
AI Sandbox

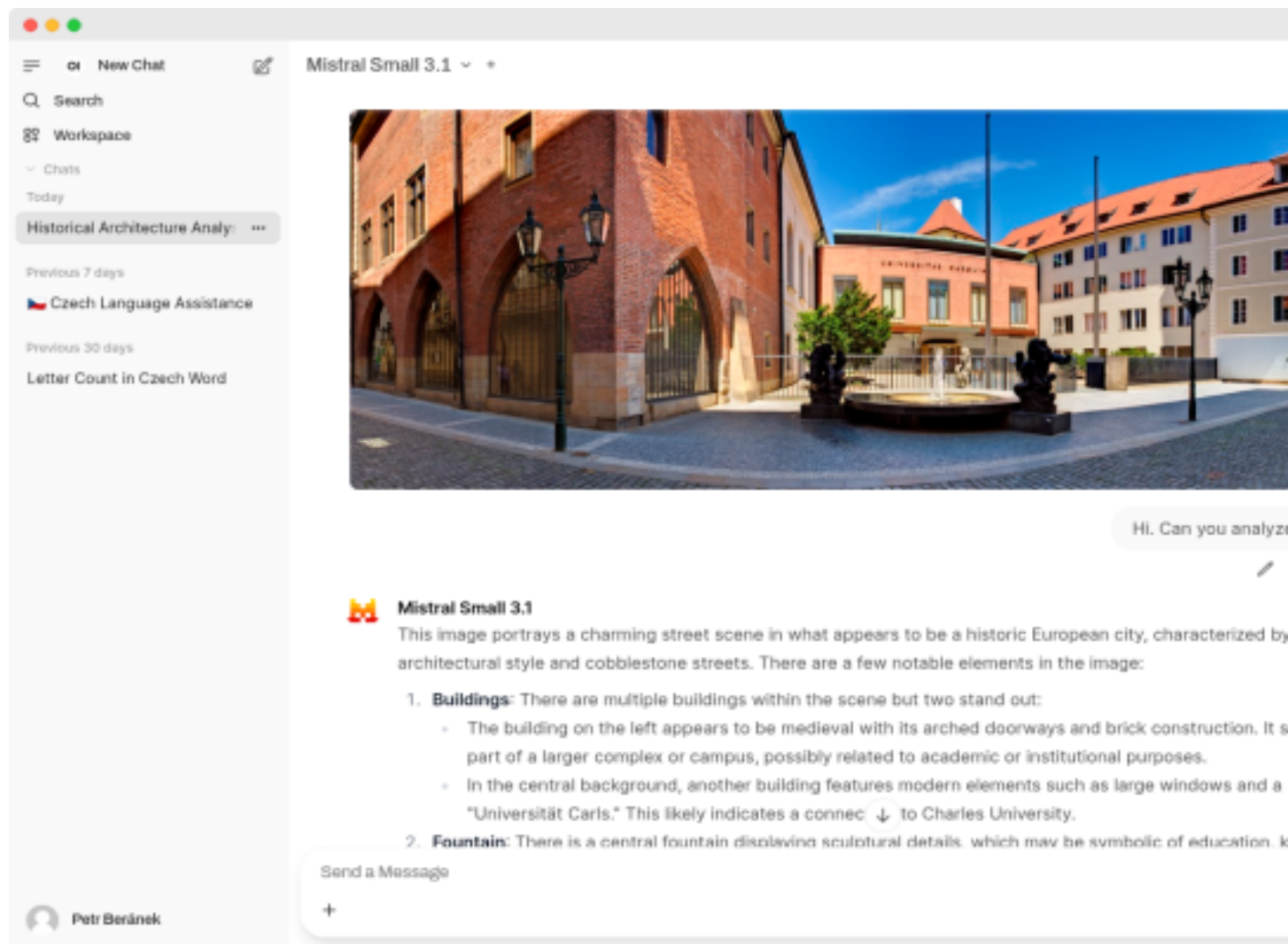
Co je AI Sandbox

Účelem aplikace AI Sandbox je **poskytnout zaměstnancům UK chatbota pro bezpečné chatování s modely generativní AI**. Vkládaná data nejsou používána k trénování těchto modelů.

Funkcionalita je v tuto chvíli minimalistická (další funkce budeme zpřístupňovat postupně):

- **chatování**
- **multimodální vstup**: text, obrázky, experimentální podpora pro Speech-to-Text (primárně angličtina)
- **tvorba jednoduchých asistentů** (obdoba GPTs v ChatGPT)
- **code interpreter a spouštění kódu** (běžové prostředí Pydide)

Aplikace je určena pro interakci na úrovni běžného chatu. Pokud potřebujete programatický **přístup k modelům přes API**, kontaktujte ai@cuni.cz .



Obrázek výše: Jako uživatelské rozhraní sandboxu slouží komponenta Open WebUI.

Jak se přihlásit

	Aplikace je ve fázi pilotního provozu. Přednostní přístup mají členové pracovních skupin (Širší prac. skupina při prg.ai; Generativní AI na UK; UISK Research Group). Pro bližší informace kontaktujte ai@cuni.cz. Přihlášením do aplikace berete na vědomí, že komunikujete s generativní AI, která může generovat faktické chyby (tzv. "halucinace"). Při používání aplikace jste vázáni dodržovat platné zákony, podmínky použití (bude doplněno) a vnitřními předpisy Univerzity Karlovy. V případě jejich porušení Vám může být přístup do aplikace zablokován. Třebaže je Sandbox nastaven tak, aby nedocházelo k trénování na vkládaných datech, v rámci pilotního provozu nekládejte data nad úroveň Veřejná, viz tabulka Kategorizace dat.
--	--

1. Ve webovém prohlížeči přejděte na stránku sandbox.ai.cuni.cz
2. Klikněte na **přihlášení přes CAS**.
3. Po úspěšném přihlášení budete přesměrováni do rozhraní **Open WebUI**. Poté Vám přístup musí **schválit administrátor** – zpravidla do 1 pracovního dne.

Uživatelská podpora

Se základními dotazy se prosím obračejte na kanál [AI Sandbox v MS Teams](#) ať nemusí být stejné dotazy zodpovídány opakovaně. Případně lze kontaktovat ai@cuni.cz.

Dostupné modely

Využívání modelů - zejména externích (placených) - může být limitováno. Uživatelé budou o případných limitech informováni.

Lokální modely

Název	Stručný popis	Vstup	Výstup
Llama 4 Scout	A 109B language model from Meta. Its efficiency and versatility make it well-suited for diverse natural language processing tasks. Features vision capabilities for image description generation.	text, obrázky	text
DeepSeek R1 0528*	A 685B reasoning-optimized language model from Deepseek AI. Excels at complex tasks including mathematics, logical reasoning, and code generation.	text	text

* V souladu s [Varováním před některými produkty společnosti DeepSeek](#) je model nasazen lokálně bez možnosti komunikace se servery výrobce. Model je k dispozici na vyžádání pro bezpečnostní testování a analýzu samotného modelu, nikoliv pro běžnou práci.

Následující modely jsou **experimentální (Experimental)** a mohou být v budoucnu odebrány nebo změněny. Doba odezvy bývá pomalejší. Zpravidla stačí počkat.

Název	Stručný popis	Vstup	Výstup
gpt-oss-120b	A 120B language model from OpenAI with strong reasoning and instruction following capabilities.	text	text
MedGemma	A 27B language model from Google designed specifically to understand and process medical text.	text, obrázky	text
Aya Expanse	A 32B Q8 multilingual model from Cohere, trained to perform well across 23 languages, including Czech.	text	text
Phi-4	A 14B Q8 model from Microsoft, trained on a mix of synthetic datasets, filtered public web content, academic books, and Q&A datasets.	text	text

Následující modely byly označeny jako **dále nepodporované (Deprecated)** a v budou v dohledné době odebrány. Generování může být velmi pomalé.

Název (počet parametrů v miliardách)	Vstup	Výstup
Llama 3.3 (70b)	text	text
Gemma 3 (27b)	text, obrázky	text
Command A (111b)	text	text
Mistral Small 3.1 (24b)	text, obrázky	text

Externí modely

	Při využívání externích modelů se na Vás vztahují podmínky použití dané jejich poskytovatelem.
--	---

OpenAI

[OpenAI Services Agreement](#) (AI Sandbox využívá jejich API platformu)

Pozor: Vzhledem k aktuálnímu soudnímu nařízení **musí OpenAI ukládat data na neomezeně dlouhou dobu a nemůže být plně v souladu s ustanoveními GDPR.** Více viz [jejich vyjádření](#).

Název	Vstup	Výstup
GPT-5 Chat	text, obrázky	text
ChatGPT-4o	text, obrázky	text

Následující modely byly označeny jako **zastaralé (Deprecated)** a v budou v dohledné době odebrány.

Název	Vstup	Výstup
o4-mini	text, obrázky	text

GPT-4.1	text, obrázky	text
GPT-4.1 mini	text, obrázky	text

Anthropic

[Commercial Terms of Service](#) (AI Sandbox využívá jejich API platformu)

Název	Vstup	Výstup
Claude Sonnet 3.7	text, obrázky	text
Claude Haiku 3.5	text, obrázky	text

Jak je to s bezpečností dat

Všechny modely označené jako lokální (Local) běží na infrastruktuře partnerské organizace [e-INFRA CZ](#) a data (vstupy a výstupy) neopouští jejich servery. Vstupy a výstupy jsou logovány pouze po dobu běhu daného serveru.

Modely označené jako externí (External) běží na serverech 3. strany (např. OpenAI), a veškerá data z daného chatu (tj. celý chat) jsou přenášena ke zpracování k nim. Tyto 3. strany se ve svých obchodních podmínkách zavazují netrénovat své modely na vkládaných datech. Bližší informace naleznete výše v sekci *Dostupné modely - Externí modely*.

Aplikace Open WebUI ve výchozím nastavení vstupy a výstupy neloguje. Příležitostně se může stát, např. v případě chybových stavů, že vstupy a výstupy mohou být dočasně uloženy, dokud není aplikace restartována – obvykle s nasazením nové verze. K těmto logům mají přístup pouze systémoví administrátoři a nejsou přenášeny nikam jinam.

Uložené konverzace jsou uloženy v databázi hostované v rámci infrastruktury e-INFRA CZ. Administrátoři jsou oprávněni konverzace číst pouze v odůvodněných případech: (1) při poskytování technické podpory, (2) vyšetřování potenciálního zneužití platformy nebo (3) z důvodů vyžadovaných zákonem. Když je konverzace smazána, měla by být také odstraněna z databáze – nicméně administrátoři e-INFRA nezávisle neověřili, zda Open WebUI plně implementuje toto chování. Databáze je zálohována do úložiště S3 na CESNET s dobou uchování 30 dní, což znamená, že starší zálohy jsou po 30 dnech smazány. Teoreticky bude smazaná konverzace zcela vymazána v tomto časovém okně. Opět, přístup k tomuto systému je omezen pouze na administrátory.

Všichni administrátoři e-INFRA CZ mají podepsanou NDA (Non-disclosure agreement).

Další informace

Tento dokument vychází z <https://docs.cerit.io/en/docs/web-apps/chat-ai>