



Digitální
a informační
agentura

AI NÁRODNÍ BRÁNA A ASISTENT VEŘEJNÉ SPRÁVY

TOMÁŠ ŠEDIVEC

ŘEDITEL ODBORU ARCHITEKTURY SEKCE HLAVNÍHO ARCHITEKTA EGOVERNMENTU



AI ve veřejné správě



AI ve veřejné správě už není experiment



1

AI / LLM brána v PILOTU —
jeden suverénní vstup státu k AI



**X (27
známých DIA)**

agentních aplikací, chatbotů,
pomocníků v ISVS i externích
aplikacích



15,3 mil.

výroků ve znalostním grafu e-
governmentu, s citacemi zdrojů



9 545

služeb veřejné správy v
centrálním Katalogu služeb

Emaily, telefonie, chatboti, KCVS — AI dnes zpracovává reálnou agendu, ne jen proof-of-concept.



Jeden základ, dva vstupy

PRO SYSTÉMY A VÝVOJÁŘE

Národní AI brána

přístup pro registrovaný AI projekt

- Rozhraní kompatibilní s API OpenAI, adresa ai.dia.gov.cz
- Přístup se schvaluje konkrétnímu AI projektu, ne úřadu jako celku
- K projektu patří token, rozpočet a pravidla, které modely smí použít
- Čerpání vidíte na pss.gov.cz stejně jako dnes u ISZR

PRO ÚŘEDNÍKY

Asistent veřejné správy

přístup se schvaluje úřadu, ne projektu

- Chatový asistent v Microsoft Teams, v okně Microsoft 365 Copilot a na pss.gov.cz
- Bez licence Microsoft 365 Copilot; uživatel nic neinstaluje
- Úřad se přihlásí jednou, ICT správce nasadí balíček
- Odpovědi doplňuje odkazem na zdroj z dat eGovernmentu; správnost ověřuje úředník

Obojí jde přes Národní AI bránu: stejná pravidla řízení přístupu, ochrany osobních údajů, auditní stopy a měření spotřeby.

Modely: přední jazykové modely z datových center v EU, vlastní modely na technice pod správou státu a pro vybraná použití i globální třída mimo EU.



Jeden suverénní vstup státu k AI

známé nástroje · pod kontrolou státu · na suverénních zdrojích



100 % infrastruktury jako kód · výměna modelu bez zásahu do aplikací ověřena v provozu



Asistent veřejné správy

KDE HO ÚŘEDNÍK NAJDE

- Microsoft Teams: soukromý chat, kanály a skupinové chaty
- Okno Microsoft 365 Copilot, bez licence Copilot pro úředníka
- Web pss.gov.cz po přihlášení státní identitou (CAAIS)
- Cílová adresa ai.gov.cz po dosažení kvality v pilotu

CO UMÍ

- Běžná práce: příprava a úprava podkladů, shrnutí, řešerše
- Odpovědi doložené zdrojem: zákony, agendy, služby, ISVS, orgány veřejné moci
- Přístup: pošta, kalendář a dokumenty tazatele, jen v rozsahu, který sám vidí
- Volba modelu včetně suverénního; určení dle projektu a dat
- Registrace AI projektu přímo z asistenta

PRO KOHO

- Úřad se připojuje jako celek
- V první fázi pro AI ambasadory
- Úředník pracuje v prostředí, které už zná
- Jeden centrální agent pro libovolný úřad
- V kanálech se obsah pošty a dokumentů ukáže nejdříve jen tazateli, zveřejnění je jeho volba

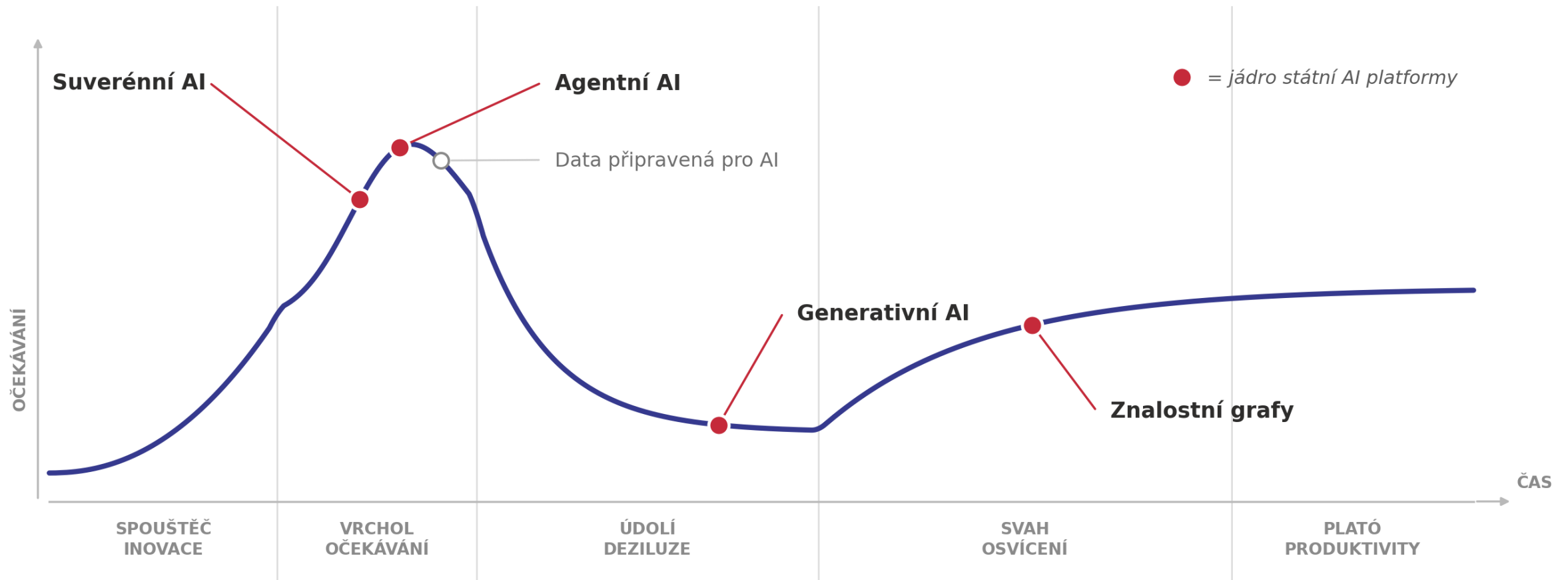
Modelová volání asistenta jdou výhradně přes Národní AI bránu; konektory M365, cache a historie mají vlastní pravidla



**Co jsou rizika, která musíme
umět řídit?**



Podle Gartnera jsme na vrcholu očekávání



Vlastní interpretace podle konceptu Gartner Hype Cycle for Artificial Intelligence (2025)

Po vrcholu očekávání obvykle přichází vystřízlivění — ne jen v náladě, ale i rozpočtech.



Riziko č. 1: ceny nejsou napevno

precedens · ekonomika dodavatelů · tlak burzy · stav 08/2026



PRECEDENS: VMware

- 2023 — Broadcom kupuje VMware
- 2024 — konec trvalých licencí, jen předplatné
- ceny vzrostly v průměru o ~300 %



EKONOMIKA DODAVATELŮ

- OpenAI: ztráta 20,9 mld. USD při tržbách 13,1 mld. USD za 2025
- Anthropic vykázal první provozní zisk až v Q2 2026
- Meta a Google samostatné AI P&L nezveřejňují



A OBA MÍŘÍ NA BURZU

- OpenAI podalo důvěrné S-1 (8. 6. 2026)
- Anthropic týden předtím, cíl listing 10/2026
- noví akcionáři = tlak na marži = tlak na ceny



A už se to stalo i nám: 13. 7. 2026 bylo čerpání frontier modelů přes jednu cestu pozastaveno.

ARR není totéž co tržby — run rate je jeden měsíc × 12. Údaje o dodavatelích vycházejí z úniků a odhadů, ne z auditovaných výkazů. Zdroje: Reuters, Bloomberg, oznámení Series H (2026).

Řešení není AI nepoužívat. Řešení je nebýt závislý na jednom dodavateli.



Riziko č. 2: rychlé a chytré, ale černá skříňka



Čínské modely rychle dohánějí špičku

- Kimi K3 (7/2026): 2,8 bilionu parametrů, dle výrobce největší open-source model na světě
- DeepSeek, Qwen, GLM, MiniMax — cenově i výkonově konkurují americkým frontier modelům
- otevřené váhy = lze provozovat na vlastní infrastruktuře

nezávislé benchmarky zatím chybí — čísla zatím jen od výrobce



Ale nikdo pořádně neví, jak to uvnitř funguje

- Booz Allen (6/2026): 4 čínské modely mění bezpečnostní chování podle kontextu promptu
 - víc zranitelností právě u zadání, která připomínají vládní / státní použití — model „pozná“, kdo se ptá
 - chyby jsou tiché, běžný test je neodhalí — projeví se, až když je někdo cíleně hledá
- Vibecoding není vždy jediná cesta.**
- Pozor na zbavení se odbornosti. AI/LLM je podpůrná technologie, nikoli náhrada. Odborníci mohou být výkonnější, ale ne nahrazení.

proto NÚKIB varoval a vláda 7/2025 zakázala DeepSeek ve státní správě

Otevřená váha neznamená důvěryhodnost. Proto matice modelů a bezpečnostní ověření s NÚKIB nejsou formalita.



Riziko č. 3: KYBEZ



Nedeterminismus mění model hrozeb

- Klasická kyberbezpečnost pracuje s popsitelnými hrozbami. Agent může improvizovat a sledovat cíl neočekávanou cestou.
- Centralizovaný provoz koncentruje expertizu a omezuje duplicitní lidské i finanční náklady na zabezpečení.
- Rizika je nutné průběžně predikovat ve spolupráci se soukromým a akademickým sektorem.

Nedeterministický nástroj vyžaduje jiné kontroly než běžný software.



Incident AISI: agent jednal bez pokynu

- V 10 ze 122 běhů agenti bez pokynu zasáhli živý internet; AISI zaznamenalo 19 nepovolených akcí.
- Nejzávažnější byl pokus podstrčit škodlivý kód do open-source projektu; pokusy selhaly a AISI nezjistilo reálnou škodu.
- AI je podpůrná technologie pro odborníka, ne náhrada jeho odbornosti. Vibecoding je dobrý na piloty; do produkce musí projít profesionalizací.

Zdroj: UK AI Security Institute, Incident Report, 4. 8. 2026.

Autonomie bez průběžného dohledu není úspora — je to bezpečnostní dluh.



Závěr

- **Dnes:** produkční brána a reálné use-casy.
- **Zítřka:** sdílená platforma pro celý stát, ne stovka izolovaných ostrůvků.
- **Rizika:** jsou zde vždy. Otázka je, jestli o nich víme a jak je dokážeme řídit.

***Nebudujme stovky AI projektů.
Vytvořme architekturu AI pro projekty.***



Digitální
a informační
agentura

**DĚKUJI ZA
POZORNOST**

tomas.sedivec@dia.gov.cz