Od bezpečné architektury LLM k jednodušším službám pro občana

Pavol Škápik - Generální finanční ředitelství ČR

Walter Pavliš - DATERA s.r.o.

ISSS 2026 **18. května 2026**

Jak provozovat AI

Enterprise AI pod kontrolou: od dat po LLM

výkon + kontrola + bezpečnost + auditovatelnost

Walter Pavliš| **18. 5. 2026** |

Na jaké platformě?

- **Volba mezi on-prem, hybrid a cloud není technologická otázka – je to kombinace:**
  - kontroly dat - citlivá data a datová suverenita (celý životní cyklus dat),
  - požadavků na výkon - výkon a provozní stabilita systémů (AI workloadů),
  - regulace - nejasná auditní stopa a governance – není jen řízení, ale spíše systém pravidel, rolí a kontrolních mechanismů,
  - predikovatelnosti nákladů.
- **Proto dává smysl hybridní přístup:**
  - citlivá data + core AI on-prem,
  - škálování nebo méně kritické scénáře v cloudu.

Strategické rozhodování

Kritérium	Cloud	Hybridní AI (Datera)
Suverenita dat	Sdílená / Limitovaná	**Absolutní (On-Prem)**
Soulad s AI Act	Závislost na poskytovateli	**Plná kontrola úřadu**
Latence / Výkon	Závislé na poskytovateli **snadná škálovatelnost**	Garantovaný výkon
Náklady	Variabilní (Pay-per-token)	**Predikovatelné (CAPEX/OPEX)**
Investice	**Platíte pouze to co spotřebujete**	Vysoké vstupní náklady

Suverenita dat v praxi

100

KONTROLA NAD DATY

%

Váš úřad, vaše pravidla

Zajišťujeme, aby citlivá data a celý životní cyklus AI modelů zůstaly pod vaší jurisdikcí a kontrolou, v souladu s českou legislativou a požadavky na kybernetickou bezpečnost.

Praktické use-casy

- **Inteligentní správce interních směrnic**
- Velké množství směrnic a jejich verzí.
- **Analýza souladu**
- Kontrola směrnic proti nově vydané legislativě. AI označí odstavce, které jsou v rozporu s novým zákonem a zdůvodní rozdíl.
- **Analýza připomínek**
- Systém pro srovnávání a správu připomínek k zákonům.
- **Vývoj a testování SW pomocí LLM**
- Neuvěřitelný vývoj za posledních několik měsíců


datera.AI
LISSA

Řečník / Speaker

datera

Walter Pavliš

BDM | DATERA

walter.pavlis@datera.cz

Cloud | AI | Security

Finanční správa
České republiky

AI inovace a Finanční správa ČR

Pavol Škápik

Finanční správa ČR

AI jako součást modernizace finanční správy

- Finanční správa ČR dnes aktivně testuje a rozvíjí využití umělé inteligence v několika oblastech:
  - podpora občanů a podnikatelů, zjednodušení interních procesů, práce s dokumenty a daty, analytická podpora, bezpečné využití AI v prostředí veřejné správy
- Naším cílem není „AI pro AI“ ale praktické využití technologií tam, kde mohou přinést:
  - vyšší efektivitu, lepší služby, nižší administrativní zátěž a větší komfort pro občany i zaměstnance

AI ve finanční správě: od pilotů k praxi

- **Interní podpora zaměstnanců:**
  - IrčA – interní AI asistent pro práci s IAŘ a metodikami
  - DIALOG – AI podpora přepisů a analýzy výslechů
- **Služby pro občany:**
  - AI pomoc s daněmi - koncept předvyplněných daňových přiznání
- **Datová analytika a digitalizace:**
  - B3 – digitalizace a analýza pokladních dokladů
  - Atlas – analýza rizikových webů

Interní AI asistentka finanční správy

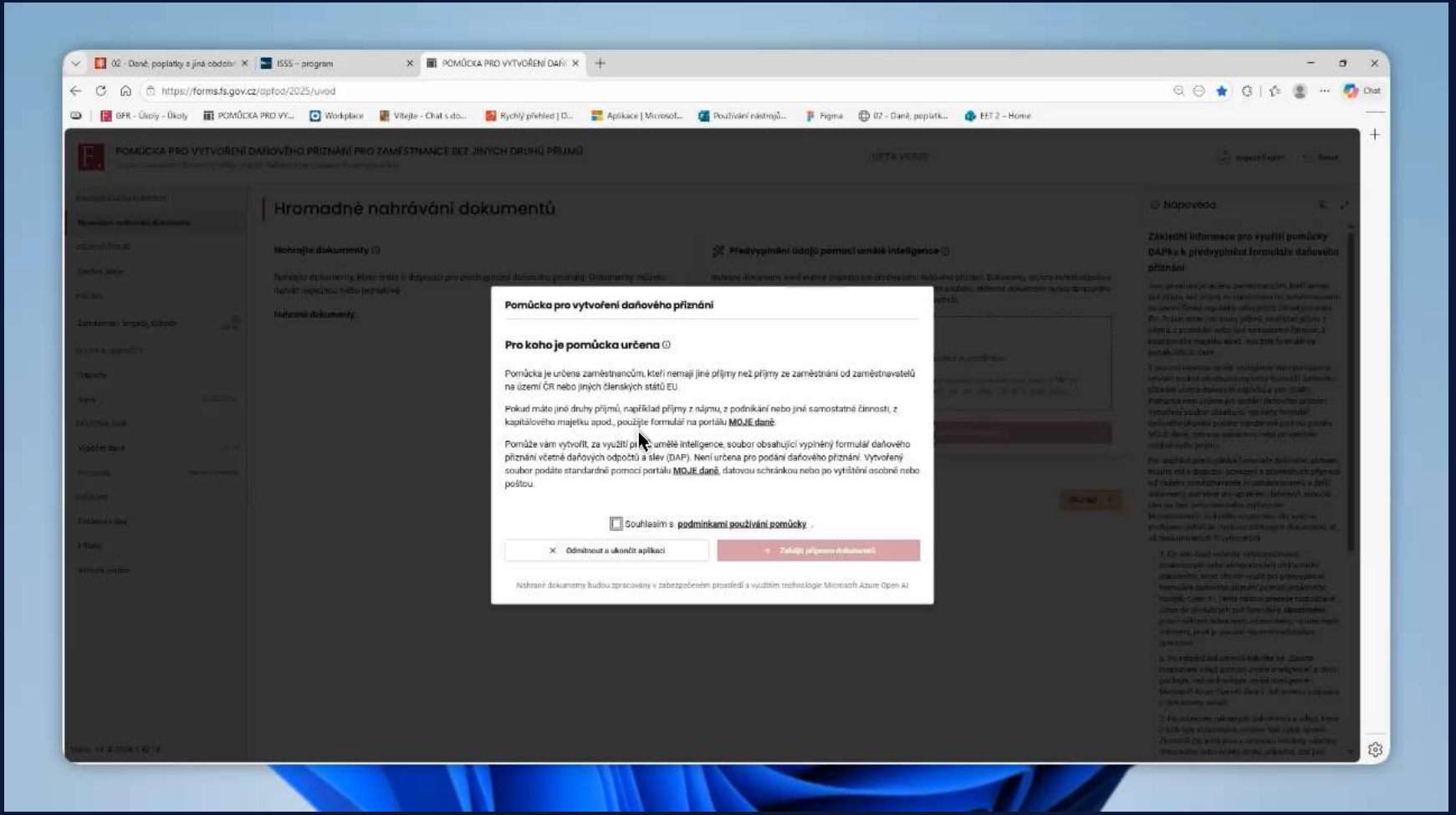
- **IrčA je interní AI nástroj určený zaměstnancům, která pomáhá s:**
  - orientací v interních dokumentech
  - metodickou podporou
  - rychlým dohledáním relevantních informací
- **Hlavní principy:**
  - kontextové odpovědi v přirozeném jazyce
  - odpovědi pouze z interních zdrojů
  - transparentní citace dokumentů
  - provoz v zabezpečeném prostředí SP CSS
  - auditovatelnost a lidský dohled

Jak vám může IrčA pomoci?

AI Pomoc s Daněmi

- **Jak celý proces funguje:**
  - 1. Nahrání podkladů občanem
  - 2. AI vytěžení a klasifikace dat
  - 3. Kontrola a validace údajů
  - 4. Předvyplněný formulář pro uživatele
  - 5. Finální potvrzení občanem
- Důležitý princip: AI pomáhá s přípravou podání, ale finální rozhodnutí vždy zůstává na člověku
- **Spolupráce**: GFŘ ČR · MF ČR · SPCSS · Datera · Microsoft · AddSign

Jak vytvořit DAP s pomocí AI?



AI jako podpora moderní finanční správy

- Finanční správa pracuje na celé řadě projektů zaměřených na:
  - inovace
  - digitalizaci
  - efektivnější služby
  - a modernější výkon správy daní

- Stále ale platí, že AI je podpora rozhodování, nikoli náhrada člověka.

AI Act: bezpečnost nestačí mít. Musí fungovat.

„Bezpečnostní pás“ musí být zapnutý – a při nárazu udržet.

DNES

Bezpečná AI landing zone

- Azure AI landing zone podle potřeb úřadu
- datová suverenita a řízení přístupu
- izolace AI aplikací a provozních prostředí
- auditovatelnost jako součást návrhu
- AI Act readiness know-how

BUDUJEME

Automatizovaná compliance AI aplikací

- kontrola vůči OWASP LLM Top 10
- důkazy shody pro AI Act / NIS2 / DORA
- kontrola: přístupy, filtry, logy, klíče
- ověření, zda se ochrany skutečně používají

VÝSTUP PRO ZÁKAZNÍKA

Gap analýza • skóre připravenosti • auditní stopa • doporučení ke zlepšení

Nestačí mít bezpečnostní opatření jen „na papíře“. Musíme umět doložit, že jsou správně nastavená, skutečně používaná a že z jejich provozu vzniká auditní stopa.

Budujeme nástroj, který nad AI aplikací ověří konfiguraci, vyhodnotí rizika podle OWASP LLM a převede technické nálezy do důkazů shody pro AI Act a další regulace.

Zajímá Vás, jak může vypadat AI compliance v praxi?
Zeptejte se nás.

Finanční správa
České republiky

Děkuji
za pozornost

Pavol Škápik

Finanční správa ČR