

Používáme pouze nástroje třetích stran, a to výhradně ty, které jsou k dispozici prostřednictvím služeb v prostředí Microsoft Azure (Azure AI Services):

Azure OpenAI Service

přístup k modelům jako GPT-4 a DALL·E

Azure AI Document Intelligence

extrakce dat z dokumentů (formuláře, tabulky)

Testování samotné AI je tedy v kompetenci poskytovatele AI služeb.

Testování technické funkčnosti komunikace s AI je samozřejmě standardní součástí vývojového cyklu aplikace.

Jak budete sledovat její chování v provozu?

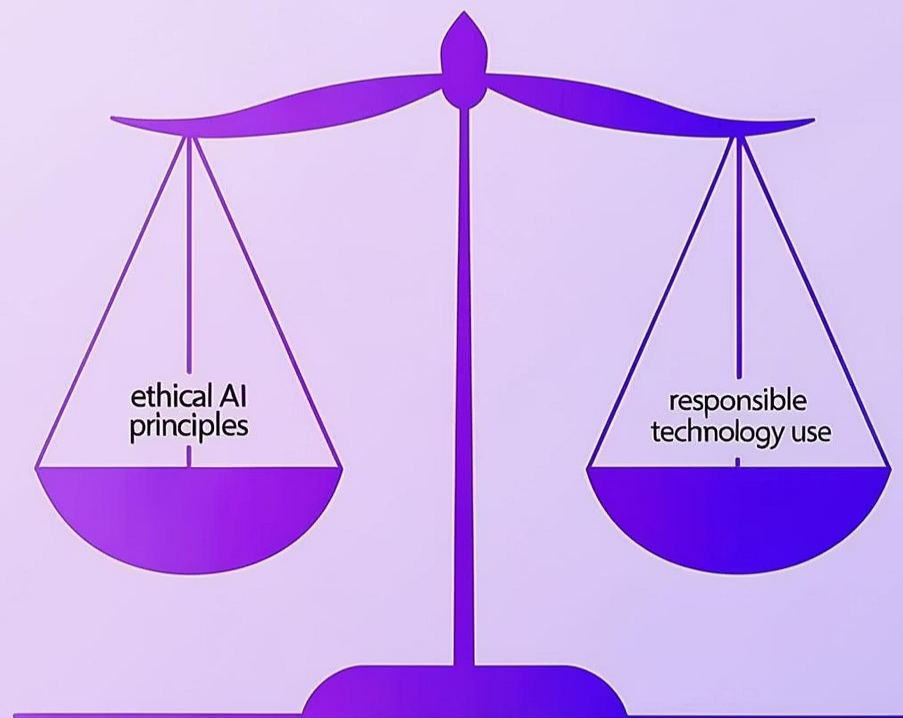
(monitoring anomálií, výstupy mimo logiku)

V aplikaci je důsledně dodržen princip, že AI pouze navrhuje možný obsah a je na uživateli, aby návrh posoudil a dle svého úsudku upravil. Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.

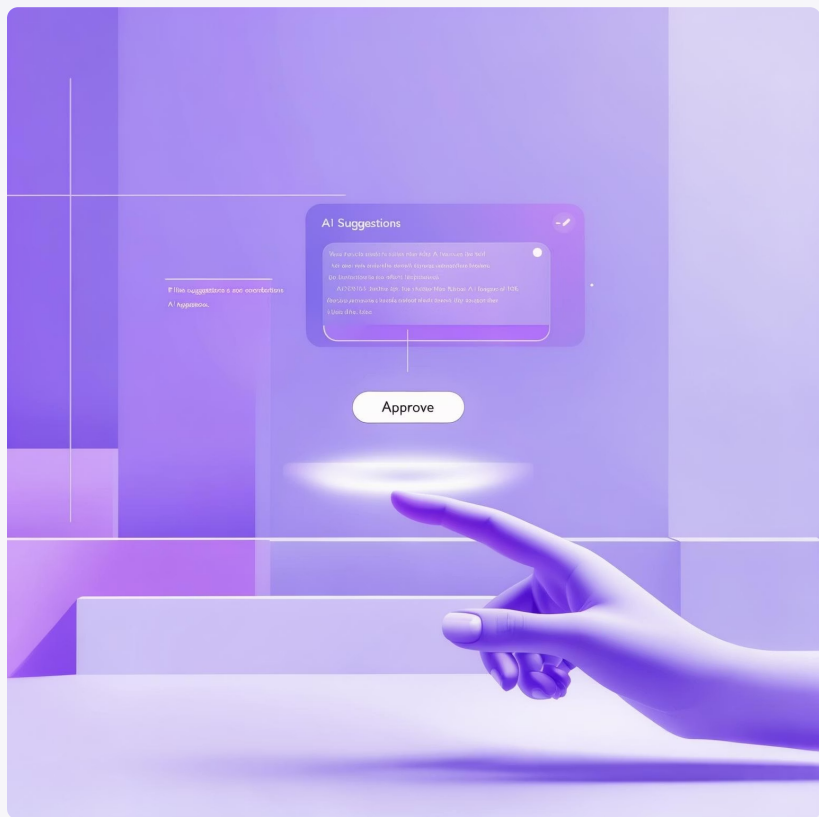
Cíleně tedy sledovat a vyhodnocovat chování AI nebudeme, nicméně pokud v rámci pravidelného testování, popř. hlášení od uživatelů, na anomálii narazíme, budeme se ji věnovat a pokud to bude v našich silách, pokusíme se upravit prompt tak, aby byla poskytována lepší kvalita výstupů.

Kapitola 6

Etika, odpovědnost a AI Act



Kdo nese zodpovědnost za chyby, pokud AI něco vyplní špatně?



V aplikaci je důsledně dodržen princip, že **AI pouze navrhuje možný obsah** a je na uživateli, aby návrh posoudil a dle svého úsudku upravil.

Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.

Jak byla zohledněna GDPR pravidla? (právo na výmaz, minimalizace dat)

Komunikace s AI **zásadně žádná osobní data neobsahuje**.

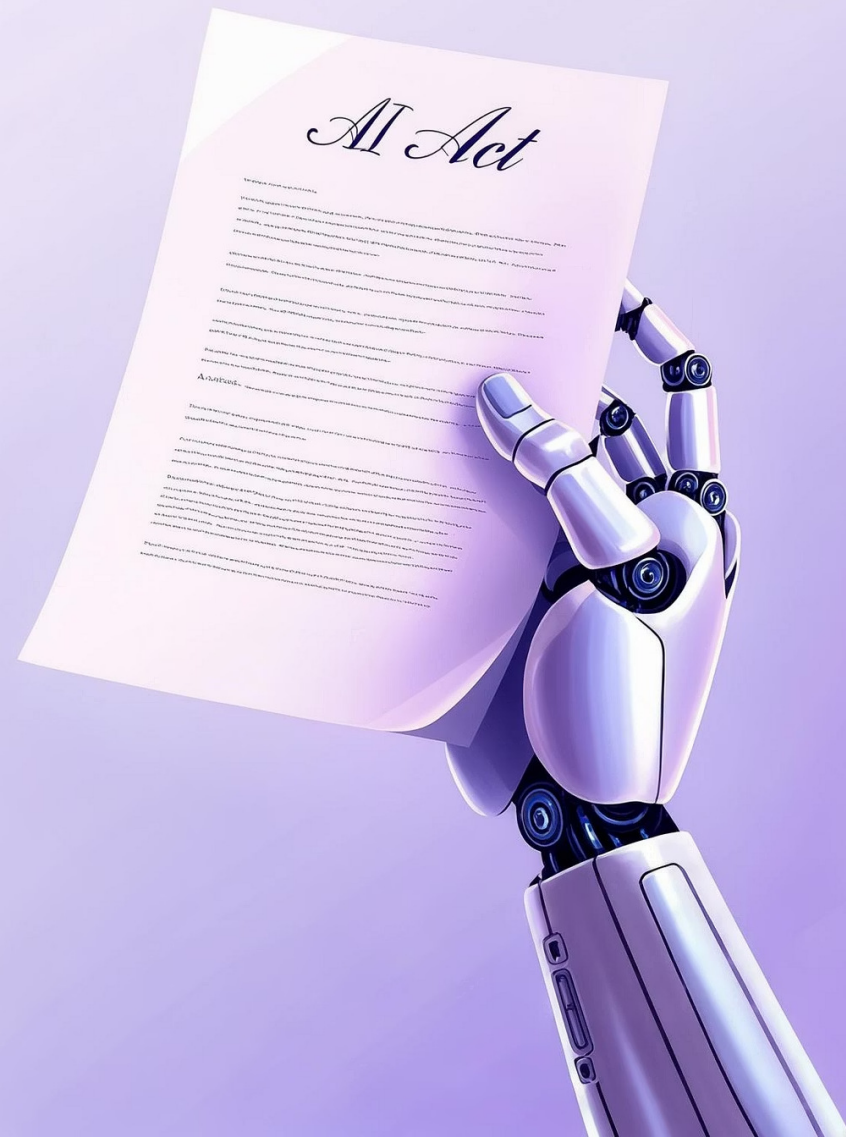
Jedinou možnou výjimkou je, pokud se organizace rozhodne do obecného popisu sebe sama vložit například kontaktní údaje. Což určitě nedoporučujeme a pro účely komunikace s AI to nepřináší žádnou přidanou hodnotu.

- ❑ Vytvoření správného popisu organizace je v její kompetenci a zodpovědnosti. Doporučujeme držet se dodaného vzorové struktury.



Jak byl zohledněn AI Act? Jste v souladu?

AI act pravidelně **sledujeme** a reagujeme na něj



Kapitola 7

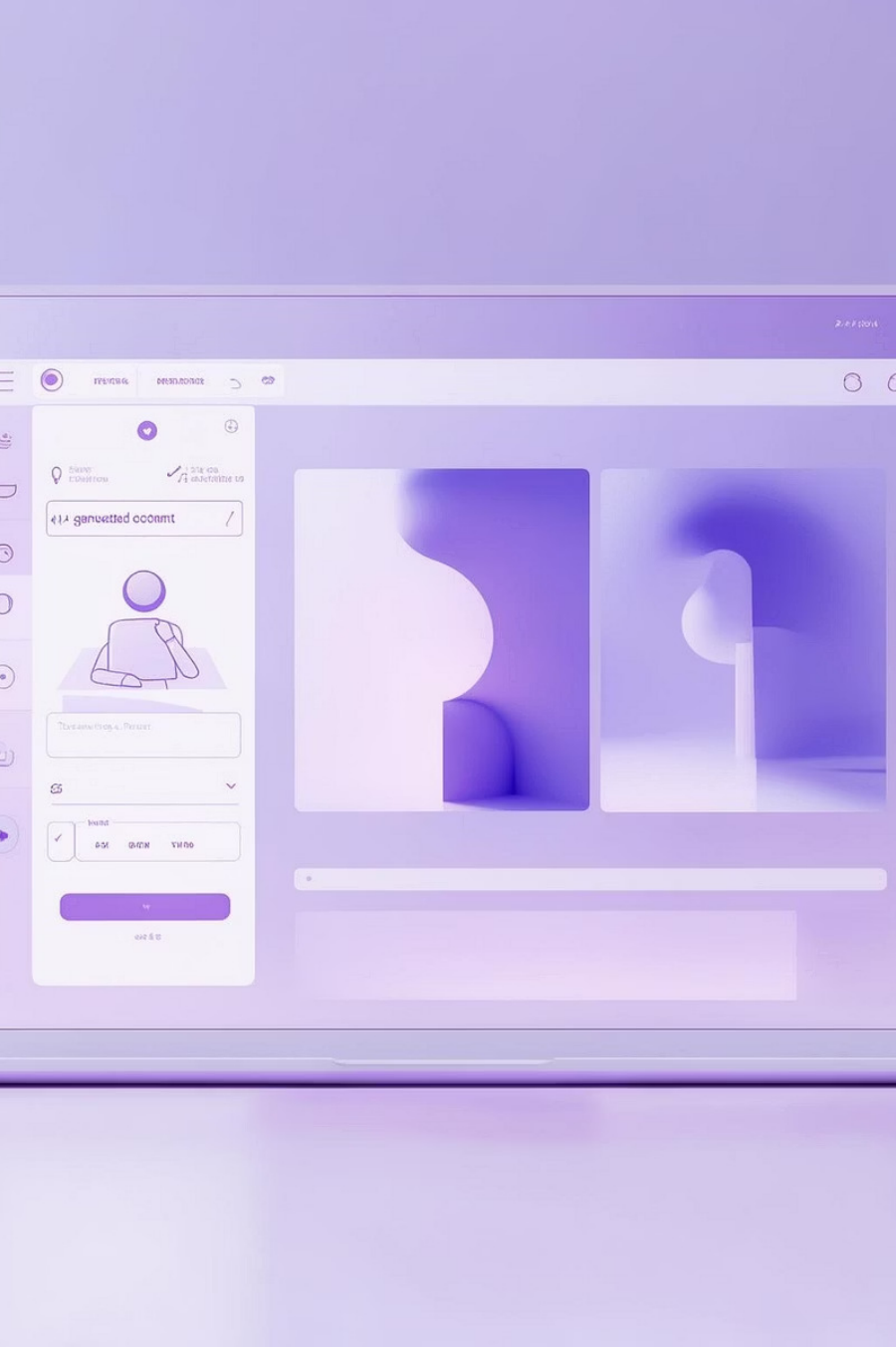
Transparentnost a auditovatelnost





Jste schopni doložit, jak AI došla k určitému výsledku?

Z principu **není možné** při použití systému založeného na neuronové síti analyticky doložit daný výsledek.



Jaké mechanismy existují pro validaci výsledků AI uživatelem?

Aplikace nenabízí žádné specifické mechanismy validace výsledků AI.

V aplikaci je důsledně dodržován princip, že AI pouze navrhuje možný obsah a je na uživateli, aby návrh posoudil a dle svého úsudku upravil.

Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.

Existuje plán pravidelných bezpečnostních auditů funkce AI?

Ano

Je to součást bezpečnostních auditů.



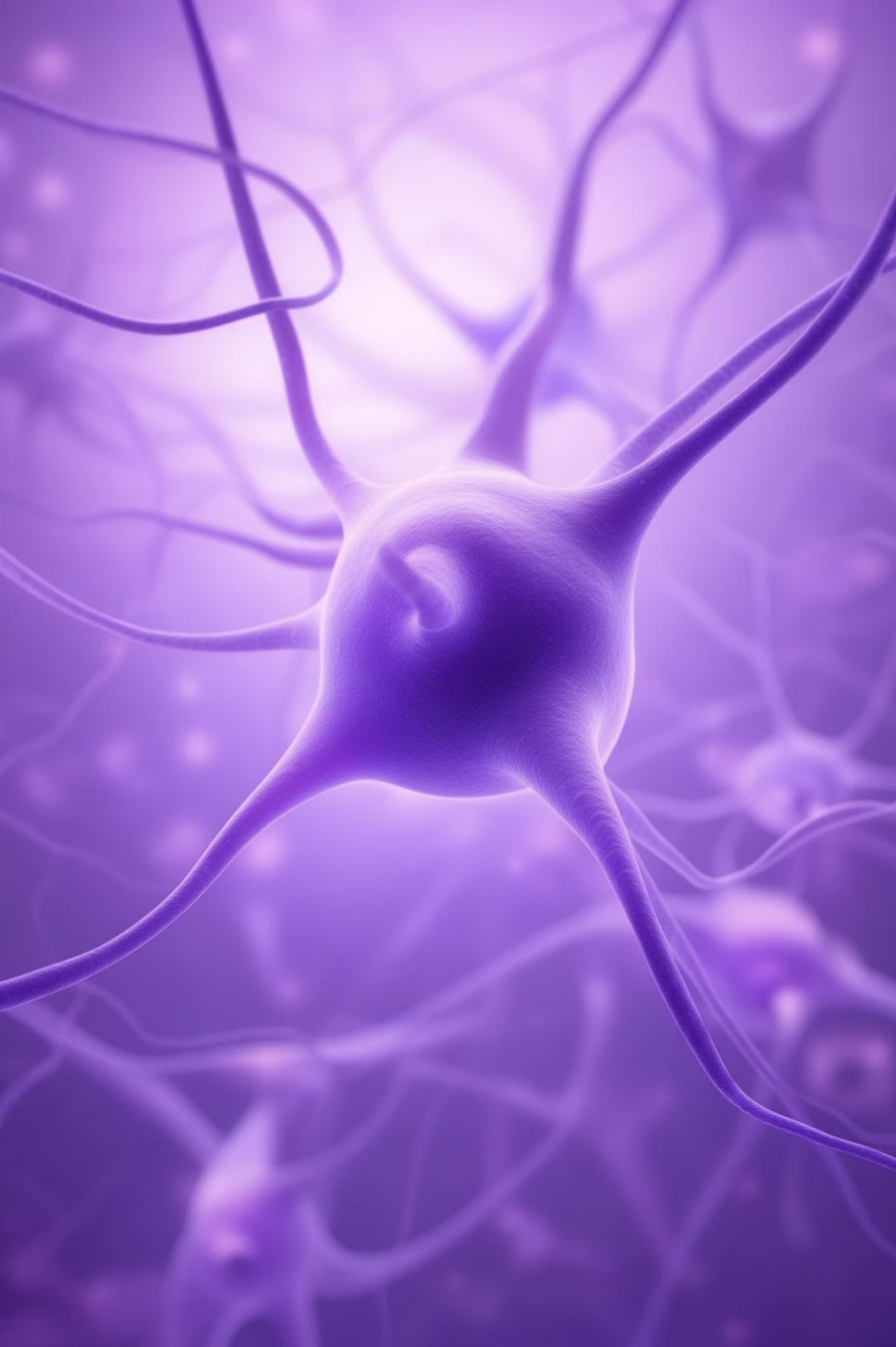
Máte mechanismus zpětné vazby od uživatelů k výstupům AI?

SOS tlačítko

Pokud nám chce uživatel poskytnout zpětnou vazbu, popř. nahlásit problém, má všude v aplikaci **tlačítko SOS**, které je přímo určené pro komunikaci ohledně technických problémů, nejasností nebo návrhů na vylepšení aplikace.

Aplikace sama o sobě nedisponuje specifickou funkcionalitou poskytování zpětné vazby pouze k návrhu AI. To také znamená, že žádná zpětná vazba není odesílána do AI služby.

V aplikaci je důsledně dodržen princip, že AI pouze navrhuje možný obsah a je na uživateli, aby návrh posoudil a dle svého úsudku upravil. Bez vědomého rozhodnutí uživatele nedochází k žádné modifikaci datového obsahu záznamů v Kybeonu.



Jak zajistíte, aby AI nemohla systematicky zkreslovat výsledky?

(např. vždy podhodnocovat hrozby)



Průběžně kontrolujeme výstupy AI a jsme připraveni upravit předdefinované dotazy v případě, že identifikujeme sníženou kvalitu odpovědí.



Zároveň testujeme nové jazykové modely a průběžně je budeme zařazovat, pokud budou poskytovat výsledky s vyšší kvalitou než aktuálně používané.

Kapitola 8

Správa a kontrola ze strany zákazníka



Jak vypnout nebo zakázat AI v MoyaKybeon?

Aktivaci/deaktivaci je možné provést v Zákaznické zóně → Nastavení → AI nastavení

Tímto způsobem máte plnou kontrolu nad používáním AI v aplikaci MoyaKybeon a můžete si přizpůsobit její chování podle vašich potřeb.



Agendy

Má organizace

Nastavení

Uživatelé

Role

Bezpečnost

Milníky

Obchodní podmínky

Ochrana osobních údajů

Nastavení

Nastavení organizace

Základní nastavení organizace

AI nastavení

Nastavení umělé inteligence pro asistenci



☒ Automatické schvalování záznamů

☐ Vynutit dvoufaktorovou autentizaci pro organizaci

☒ Povolit AI asistenci

☒ Využívat v AI promptu vaše data, která jste zadali v MoyaKybeon (detaily v nápovědě).

Kontextové informace o naší organizaci

1) Základní údaje o organizaci
Název organizace:
Perspia a.s.
Odvětví:

 Jak poskytnout kontextové informace o naší organizaci?

Co když administrátor dočasně AI povolí a pak zase vypne – odešlou se do AI nějaká data?

Data se odesílají **pouze jako součást promptu**, tj. kdykoliv uživatel použije AI funkci.

Samotnou aktivací nebo deaktivací AI funkcionality **nedochází k odeslání dat**. Detailně je pro každý dotaz popsáno v nápovědě, jaká data se odesílají.



Jak poskytovat zpětnou vazbu nebo nahlásit problém?

Pomocí SOS tlačítka přímo v aplikaci.

