Digitální
a informační
agentura

AI VE VEŘEJNÉ SPRÁVĚ a UV589/2026

TOMÁŠ ŠEDIVEC

ŘEDITEL ODBORU ARHCITEKTURY 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

KDO

Občané a úředníci

kontaktní kanály, klient, Teams

Úřady a jejich systémy

eDoklady, NIA, IAR, +
libovolný úřad

Národní AI brána

jeden kontrolovaný vstup státu

- **řízení přístupu — per úřad i uživatele**
- **ochrana dat (DLP) — pseudonymizace / anonymizace**
- **měření a limity nákladů, auditní stopa interakcí**
- **napojení libovolného úřadu možné už dnes**

KDE TO BĚŽÍ — suverénní zdroje

Vlastní GPU pod správou DIA

vlastní modely, běží dnes

Frontier modely

EU data zone, governed proxy, přímé kontrakty

SPCSS / on-prem alternativa

nejvyšší míra suverenity, v přípravě

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, rešerše
- 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

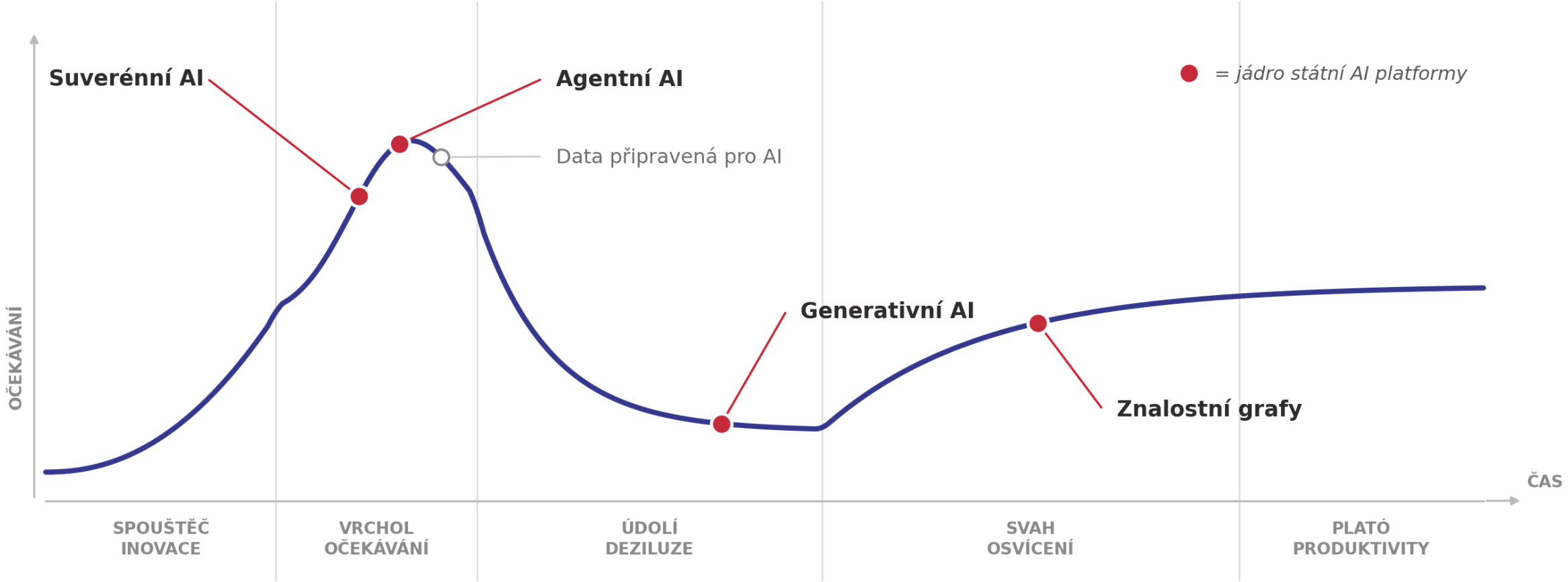
PRO KOHO

- 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 nejdřív 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 nahrazeni.

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 popsatelnými 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.

UV 589/2026

Cesta k eGovernance

Co usnesení upravuje

Jeden rámec pro záměr ICT, jeho prioritu, konzultaci kapacit a konkrétní veřejnou zakázku

1	**Evidence záměru**	Záznam vzniká, jakmile jsou známy účel, předpokládaný rozsah a předpokládané náklady.
2	**Priorita**	P1, P2 nebo P3; bez evidované priority nelze zahájit realizaci ani čerpat prostředky, nestanoví-li usnesení jinak.
3	**Konzultace kapacit**	Možnost využití kapacit NAKIT, SPCSS nebo CENDIS podle povahy záměru.
4	**Zakázka ICT**	Zakázka ICT se předkládá Předsednictvu RVIS k projednání.

Záměr ICT a zakázka ICT

Zakázka je veřejná zakázka, kterou se záměr zcela nebo zčásti realizuje

Záměr ICT

Záměr, který podle zákona č. 365/2000 Sb. podléhá povinnosti získat souhlasné vyjádření DIA.

Záměr podléhající informační povinnosti podle UV 86/2020, bez použití finančního limitu.

Záměr zahrnující systém AI ve smyslu aktu o AI, včetně velkých jazykových modelů.

Zakázka ICT

Veřejná zakázka, kterou se zcela nebo zčásti realizuje záměr ICT.

Povinnost předložení platí bez ohledu na druh zadávacího řízení nebo způsob zadání, nestanoví-li příloha jinak.

Zahrnuje také postupy podle § 222, § 134, § 135 a § 141 ZZVZ.

Zakázka ICT realizuje záměr ICT zcela nebo zčásti.

Kdy se zakázka ICT předkládá

Podle čl. 3 odst. 1 přílohy usnesení

Zadávací řízení	Před zahájením zadávacího řízení
Mimo zadávací řízení	Před jejím zadáním
Vertikální / horizontální spolupráce nebo jiná výjimka	Před uzavřením smlouvy nebo jiným právním jednáním
Změna závazku podle § 222 ZZVZ	Před právním jednáním, kterým má být změna provedena

Výsledek projednání a další postup

Výsledky a navazující kroky se zapisují do záznamu záměru

Stanovisko

Předsednictvo RVIS zakázku projedná a přijme k ní stanovisko.

Případné podmínky

Do záznamu se zapíše způsob splnění případných podmínek.

Následné kroky

Zapisuje se zahájení zadávacího řízení nebo zadání zakázky a uzavření smlouvy.

Významná změna

Projednává se pouze změna, nikoli znovu celý záměr nebo zakázka.

Governance v praxi: cesta ICT záměru

01 · NOVĚ

Hlášení záměru

ICT i AI záměry se hlásí a řídí podle usnesení vlády č. 589/2026 – ještě před povinnostmi z UV 86/2020.

02

Žádost

Úřad popíše projekt ve formuláři včetně modelu architektury v ArchiMate.

03

Posouzení

OHA ověří soulad s principy, Národní architekturou a využití sdílených služeb.

04

Stanovisko

Zpravidla do 30 dnů, ve složitých případech do 60 dnů. Může obsahovat i další doporučení.

05

Kolaudace

Před spuštěním OHA posoudí provozní dokumentaci systému.

KDO ŽÁDÁ O STANOVISKO

Správci určených ISVS podle zákona č. 365/2000 Sb., ústřední správní úřady podle usnesení vlády č. 86/2020 a žadatelé o dotace z IROP a NPO.

JAK

Elektronicky v Informačním systému dlouhodobého řízení (ISDŘ) – v produkčním provozu od 1. 7. 2026, včetně dialogu s hodnotitelem.

Závěr

- **Dnes:** pilotní AI brána a využívání na reálných use-case. Začátek eGovernance
- **Zítra:** sdílená platforma pro celý stát, ne stovka izolovaných ostrůvků. Nové zákony.
- **Rizika:** jsou zde vždy. Otázka je, jestli o nich víme a jak je dokážeme řídit.

Nebudujme stovky AI projektů.
Vytvořme architekturu AI pro projekty.

Děkuji
za pozornost

Tomáš Šedivec

tomas.sedivec@dia.gov.cz

archi.gov.cz