Egovernment
elektronizace veřejné správy

# JE TU DOBA AIOVÁ



NETUŠÍME, CO JE PŘED NÁMI

# Obsah


**Redakce**

Obsah, tiráž ..... 2
Úvodní slovo ..... 4

A brána se otevírá ..... 6–7
Dostali jsme sirky. A jdeme si hrát do stohu. ..... 8–9
Vláda posiluje řízení výdajů na ICT a umělou inteligenci. ..... 10–11
AI a citlivá data ve státní správě. ..... 12–13
Ověřitelné kontroly AI ve veřejné správě ..... 14–15
Policejní síť dostala společná pravidla ..... 16–19
Suverenita není izolace. ..... 20–23
Důvěra začíná ještě před podpisem ..... 24–25
Od spisové služby k digitálnímu ekosystému ..... 26–27
Spolehlivá IT infrastruktura ..... 28–29



***V rámci České a Slovenské republiky vydává:***
info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze
pod č. C – 81357
**tel.:** 241 412 518
**e-mail:** egovernment@egovernment.cz
**http:** www.egovernment.cz
**platforma X:** @EgovernmentMag
**facebook:** @EgovernmentMagazin
**linkedin:** @egovernmentmag
**instagram:** egovernmentmagazin

**Šéfredaktor:** Ing. Michal Jirkovský
**Asistentka:** Zdeňka Borecká

**Grafika:** PROPAGANDA, Malá Štupartská 7, Praha 1
**Tiskárna:** A. R. GARAMOND s.r.o., Belnická 758, 252 42 Jesenice
**Registrační číslo:** MK ČR E 11364
ISSN 1801-9420



Reprodukce celku ani jeho částí v jakémkoliv provedení není povolena bez výslovného souhlasu Egovernment – info◆com.
Neoznačené texty jsou redakčními články.


## Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**.
Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **300 Kč** bez DPH**/výtisk, tj. 900 Kč** bez DPH **ročně**.
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

# Kam se posouvá digitalizace Česka a rozvoj eGovernmentu?

Odpovědi přinese již **29. ročník konference**

# isss

**17.–18.5.**27
**Hradec**Králové



Potkejte se
s **klíčovými decision-makery**

Inspirujte se **případovými studiemi**

Mějte nejnovější vhled
do **světa českého**
**eGovernmentu**

Více informací a registrace na
**isss.cz**

pořadatelé

TRIÁDA · Kraj Vysočina

spolupracují

Královéhradecký kraj · Hradec Králové · Calendarium Regina

## JE TU DOBA **AI**OVÁ: NETUŠÍME, CO JE PŘED NÁMI

Plujeme si v proudu AI služeb, který pomalu nabírá na síle. Zdá se, že jsme spokojeni, neboť nástroje využívající AI jsou neskutečně rychlé, neskutečně přesné a neskutečně výkonné, pokud jsou tedy dobře nastavené. Ale patrně, stejně jako ten rybář z titulní stránky, nemáme ani my úplně jasno, kam nás ten proud vlastně zanese, ani co nám přinese.

Takový proud může být vítaným a životodárným tokem, může se stát bouřlivými peřejemi, ale také před námi může být hluboký, smrtící vodopád.

Ale my nevíme, kam ta říčka směřuje a jakou sílu bude mít. Než čekat „co z toho vyleze", bylo by lepší to koryto předem trochu „vykolíkovat". Mít situaci pod kontrolou. V rychlosti reakcí s AI soutěžit skutečně nemůžeme. Rozumné je převzít nad situací kontrolu dříve, než bude nutné reagovat.

Máme situaci pod kontrolou?

Odpověď jsme hledali v rámci konference e-government 20:10 na zámku Mikulov, od které se odráží obsah tohoto čísla magazínu. Nabízíme Vám náhled do toho, co AI přináší, co znamená i jaké kontrolní mechanismy si, alespoň v rámci veřejné správy, začínáme budovat.

Otázkou je, zda to či ono děláme skutečně ve správný čas. Zda „nekolíkujeme" koryto řeky ve chvíli, kdy ona už si teče, kudy chce?

Michal Jirkovský,
šéfredaktor


Skupina ICZ
VÁŠ PARTNER
V DIGITÁLNÍM SVĚTĚ
ICZ
www.iczgroup.com

# A BRÁNA SE OTEVÍRÁ …

***Je to sen mnoha generací. Po desetiletí, možná po staletí řada vědců, učenců, badatelů, zvědavců či šarlatánů touží po tom nalézt bránu do jiné dimenze. Nějaký otvor v časoprostoru, trhlinu, nebo něco takového, kudy se dá prostoupit do jiné dimenze. A nám, tedy alespoň úřadům veřejné správy, se teď taková brána pomalu otevírá. Brána k AI, brána do dimenze světa prodchnutého umělou inteligencí. Jen ještě úplně nevíme, jak ta brána vypadá a co nás přesně za ní čeká.***

Na konferenci e-government 20:10 na zámku Mikulov na toto téma hovořili první náměstek ministra vnitra a vládní zmocněnec pro digitalizaci a strategickou bezpečnost Lukáš Klučka, vládní zmocněnec pro AI Lukáš Kačena a místopředseda RVIS Adam Paclt. Umělá inteligence podle nich nesmí zůstat souborem nespojených experimentů, je nutné spojit technologie s jasným řízením, odpovědností a měřitelným přínosem. A právě to je důvodem, proč by stát měl vytvořit AI a LLM bránu, tedy bezpečný a hospodárný přístup k jazykovým modelům.

O tom, že AI „vtrhla" i do veřejné správy není pochyb, ale právě s ohledem na data, se kterými veřejná správa pracuje, i na skutečnost, že se jedná o veřejné finanční prostředky, je třeba tuto živelnost korigovat. Nová strategie vlády Digitální Česko 2.0, o které rovněž na konferenci pánové hovořili, je postavena na propojení jednotlivých dat, služeb i odpovědností do jednoho funkčního celku. Každý strategický projekt zde má mít svého konkrétního vlastníka, ověřenou potřebu, měřitelné milníky a transparentně řízené náklady, vazby a rizika. I proto je potřeba budovat společnou AI infrastrukturu. Místo desítek oddělených AI řešení by měla být takto nabídnuta úřadům důvěryhodná cesta k jazykovým modelům. Tímto nástrojem by měla být Národní AI brána, která bude ověřovat oprávnění konkrétního uživatele, chránit osobní a citlivé údaje a zvolí model, který odpovídá dané úloze a následně výsledek předá zpět úřadu. Každý z těchto kroků přitom za sebou zanechá kontrolovatelnou auditní stopu.

## CO BY MĚLA NÁRODNÍ AI A LLM BRÁNA ZAJIŠŤOVAT?

- **Řízený přístup k modelům** – zpřístupní více komerčních i otevřených modelů a požadavky bude směrovat podle citlivosti dat, ceny, rychlosti a ověřené kvality.
- **Ochranu osobních a citlivých údajů** – před odesláním dotazu musí systém kontrolovat či anonymizovat obsah a zabránit předání neveřejných informací do nevhodného prostředí.
- **Auditní stopu a odpovědnost** – bude vždy možné doložit, jaký model byl použit, s jakým zadáním a výsledkem. Otevřený reporting a dohledatelnost jsou podmínkou důvěry.
- **Kontrolu nákladů a spotřeby** – centrální měření umožní sledovat využití napříč resorty, řídit limity a hospodařit lépe než při roztříštěných nákupech.
- **Bezpečnostní a kvalitativní kontroly** – bude filtrovat rizikové vstupy, testovat výstupy, řídit oprávnění a nabízet prověřené postupy pro opakované úřední činnosti.
- **Technologickou nezávislost** – společná rozhraní oddělí úřední aplikace od konkrétního modelu, aby stát mohl reagovat na změny ceny, výkonu i bezpečnostního profilu bez nákladné přestavby služeb.



## PROČ?

Digitalizaci a strategickou bezpečnost nelze řídit odděleně. S rostoucím využíváním AI roste význam toho, kde jsou data uložena, kdo k nim přistupuje a jak lze celý proces zpětně prověřit. Pro některé agendy může být přijatelné využití veřejného cloudu, jiné budou vyžadovat důvěryhodné nebo přímo státem kontrolované prostředí. Gateway proto musí uplatňovat pravidla podle klasifikace dat a rizika, nikoli podle pohodlí uživatele. Současně musí posilovat odolnost vůči kybernetickým útokům, manipulaci vstupů i selhání dodavatelského řetězce.

## JAK?

Důvěra nevzniká nálepkou „národní". Vzniká pravidelným bezpečnostním testováním, hodnocením kvality modelů v češtině, řízením verzí, jasnými pravidly pro uchovávání záznamů a kontrolou dopadů. Potřebujeme postupy pro incidenty i možnost rychle odstavit problémový model, datový zdroj nebo scénář použití. Osobní odpovědnost konkrétního manažera, průběžný reporting a přehled o rizicích budou u této infrastruktury stejně důležité jako její technické parametry.

Každé využití AI zároveň bude zařazeno do standardního řízení Digitálního Česka 2.0. Musí mít jmenovaného garanta, předem stanovené ukazatele přínosu a pravidelně zveřejňovaný stav. Společná pravidla však neznamenají uzavření trhu. Naopak cílem je udržet možnost volit mezi různými modely a dodavateli. Stát má vlastnit standardy, rozhraní a kontrolní mechanismy, nikoli být trvale připoután k jedné technologii.

## KDE MŮŽEME AI BRÁNU NAJÍT?

A kde je ona brána, která nám pootvírá vstup do nové dimenze, do dimenze účinné, bezpečné a podmaněné AI? Zatím nikde. Nejprve musí být otestována beta verze. K plošnému spuštění pro všechny úřady by mělo, s ohledem na výsledky testování, dojít v průběhu prvního čtvrtletí roku 2027. Pokud chcete vědět, kdy a za jakých podmínek budete moci do brány „vstoupit", tedy ji začít využívat, bližší informace by vám měly být k dispozici tzv. AI officery nebo prostřednictvím kanálu AI.gov.cz. Můžete podle toho zvažovat svou vlastní strategii dalšího rozvoje úřadu pomocí nástrojů AI.

## JAKÝ BUDE POSTUP?

1. Začne se na agendách s vysokým objemem rutinní práce a nízkým rizikem nevratného rozhodnutí.
2. Pro každý scénář bude určen vlastník, právní základ, povolené zdroje dat, metriky kvality a roli lidské kontroly.
3. Oddělí se experimentální prostředí od produkčního.
4. Zavede se jednotné testování faktické správnosti, bezpečnosti a odolnosti proti manipulaci.
5. Rozvíjení kompetencí úředníků souběžně s technologií; bez schopnosti ověřovat výstupy se rychlost snadno změní v nové riziko.

## NÁRODNÍ AI BRÁNA JAKO SOUČÁST DIGITÁLNÍHO ČESKA 2.0

**Mikulovská diskuse potvrdila, že už se nemáme ptát, zda stát bude AI používat, ale jak ji zavede odpovědně a ve velkém. Národní AI a LLM Gateway může být praktickým základem této změny: omezí duplicity, ochrání data, zprůhlední náklady a umožní přenášet úspěšná řešení mezi úřady. Především ale zapadá do pojetí Digitálního Česka 2.0 – digitálního státu řízeného podle dat a faktů, s jasnými prioritami a odpovědností za výsledek. Úspěch nebude měřen počtem připojených modelů či dotazů. Bude měřen tím, zda občan vyřídí svou věc rychleji a srozumitelněji, zda úředník získá lepší nástroje a zda stát zůstane bezpečný a odolný.**

-red-

# Dostali jsme sirky. A jdeme si hrát do stohu.

***Dostali jsme do ruky sirky a jdeme si hrát do stohu. Asi tak dnes vypadá zavádění AI. Čím větší stoh – firma, banka, ministerstvo nebo stát – tím větší legrace. Škrtáme, zkoušíme, zapalujeme malé kupičky sena a čekáme, co se bude dít. Je to jízda.***

A mezi námi chodí spousta dobráků, mezi které se ostatně také počítám, kteří rozdávají další sirky.
„Tohle musíte zkusit."
„Dejte tam své dokumenty."
„Napojte to na data."
„A teď uděláme agenta."
Zatím žádný opravdu velký požár nebyl, takže získáváme odvahu. Nejdříve jsme zapalovali seno před stodolou. Teď už zkoušíme, co to udělá uvnitř. Snad shoří jen stodola.

## Nejdřív sirky. Potom hasicí přístroje.

Pochopitelně jde také o business. Výrobců sirek je hodně, konkurence obrovská a každý potřebuje něco prodávat. A když už mají sirky skoro všichni, je potřeba najít další trh. Naštěstí každý dobrý marketér ví, že výborně se prodává strach. Takže přichází nový business: **bezpečnost AI**.

Je to vlastně dokonalý model. Nejdřív lidem rozdáte sirky, a potom jim prodáváte hasicí přístroje. Samozřejmě, bezpečnost AI je skutečné a velmi důležité téma. Jen mám někdy pocit, že počet lidí, kteří nám vysvětlují, jak AI zabezpečit, roste rychleji než počet lidí, kteří skutečně vědí, jak AI funguje.

Ale nevadí. Když nebudeme vědět, zeptáme se AI. Ona už něco vymyslí. Můžeme například každého, kdo pobíhá ve stohu se sirkami, vybavit nehořlavými brýlemi. To se bude dobře prodávat. Nebo vyrobíme „bezpečnou AI". Co přesně to znamená, není zase tak důležité. Hlavně když je to napsané na krabici.

## AI je psychopat.

Mám ale jednu uklidňující teorii. Nejlepší ochranou proti AI bude nakonec jiná AI. Jedna AI něco vytvoří, druhá to zkontroluje, třetí najde chyby a čtvrtá vysvětlí, proč se ta třetí mýlí. Moderní varianta starého českého principu: **vyhánění čerta ďáblem**.

A ono to překvapivě funguje. Když si nechám od jedné AI něco důležitého připravit, často to dám zkontrolovat jiné. A je až zábavné sledovat, s jakým sebevědomím jedna AI rozebere chyby té druhé. AI je totiž svým způsobem psychopat. Nemá svědomí. Nemá strach. Nemá odpovědnost. A především nemá problém Vám s naprostou jistotou sdělit úplný nesmysl. Když ji na to upozorníte, odpoví: „Máte pravdu. Děkuji za upozornění." A jede dál. Což je vlastně sympatické. Znám i lidi, kteří to neumějí.

## Největší riziko není AI.

Čím déle AI používám, tím víc jsem přesvědčený o jedné věci. Největším rizikem není to, že se AI splete. **Největším rizikem je člověk, který přestane kontrolovat, jestli se spletla.**
AI dnes používám skoro na všechno. Na práci, rešerše, texty, nápady, analýzy, nákupy i úplné banality. Je neuvěřitelně užitečná. A čím víc ji používám, tím méně jí bezvýhradně věřím.

## To není paradox.

Je to podobné jako s mimořádně schopným kolegou. Pracuje rychle. Ví skoro všechno. Nikdy není unavený. Jen má jednu drobnou vlastnost. Občas si něco vymyslí. A neřekne Vám to.

Proto si myslím, že hlavní dovedností doby AI nebude promptování. Nebude to znalost neuronových sítí. Nebude to ani schopnost vybrat ten nejlepší model. Bude to obyčejná schopnost říct: **„Tohle vypadá skvěle. Ale není to náhodou blbost?“**

## Vítejte v době Alové.

Máme tedy sirky. Máme stoh. Máme spoustu nadšených lidí. Máme výrobce sirek. Máme výrobce hasicích přístrojů. A pomalu vznikají i požární předpisy. To ale neznamená, že bychom měli sirky zahodit. Naopak. AI je podle mě jeden z nejzajímavějších nástrojů, který jsme kdy dostali do ruky. Jen bychom si měli zachovat jednu velmi staromódní schopnost: **přemýšlet, než škrtneme.** Protože nejlépe hoří suché chrastí v pořádně vysušeném lese. Třeba na Šumavě.

Ing. Jan Petr
Odbor hlavního architekta
Digitální a informační agentura



# Vláda posiluje řízení výdajů na ICT a umělou inteligenci.




***Vláda České republiky schválila nové zásady pro řízení výdajů v oblasti informačních a komunikačních technologií a umělé inteligence. Usnesení zavádí jednotnou evidenci ICT záměrů, jasné určování priorit, projednávání ICT zakázek Předsednictvem Rady vlády pro informační společnost a lepší využití kapacit státních ICT organizací. Navazuje tak na směr programu Digitální Česko 2.0, který staví na odpovědném, koordinovaném a datově řízeném postupu digitalizace.***

Nová pravidla reagují na potřebu lépe plánovat a řídit digitální projekty napříč státní správou. Záměry ICT, na které se usnesení vztahuje, budou vedeny v jednotném záznamu záměru, který bude obsahovat údaje o účelu, rozsahu, předpokládaných nákladech, prioritě, případném využití umělé inteligence, průběhu projednání zakázky a významných změnách. Cílem je, aby stát měl průběžný přehled o připravovaných projektech, jejich financování, rizicích i návaznostech.

„Digitalizace státu nemůže být souborem mnoha vizí, prezentací a izolovaných projektů. Projekty pak do sebe nezapadají, což komplikuje celý proces digitalizace. Občan potom často nepociťuje dopad vynaložených prostředků. Tímto usnesením nastavujeme pravidla, která umožní včas vidět, co stát připravuje, proč to připravuje, kolik to bude stát a jaký přínos to má mít pro občany, podnikatele i úřady. Chceme, aby veřejné prostředky směřovaly do projektů, které jsou skutečně prioritní, bezpečné, moderní a dávají smysl v celkové architektuře digitálního státu," uvedl Lukáš Klučka, 1. náměstek ministra vnitra a vládní zmocněnec pro digitalizaci a strategickou bezpečnost.

Usnesení stanoví tři úrovně priorit, jež navazují na usnesení vlády ze dne 25. května 2026 č. 314 o systému řízení strategických programů a projektů z oblasti informačních a komunikačních technologií. První prioritu získají záměry vyplývající z priorit vlády, druhou pak projekty nezbytné pro splnění právních povinností nebo závazků vůči Evropské unii a třetí ty, které Předsednictvo Rady vlády pro informační společnost vyhodnotí jako významné zejména podle přínosu pro koncového uživatele. Bez evidované priority nebude možné u nových ICT záměrů zahájit realizaci, ani čerpat prostředky ze státního rozpočtu nebo fondů Evropské unie, s vyjímkami stanovenými usnesením. Součástí nového systému je také předkládání vymezených ICT zakázek k projednání Předsednictvu Rady vlády pro informační společnost. Posuzovat se bude zejména soulad konkrétní zakázky s evidovaným záměrem, přiměřenost cen a harmonogramu, kvalifikační požadavky i technické a kvalitativní parametry smluv. Výsledky projednání se budou zapisovat do záznamu záměru a přehled projednaných zakázek ICT a přijatých stanovisek bude Digitální a informační agentura zveřejňovat způsobem umožňujícím dálkový přístup.

# Nová pravidla zefektivní digitalizaci státu a zvýší transparentnost zakázek.

## Klíčové přínosy nového systému tedy jsou:

- **lepší přehled vlády i veřejné správy o připravovaných ICT záměrech;**
- **jasné priority pro financování digitálních projektů;**
- **transparentnější projednávání ICT zakázek;**
- **kontrola výdajů na státní ICT;**
- **kontrola přiměřenosti cen, harmonogramů a smluvních parametrů;**
- **systematičtější práce s projekty obsahujícími prvky umělé inteligence;**
- **lepší využití kapacit státních ICT organizací a snížení roztříštěnosti řízení.**

Nový rámec odpovídá principům Digitálního Česka 2.0: stát má mít přehled o tom, kdo za digitalizační iniciativy odpovídá, v jakém jsou stavu a jaké mají dopady; resorty mají spolupracovat v jednotném rámci a zásadní rozhodnutí se mají opírat o sdílená data o postupu, termínech, rizicích a výsledcích. Digitální stát podle programu potřebuje nejen technologie, ale především jasné řízení, transparentně sdílené informace a odpovědné rozhodování.

Usnesení zároveň zapojuje státní podniky do konzultací připravovaných záměrů. Předkladatelé budou prověřovat, zda lze pro konkrétní projekt využít kapacity Národní agentury pro komunikační a informační technologie, Státní pokladny Centra sdílených služeb nebo CENDIS podle jejich zaměření. Výsledek konzultace bude součástí záznamu záměru, aniž by tím byla dotčena pravidla zadávání veřejných zakázek

**Program Digitální Česko 2.0 přináší další etapu digitalizace veřejné správy, jež má směřovat k integrovanému digitálnímu státu založenému na propojených službách, odpovědném řízení a měřitelných výsledcích.**

**Nové usnesení tento směr promítá do konkrétních pravidel pro přípravu, financování, projednávání a vyhodnocování ICT záměrů a zakázek.**

Digitální a informační agentura má do tří měsíců zajistit, aby informační systém umožňoval vedení záznamů záměrů – včetně údajů o umělé inteligenci, evidenci priorit, konzultací, stanovisek a významných změn.

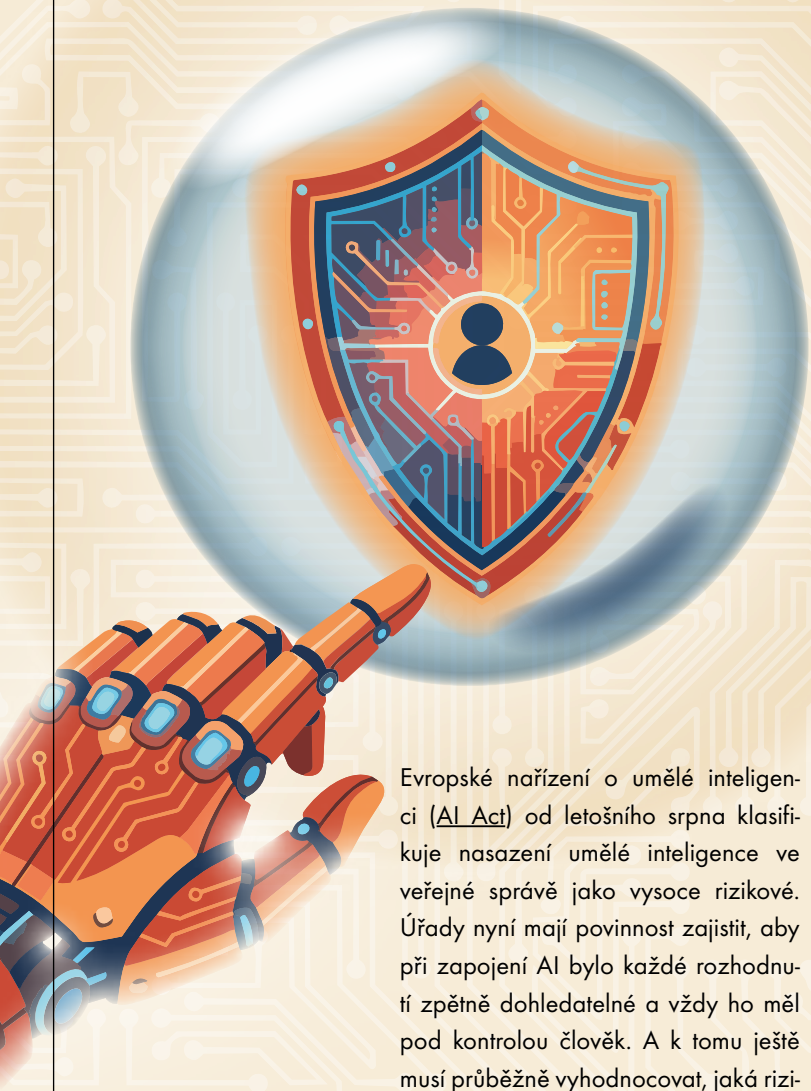
„Digitální a informační agentura bude v novém systému hrát roli při vedení evidence záměrů, metodické podpoře resortů a zajištění transparentního sdílení informací. Naším cílem je, aby úřady měly k dispozici srozumitelný a praktický nástroj, který jim pomůže připravovat digitální projekty kvalitněji, předvídatelněji a s větším důrazem na skutečný přínos pro uživatele," uvedl Bohdan Urban, ředitel Digitální a informační agentury.

-red-

# AI a citlivá data ve státní správě.

## Kudy vede bezpečná cesta?

***Nutkání využívat umělou inteligenci tam, kde může člověku ulevit s prací, se neubrání ani samotní zaměstnanci státního sektoru. O to spíš, jsou-li dlouhodobě pod kapacitním tlakem a zavaleni množstvím požadavků, které nestíhají zpracovávat. Jenže když si úředník pomůže veřejně dostupným AI nástrojem na vlastní pěst, citlivá data opouštějí infrastrukturu úřadu bez jakékoliv kontroly. NÚKIB z toho důvodu spolu s Úřadem vlády vydali Průvodce pro etické využívání AI ve veřejné správě, Digitální a informační agentura (DIA) spravuje katalog ověřených řešení a úřady postupně nasazují uzavřená prostředí pod licencí velkých poskytovatelů. Pro řadu agend to stačí. Pro všechny ale ne. Co je potřeba zvážit, než úřad sáhne po konkrétním řešení?***



Evropské nařízení o umělé inteligenci (AI Act) od letošního srpna klasifikuje nasazení umělé inteligence ve veřejné správě jako vysoce rizikové. Úřady nyní mají povinnost zajistit, aby při zapojení AI bylo každé rozhodnutí zpětně dohledatelné a vždy ho měl pod kontrolou člověk. A k tomu ještě musí průběžně vyhodnocovat, jaká rizika z nasazení AI plynou.

Odpovědnost neleží jen na úřadech. Také dodavatelům, kteří pro ně AI systémy staví a nasazují, hrozí při nesplnění povinností pokuty až 35 milionů eur, nebo 7 % celosvětového obratu. Pro samotné orgány EU stanovuje nařízení strop 1,5 milionu eur, českým úřadům bude výši sankcí určovat národní legislativa. Pokud úřad selže, hrozí mu stažení systému z provozu i reputační škoda, která může být pro instituci horší než jakákoli pokuta.

### Největší AI nástroje fungují přes cloud. Co ale s daty, která ven nesmí?

Vedle AI Actu na práci s citlivými daty dopadá GDPR a zákon č. 110/2019 Sb. o ochraně osobních údajů i zákon o kybernetické bezpečnosti ve výkladu NÚKIB. Žádné z těchto informací zkrátka nesmí opustit IT infrastrukturu úřadu bez záruky, že zůstanou chráněné. I proto úřady postupně přecházejí na uzavřená prostředí pod licencí velkých poskytovatelů, jako je například Microsoft. Tato řešení ale běží na cloudové infrastruktuře třetích stran, která podléhá jurisdikci mimo EU. Kontrola nad zpracováním je omezená a otázka souladu s předpisy se stává přinejmenším nejasnou. Podle odhadu Gartneru přitom do roku 2028 zavede 65 % vlád po celém světě požadavky na technologickou suverenitu právě jako ochranu před vlivem legislativy třetích zemí.

## Nejde jen o výběr jazykového modelu

Alternativou k veřejnému cloudu je provoz AI na vlastní infrastruktuře úřadu, takzvané on-premises nasazení. Jenže debaty o něm se příliš rychle zužují na jedinou otázku: který model nasadit? Velký jazykový model (LLM) je přitom jen poslední vrstva mnohem složitějšího celku. Pod ním stojí databáze a aplikace, které úřad již provozuje, nad nimi integrační vrstva, která je propojuje se samotným modelem. A vedle toho řada podpůrných služeb pro práci s daty, jejich vyhledávání a řazení dotazů. Všechny dnes existují i ve variantách pro lokální provoz. Podstatné ale je, aby lokálně běžel celý systém, nejen model samotný.

Pokud se úřad pro lokální nasazení rozhodne, první otázka, na kterou narazí, je GPU paměť. Lokální nasazení vyžaduje fyzický server osazený grafickou kartou o kapacitě minimálně 48 GB, pro produkční provoz s živými uživateli se doporučuje 96 GB. Celý server vychází zhruba na půl milionu korun, což je investice, kterou je třeba poměřovat s tím, co úřad získá a co riskuje, pokud ji neudělá. S hardwarem pak úzce souvisí škálovatelnost. Lokální systém má fyzický strop daný kapacitou serveru a při špičce dotazů neroste elasticky jako cloud.

## Zbavíme se technické závislosti?

Velkým tématem je nyní i volba samotného modelu, protože zdaleka ne každý je pro evropskou veřejnou správu použitelný. Mezi aktuálně nejvhodnější volby pro lokální nasazení patří Gemma 4. Z evropských alternativ pak vyniká francouzský Mistral Large 3, který je plně otevřený pod licencí Apache 2.0, s podporou ve více než 40 jazycích a infrastrukturou provozovanou v EU. V delším horizontu pak stojí za pozornost projekt OpenEuroLLM financovaný Evropskou unií, jehož ambicí je vybudovat vícejazyčné modely pro všech 24 úředních jazyků Unie.

Klíčové je nesledovat každou novinku, ale zvolit správnou rodinu modelů. Rozhodující je, zda má odpovídající licenci, dostatečnou historii vývoje a jasný plán do budoucna (tzv. roadmap). Francouzský Mistral i Gemma od Googlu tyto předpoklady dnes splňují. Hardware, který úřad pořídí, nezastarává. Každý rok na něm pouze poběží lepší model než ten předchozí. On-premises nasazení zároveň neznamená, že si úřad vše spravuje sám, ale že musí mít jasně rozdělené role mezi vlastním IT a dodavatelem.

## Anonymizace a dohledatelnost

Řízený systém, který AI Act vyžaduje, stojí na dvou pilířích: anonymizaci dat a průkazné auditní stopě. Anonymizace přitom musí fungovat jako vstupní brána před modelem, nikoliv jako dodatečný krok. Každý dokument či dotaz, který do systému vstupuje, by měl nejprve projít automatizovanou detekcí citlivých údajů. Do modelu LLM pak už pokračují jen anonymizovaná data, původní údaje zůstávají v zabezpečeném úložišti na infrastruktuře úřadu a model je nikdy neuvidí. Výstup se deanonymizuje teprve na zpáteční cestě, v prostředí pod plnou kontrolou úřadu. Totéž platí pro dohledatelnost. Systém musí logovat každý vstup a výstup, verzi modelu i čas zpracování, a tyto záznamy musí být uloženy odděleně od produkčního prostředí, v režimu pouze pro čtení, kam provozní tým nemá oprávnění zasahovat. Kontrolní orgán k nim musí mít přístup bez jakéhokoliv zásahu do běžícího provozu.

## Co když plně lokální nasazení není možné?

Ne každý úřad disponuje kapacitou provozovat celý stack na vlastních serverech a bylo by nerealistické to očekávat. Velcí poskytovatelé cloudové infrastruktury AWS, Microsoft Azure i Google Cloud proto nabízejí různé formy takzvaného suverénního EU cloudu s daty fyzicky umístěnými v Evropské unii. Jenže americký CLOUD Act z roku 2018 umožňuje americkým úřadům vyžádat si data od jakéhokoli poskytovatele pod americkou jurisdikcí, bez ohledu na to, kde jsou fyzicky uložena. Evropská komise na to v červnu 2026 reagovala přijetím Cloud and AI Development Act (CADA), který zavádí čtyřúrovňový rámec cloudové suverenity a z nejvyšších úrovní zabezpečení de facto vylučuje poskytovatele podléhající mimoevropské jurisdikci.

Nasazení AI ve veřejné správě není technický projekt. Jsou to rozhodnutí, jejichž dopady se projeví v dalších letech. Úřad přitom nepotřebuje čekat na dokonalé řešení. Potřebuje hlavně zmapovat, co kde může být, kdo za co ručí a jak celý systém obstojí ve chvíli, kdy se na něj někdo skutečně podívá. Řízená AI pod kontrolou úřadu bude vždy lepší, než stínová AI bez dohledu.

Filip Morávek,
CEO Easy8, platformy
pro řízení projektů a práce

# Ověřitelné kontroly AI ve veřejné správě

***Při nasazování AI ve veřejné správě je třeba určit, k čemu služba slouží, kdo za ni odpovídá a jak se ověří její ochranná opatření. DATERA tento přístup představila na mikulovské konferenci e-government 20:10. Kontrolní část pak rozvíjí v platformě ReguAudit AI.***

## Výběr technologie podle konkrétní agendy

Před výběrem technologie je třeba určit, co má AI zlepšit, z jakých dat smí čerpat, kdo ověřuje její výstupy a kdo za službu odpovídá. Podle toho se volí cloud, vlastní prostředí, nebo jejich kombinace.

DATERA na konferenci představila interní asistentku IrčA pro Finanční správu ČR, která pracuje s interními dokumenty a uvádí zdroje odpovědí. V konceptu „AI Pomoc s Daněmi" ukázala, jak může AI připravit podklady pro daňové přiznání, které občan zkontroluje a potvrdí. V obou případech je třeba navrhnout jak postup, tak i lidský dohled.

## Od pravidel k ověřitelnému výsledku

Interní pravidla určují, jak má úřad AI používat, sama o sobě však neukážou, jak služba funguje v praxi. DATERA proto rozvíjí ReguAudit AI pro ověřování přijatých opatření a doložení výsledků.

Vedení úřadu potřebuje znát otevřená rizika a rozhodnout o nápravě. Vývojový a bezpečnostní tým oba potřebují vědět, zda přijatá opatření obstála při ověření. ReguAudit AI poskytuje těmto týmům společný podklad.

Výsledkem je technicky podložená zpráva pro audit – s jasně vymezeným rozsahem a závěry. Poskytuje základ pro rozhodnutí o dalších krocích.

Rozsah hodnocení se vždy přizpůsobuje konkrétnímu využití AI a specifickým požadavkům organizace.

## Hodnotit službu v jejím kontextu

Úřad nezavádí jen jazykový model, ale službu pro konkrétní uživatele a agendu. Záleží tedy na zamýšleném použití, datech, odpovědnosti za rozhodnutí i provozním prostředí. Ověření proto musí vycházet z výsledné služby a jejího účelu. ReguAudit AI pomáhá doložit, jak služba v dohodnutém rozsahu obstála vůči vybraným požadavkům na bezpečnost a odpovědný provoz. Výstup pomáhá určit, které oblasti upravit před nasazením a které sledovat v provozu. Rozsah posouzení se odvíjí od rizik konkrétní agendy.

Změna dat, funkcí nebo prostředí může změnit i rizika služby. Úřad proto potřebuje podklady pro rozhodnutí, zda dosavadní opatření stále odpovídají aktuálnímu stavu.




## Co technické testy dokládají

Povinnosti podle AI Actu závisejí mimo jiné na účelu a rizikové kategorii systému i na roli organizace. Technické ověření může doložit chování služby ve vymezeném rozsahu a podpořit řízení rizik. Samo o sobě nepotvrzuje právní soulad; ten totiž vyžaduje také právní a organizační posouzení.

## Pilot nad jednou agendou

Workshop nad jednou agendou může vymezit očekávaný přínos, vstupní data, odpovědnost za výstupy a způsob ověření. Na tomto základě lze zvolit prostředí a navrhnout pilotní službu s průběžnou kontrolou.

datera

Walter Pavliš,
Business Development Manager, DATERA
info@datera.cz

APG
ASOCIACE PODNIKATELŮ V GEOMATICE

## Hledáte, nebo plánujete řešit některé z těchto témat?

digitální technická mapa | evidence technické infrastruktury | digitalizovaný model připravované stavby | evidence zeleně | evidence majetku | práce s daty z katastru nemovitostí | zpracování a vizualizace geografických dat pro komunikaci s občany | zadržování vody v krajině | záznam průběhu stavby a staveniště | ochranu před povodněmi | eroze půdy | kartografické výstupy | digitální dvojče připravovaného projektu | a další geomatické služby, která řeší česká:

**Města** | **Kraje** | **Obce** | **Servisní organizace** | **Subjekty státní správy**

## Prostě potřebujete a chcete pracovat s geografickými daty digitálně a poskytovat moderní služby občanům?

Obraťte se na nás

### Jsme Asociace podnikatelů v geomatice

Sdružujeme 44 významných společností, poskytujících geomatické služby, pro které zajišťujeme odborné, vzdělávací, propagační, komunikační a legislativní zázemí.

www.apgeo.cz

#digitalizujemecesko

# Policejní síť dostala společná pravidla

***Modernizovat síť téměř tisícovky policejních lokalit neznamenalo jen vyměnit zastaralá zařízení. Bylo třeba sjednotit technické prostředí, které vznikalo postupně po řadu let, vyjasnit odpovědnost za jeho správu a provést změny s minimálním dopadem na fungování jednotlivých pracovišť policie. Program Modernizace komunikační infrastruktury II ukazuje, proč jsou společná pravidla stejně důležitá, jako nové technologie.***

Komunikační síť zůstává obvykle mimo pozornost, dokud funguje. U Policie ČR však její výpadek může zasáhnout nejen běžný chod pracovišť, ale také krizové řízení a spolupráci v integrovaném záchranném systému. Spolehlivost a bezpečnost infrastruktury proto nejsou jen záležitostí IT oddělení – jsou podmínkou fungování celé instituce.

Původní policejní síť vznikala prostřednictvím dílčích projektů, podle aktuálních potřeb a dostupných financí. Jednotlivá pracoviště se lišila stářím zařízení, zapojením i konfigurací. Také zabezpečení a způsob správy nesly otisk místních podmínek. Zavádění změn proto vyžadovalo mnoho ruční práce a znalosti konkrétních správců se obtížně přenášely mezi kraji.

Program Modernizace komunikační infrastruktury II, zkráceně MKI II, který probíhal od jara 2023 do srpna 2026, měl tuto roztříštěnost překonat. Vedle obnovy techniky přinesl společnou architekturu a provozní model pro řízení sítě jako služby. Na konferenci e-government 20:10 v Mikulově jej představili plk. Mgr. Branislav Samek, ředitel Národního centra informačních a komunikačních technologií Policejního prezidia ČR, a Ing. Jan Holub, ředitel programu za dodavatele ALEF NULA.

## Od místních řešení ke společnému standardu

Potíže různorodého prostředí se nejvýrazněji projeví při rozsáhlejší změně nebo řešení incidentu. Správce, který dobře zná vlastní síť, nemusí být schopen stejně rychle pomoci v jiném kraji. Zastupitelnost je omezená a provoz se soustředí spíše na odstraňování problémů, než na jejich prevenci.

Diagnostika spotřebovává čas odborníků, zastaralá zařízení přinášejí riziko neplánovaných výdajů a vedení obtíž-



*„Naším cílem nebyla jen obměna zařízení, ale garantovaná síťová služba, kterou policie bezpodmínečně potřebuje. Získali jsme schopnost řídit síťovou infrastrukturu jako službu, kontrolovat její provoz a garantovat dostupnost i bezpečnost. Nová síť nám zároveň umožňuje další rozvoj, segmentaci a centralizovanou správu bez zásahů na jednotlivých lokalitách. Projekt hodnotím jako úspěšný: podařilo se nám dosáhnout zásadního cíle, který jsme si na začátku stanovili.“*

plk. Mgr. Branislav Samek, ředitel Národního centra informačních a komunikačních technologií Policejního prezidia ČR

něji předvídá náklady i dobu potřebnou k nápravě. Odlišné bezpečnostní politiky navíc komplikují kontrolu toho, jak se pravidla zabezpečení skutečně uplatňují.

Odpovědí se stala standardizace. Lokality byly rozděleny podle významu na velké a střední uzlové objekty a menší koncová pracoviště. Pro jednotlivé typy vznikla společná pravidla vybavení, zapojení a konfigurace. Sjednocení zahrnuje také označování zařízení, adresní plán a síť určenou pro správu.

Neznamená to, že všechny policejní budovy mají mít stejné vybavení. Rozdíly však vycházejí z předem definovaného návrhu, nikoli z historických zvyklostí. Konfigurační šablony se používají pro propojení jednotlivých objektů i jejich místní sítě. Administrátoři tak mohou pracovat podle společných pravidel místo toho, aby pokaždé poznávali jiné prostředí.

## Šestnáct projektů, jeden celek

Koncept programu vznikl na jaře 2023, v září následoval návrh architektury a detailního řešení. V roce 2024 pracovníci Národního centra informačních a komunikačních technologií společně se zástupci smluvního partnera navštívili všechna krajská ředitelství a zmapovali skutečný stav i potřeby jednotlivých útvarů. Program byl dokončen v srpnu 2026.

MKI II zahrnoval šestnáct dílčích projektů. Financování z Národního plánu obnovy umožnilo modernizaci v celorepublikovém rozsahu, který přesahoval možnosti běžné obnovy. Jednotlivé části navazovaly na koncepci Ministerstva vnitra, předchozí modernizační projekty a standardy resortní infrastruktury.

Obnova se soustředila na tři technologické vrstvy. Páteřní přepínání na úrovni L3 zahrnovalo 277 zařízení ve sto lokalitách a jeho implementace skončila v prosinci 2024. Propojení pracovišť prostřednictvím CE routerů představovalo 1 040 zařízení v 948 lokalitách. Zakázky krajských ředitelství na přístupovou vrstvu, k níž se připojují uživatelé a koncová zařízení, zahrnovaly 3 179 přepínačů v 875 lokalitách. Jde o různé části téže infrastruktury, nikoliv o samostatné skupiny pracovišť, jejichž počty lze sečíst.

Stejně důležité jako technické řešení, bylo rozdělení odpovědnosti. Ministerstvo vnitra a NAKIT zajišťují transportní síť, Policie ČR vystupuje jako zákazník a garant požadavků na službu. Modernizace tak vymezila také hranice mezi poskytováním konektivity a správou policejní sítě.

## Síť pod centrálním dohledem

Jedním z hlavních prvků modernizace je softwarově řízená síť SD-WAN. Konfigurace a pravidla komunikace se díky ní spravují centrálně, nikoliv ručním nastavováním každého routeru zvlášť. Nad transportním připojením tak vzniká společná řídicí vrstva, která může pracovat s různými technologiemi připojení.

Zavedení SD-WAN ovšem vyžadovalo důkladnou přípravu. Bylo nutné prověřit stávající síť, její rozdělení do




*„Samotná migrace může vypadat jednoduše: přivezete zařízení, zapojíte ho a konfigurace se stáhne z centrálního systému SD-WAN. Jenže za tím jsou měsíce intenzivní přípravy. Každou lokalitu jsme museli detailně zmapovat a vše sladit s policií i NAKITem, protože nebyl prostor se na pracoviště opakovaně vracet. Nasazení se muselo povést napoprvé a pracoviště policie přitom musela dál fungovat. V nejintenzivnější fázi jsme migrovali souběžně v deseti krajích, až šestnáct lokalit najednou. Průměrně jsme zvládli pětadvacet pracovišť denně, v některých dnech i sedmdesát. Za celou migraci nastal jediný neplánovaný výpadek, který trval přibližně třicet minut. To považuji za úspěch."*

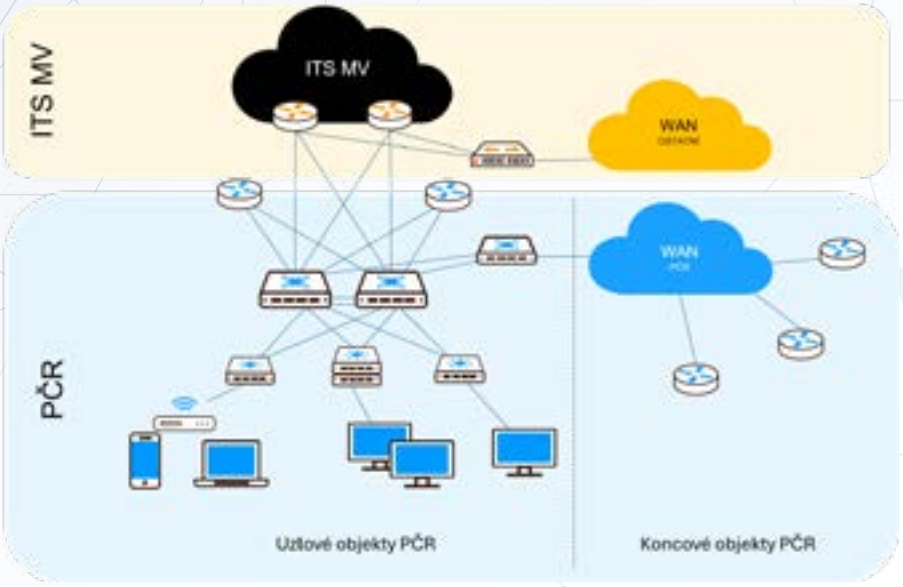
Ing. Jan Holub, ředitel programu za ALEF NULA

**CE Routery** ✓

**L3 Switche** ✓

**Acces** ✓

**Koncové stanice**




oddělených segmentů, nároky na dostupnost i plánovaný rozvoj. K důležitým krokům patřilo ověření centrálních systémů a pilotní nasazení na vybrané skupině lokalit. Teprve odladěné konfigurační šablony vytvořily základ pro hromadné zavádění změn.

Společná pravidla se týkají také přístupů administrátorů. Pro jejich centrální ověřování a řízení oprávnění řešení využívá Cisco ISE a TACACS+. Součástí standardizace je centrální ukládání provozních záznamů a sběr informací o síťových tocích pomocí NetFlow. Tyto nástroje poskytují podklady pro dohled nad sítí a diagnostiku problémů. Správa místních sítí stojí na Cisco Catalyst Center, propojení lokalit na Cisco SD-WAN. Obě oblasti spojuje centrální řízení, konfigurační šablony a jednotné bezpečnostní nastavení. Pravidla zabezpečení tak nezůstávají pouze doporučením pro jednotlivá pracoviště, ale lze je uplatňovat napříč sítí. Segmentace, řízení přístupů, šifrování a možnost zpětné kontroly zároveň podporují plnění požadavků kybernetické bezpečnosti.

## Migrace s minimem odstávek

Převést stovky fungujících pracovišť do nového prostředí nebylo jen technickým úkolem. Policejní síť zahrnuje budovy sdílené s dalšími organizacemi rezortu vnitra, lokality bez stálé přítomnosti pracovníků i pracoviště u jiných subjektů. Do harmonogramu navíc průběžně zasahovala stěhování, rekonstrukce a nové objekty.

Nasazení L3 přepínačů předcházela analýza všech sta lokalit a úprava návrhu podle jejich skutečných podmínek. Realizace této etapy trvala tři měsíce, samotná migrace tři týdny. Přímo na pracovištích se zapojilo více než padesát pracovníků dodavatele. Společný návrh uzlových objektů a jednotný postup pomáhaly omezit odstávky.

Migrace CE routerů vyžadovala koordinaci více než devíti set lokalit během dvou měsíců. Práce probíhaly souběžně v deseti krajích a postupovaly od velkých uzlových objektů přes další uzly až k menším pracovištím. Zapojilo se více než sto pracovníků policie a přes padesát pracovníků dodavatelů.

Postup zahrnoval ověření místních podmínek, zajištění instalačního materiálu a automatizované zprovoznění zařízení, označované jako zero-touch nasazení. Přechod řídil migrační velín podle harmonogramu a instalační týmy měly k dispozici centrální telefonní linku pro okamžitou podporu. Souběžně se převádělo šestnáct lokalit a průměrné tempo dosahovalo pětadvaceti pracovišť denně. Migraci CE routerů provázel jediný neplánovaný výpadek. Omezení dopadů na provoz přitom záviselo nejen na automatizaci, ale také na přípravě, pilotním ověření postupů a průběžné komunikaci všech zapojených stran.

MKI II vytvořil společný technologický základ a provozní model pro další rozvoj policejní sítě. Nejdůležitější změnu však nelze vyjádřit počtem nových zařízení – ale tím, že místo souboru místních řešení má policie infrastrukturu se společnými pravidly a jasně rozdělenou odpovědností. Právě to vytváří předpoklady, aby síť dokázala růst bez návratu k původní roztříštěnosti.

-red-

Financováno Evropskou unií
NextGenerationEU
NÁRODNÍ PLÁN OBNOVY

ALEF

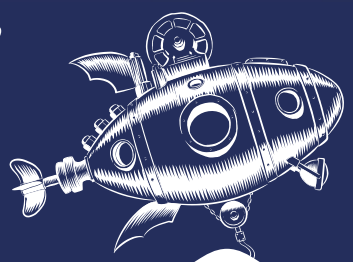
cisco Distributor

# NOVÁ GENERACE FIREWALLŮ
# NOVÁ ÉRA BEZPEČNOSTI



## Cisco Secure Firewall 200 Series
Silnější. Rychlejší. Chytřejší.

Cisco představuje novou řadu firewallů, které posouvají hranice bezpečnosti pro firmy všech velikostí.



## Cisco Security Hub

**Kybernetická bezpečnost** od endpointu až po cloud - na jednom místě.

SCAN ME

# Suverenita není izolace.
## Je to schopnost volby a kontroly.

***Česko aktivně používá umělou inteligenci ve 31,2 % pracující populace a je 27. na světě — v globálním žebříčku jsme se během jediného roku propadli z 24. na 27. místo, protože ostatní země jsou v adopci AI rychlejší než my. Ztrácíme tak konkurenceschopnost v Evropě, i ve světě. Podle šéfa českého Microsoftu o budoucnosti nerozhodne technologie, kterou má dnes k dispozici každý, ale to, kolik lidí ji umí použít. Mluvili jsme o tom, co může stát udělat, kde nám ujíždí vlak a proč digitální suverenita neznamená, že si všechno musíme postavit sami.***

**Konference skončila, sešla se na ní prakticky celá česká státní správa. S čím jste odjížděl?**

S dobrým pocitem, a to myslím upřímně. Ještě před dvěma lety jsme se bavili hlavně o strategiích a plánech. Dnes se bavíme o provozu. Voicebot Eva na call centru MPSV zvládá přes pět tisíc hovorů denně. Finanční správa má daňového asistenta DAPku. Na Ministerstvu zahraničí automatizujeme vízovou agendu a jednomu úředníkovi to ušetří až dvě hodiny rutinní práce denně. To už není pilot pro pár nadšenců, to je mozaika, která funguje napříč rezorty.

Zároveň ale říkám jednu věc pořád dokola: neukazujte mi AI. Ukažte mi změněný proces a změřený výsledek. Debata se posunula od „pojďme si to vyzkoušet“ k mnohem těžší otázce – co díky tomu děláme jinak.

**Jak si tedy Česko reálně stojí? Zaostáváme, nebo ne?**

Z globálního pohledu na první dojem nezaostáváme. Podle Microsoft AI Diffusion Reportu používá aktivně umělou inteligenci 31,2 % naší pracující populace, což nás řadí na 27. místo na světě. Jsme zhruba na úrovni Německa, Polska i Spojených států. V Evropě jsme ale až patnáctí a země na čele světového žebříčku se pohybují kolem šedesáti procent. Kromě toho rychlost adopce v jiných zemích nabírá na obrátkách, a my se naopak postupně propadáme.

A tady je ta podstatná věc: ten rozdíl nedělá technologie. Tu má dneska k dispozici každý. Dělá ho to, kolik lidí ji umí použít. A dovednosti máme ve svých rukou, ty můžeme přímo ovlivnit. Já to přirovnávám k hokeji – když jedu na mistrovství světa, nechci se zúčastnit. Chci hrát finále. Tak pro to musím něco udělat.

**Kde nám tedy ujíždí vlak?**

Ve třech věcech. První je rychlost. Umíme skvěle pilotovat, ale mezi prototypem a ostrým provozem napříč úřadem je propast, kterou překonáváme příliš pomalu. Druhá je měřítko dovedností – Úřad práce popisuje, že až třetina lidí se kvůli nedostatku digitálních dovedností nedostane ani k pracovnímu pohovoru. To není IT problém, to je ekonomický problém. A třetí je čekání. Čekání na dokonalou metodiku, na dokonalý zákon, na to, až to někdo vyzkouší první. Technologie se za tu dobu změní dvakrát.

**Co tedy může stát udělat konkrétně?**

Tři věci, a žádná z nich není o nákupu technologie. Za prvé udělat z AI dovedností standardní výbavu úřadu, ne benefit pro nadšence. Za druhé zadávat měřitelný výsledek, ne nástroj – tedy „chceme zkrátit vyřízení této agendy“, ne „chceme nasadit AI“. A za třetí sdílet mezi institucemi, co už funguje. Ty projekty existují, jen o sobě často navzájem nevědí.

Naše ambice je dostat Česko mezi deset zemí s nejvyšší adopcí AI na světě. Není to nereálné. AI je pro nás cesta ven z montovny, ne další položka v IT rozpočtu.

**Microsoft do toho vstoupil vzdělávacím programem. Proč zrovna jím?**

Protože jsme si spočítali, kde je úzké hrdlo. Proto jsme v červnu 2025 spustili AI National Skilling Plan s cílem proškolit 350 tisíc lidí a v první fázi do něj investovali přes deset milionů korun. Jeho součástí je program „AI na úřad“, který děláme s Úřadem vlády a Digiskills. Je zapojeno padesát organizací veřejné správy včetně devíti ministerstev, Českého statistického úřadu nebo Českého telekomunikačního úřadu, prostředí je připravené




pro 24 tisíc úředníků a pro zapojené instituce je zdarma. Každý týden přibývají v průměru čtyři nové organizace. A mám oblíbené číslo. Na Úřadu vlády prošlo programem 577 zaměstnanců a dokončili přes 45 tisíc online minikurzů – v průměru skoro osmdesát na člověka. Nikdo je k tomu nenutil. Úředníci se učit chtějí, jen potřebují bezpečný prostor a kvalitní obsah.

**Co se v těch kurzech úředník vlastně naučí?**

Začíná se AI gramotností, tedy tím, jak AI používat bez rizik. Co do ní nepatří, jak poznat halucinaci, jak neposlat citlivý dokument do nástroje, který k tomu není určený. Teprve pak přichází praktická práce – shrnování podkladů, příprava na jednání, dokumentová agenda. Učitelé k tomu dostávají příručku se 101 tipy pro školství; základní škola v Aši díky tomu snížila administrativní zátěž učitelů o šedesát procent.

Pyšný jsem na spolupráci s Národní knihovnou. Máme nejhustší síť knihoven v Evropě a ta otevírá AI vzdělávání i lidem, kteří nesedí v kanceláři u počítače – seniorům, uchazečům o práci, studentům. Od října na to navazuje AI Academy, sto dvacet minut online každý měsíc.

**Hodně se teď mluví o kyberbezpečnosti státu. Jak se změnila hrozba?**

Já s oblibou říkám, že prodávám důvěru. A ta situace je dnes zajímavá v tom, že AI používají obě strany – útočníci i obránci. Útočníkovi umožňuje automatizovat,

rychleji hledat slabiny a psát věrohodnější phishing. Za mě je rovnice jednoduchá: AI mění útok, musí proto změnit i obranu. Na útok, který probíhá rychlostí stroje, nemůžete dlouhodobě odpovídat jen rychlostí člověka.
Pro státní správu z toho plyne něco nepříjemného, i něco povzbudivého. Nepříjemné je, že veřejná správa spolu s IT sektorem patří k nejzasaženějším cílům. Povzbudivé je, jak levná je většina obrany. Sedmadevadesát procent útoků na identitu je prosté hromadné zkoušení slabých hesel – žádná rafinovanost, jen strojová rychlost. A moderní vícefaktorové ověření sníží riziko kompromitace identity o víc než devadesát devět procent. To dnes zvládne každý telefon.

**A deepfake a sociální inženýrství?**

To je ten klíčový posun: podvod se přesunul od technologie k člověku. Útočník už nemusí prolomit systém, stačí mu přesvědčit úředníka. Deepfake dnes nepotřebuje laboratoř, potřebuje třicet vteřin vašeho hlasu z videa na sociální síti.
Proto je obrana hlavně procesní. Domluvte si na úřadě i doma, že žádost o peníze nebo o změnu čísla účtu se vždycky potvrzuje druhým kanálem. Berte naléhavost jako varovný signál, protože spěch je hlavní nástroj útočníka. A mějte pravidlo čtyř očí u každé platby nad domluvenou částku. Ta jedna věta ochrání víc než většina softwaru – technika je až druhá vrstva.
Bezpečnost je ale týmový sport. Proto jsme podepsali memorandum o spolupráci s NÚKIB o sdílení poznatků o hrozbách a transparentní komunikaci o incidentech a už předtím jsme podobné memorandum podepsali s Armádou ČR. A evropským vládám nabízíme zdarma European Security Program.

**Ve státní správě sílí názor, že skutečně suverénní budeme, až si všechno postavíme sami. Co na to říkáte?**

Že si pleteme suverenitu s izolací. Suverenita není otázka adresy serveru. Je to kontrola nad daty, šifrováním, přístupem a kontinuitou služeb – a schopnost rozhodnout, jaká rizika jste ochotni přijmout. Žádná lokalita serveru sama o sobě nezaručuje kontrolu, ani bezpečnost. A izolace odolnost často spíš snižuje, protože vám bere zálohu, když se něco stane.
Taky se mýlí představa, že lokální poskytovatel je automaticky mimo dosah cizích soudů. Nedávno kanadský soud nařídil francouzskému poskytovateli vydat data uložená v Evropě. Kontrolu vám nedá vlaječka na budově, ale architektura, šifrování, správa klíčů a smluvní závazky.
A ty závazky jsme dali na papír. Zavázali jsme se provozovat cloudové služby v souladu s evropským právem a právně garantovali, že pokud by se někdo pokusil nařídit přerušení služeb pro evropské zákazníky, budeme to napadat soudní cestou. Zákaznická data nepoužíváme pro sebe, ani pro trénování modelů – to není marketingová věta, to je smluvní závazek. Evropskou datacentrovou kapacitu navyšujeme o 40 % během dvou let. A v Česku máme nejvyšší bezpečnostní úroveň pro veřejný cloud posouzenou NÚKIB a DIA.
Takže ne, suverenita není izolace. Je to schopnost volby a kontroly.

**Znamená to, že se stát bez globálního dodavatele neobejde?**

Znamená to, že potřebuje obojí. My přinášíme technologii a bezpečnostní rámec. Znalost konkrétního úřadu, jeho procesů a odpovědnosti má český partner nebo integrátor – a právě otevřený ekosystém umožňuje státu kombinovat globální technologii s místní znalostí. Mimochodem, Praha je domovem největšího vývojového centra Microsoftu v kontinentální Evropě, přes 1 200 inženýrů z více než padesáti zemí. Vyvíjí se tu část platformy Microsoft Entra, tedy přesně ta oblast, která organizacím umožňuje řídit identity a přístupy.

**Co byste vzkázal úřadu, který s AI zatím nezačal?**

Nezačínejte technologií. Začněte jedním procesem, který vás dlouhodobě štve, a zkuste ho změnit. A pošlete lidi do kurzu dřív, než koupíte licenci – to pořadí je důležitější, než se zdá.
A ještě jednu věc. Microsoft je partner státu, ne jenom jeho dodavatel. Technologii a bezpečnostní rámec přinášíme my, ale rozhodnutí dělat věci jinak vzniká uvnitř českých institucí. A právě proto to u nás funguje.

Microsoft

# INTERNETOVÉ SLUŽBY

**DOMÉNY | HOSTING | WEBY | ONLINE BEZPEČNOST | SERVERY | AI**

V Zoneru již více než 30 let patříme k nejspolehlivějším technologickým partnerům v ČR. Naše internetové oddělení staví na tradici i inovacích – od nejrychlejšího hostingu a VPS přes nejširší nabídku doménových koncovek až po vlastní AI cluster.

## CZECHIA.COM

Registrátor s nejširší nabídkou domén v ČR s nejrychlejším WordPress hostingem na trhu.

## SSLmarket.cz

Největší vydavatel SSL/TLS certifikátů v Evropě a lídr v oblasti PKI a digitální důvěryhodnosti.

## ZonerCloud.cz

Nejvýkonnější virtuální servery a pokročilá GPU infrastruktura pro trénování a provoz AI.

## inPage.cz

Profesionální tvorba webů a e-shopů na vlastním CMS a na WordPressu.

## Asome.cz

Prodejce pracovních a herních PC a HDR monitorů s 98% hodnocením na Heurece.

## ZonerAI.com

AI platforma pro generování a úpravu obrázků, dostupná z webového prohlížeče.

CERTIFIKOVANÝ REGISTRÁTOR

NIS2 READY

MADE IN CZECHIA

DNSSEC ZDARMA

KVALIFIKOVANÝ DODAVATEL

POSKYTOVATEL CLOUD COMPUTINGU

www.zoner.eu admin@zoner.cz +420 543 257 018

# Důvěra začíná ještě před podpisem

## Život elektronického dokumentu v prostředí rostoucích kybernetických hrozeb

***Také letos jsme měli příležitost zúčastnit se konference e-government 20:10 v Mikulově, jednoho z nejvýznamnějších setkání věnovaných digitalizaci české veřejné správy. Každoročně propojuje odborníky, zástupce ministerstev, krajů, měst a obcí s technologickými partnery a otevírá témata, která určují další směřování českého eGovernmentu. Jedinečná atmosféra Mikulova a jeho zámku navíc dává odborným diskusím a osobním setkáním výjimečný rámec.***

Pro První certifikační autoritu (I.CA), která letos slaví 25 let působení na trhu jako akreditovaný poskytovatel certifikačních služeb, představuje konference především příležitost sdílet zkušenosti z konkrétních projektů digitalizace veřejné správy. I.CA dnes patří mezi přední evropské poskytovatele kvalifikovaných služeb vytvářejících důvěru podle nařízení eIDAS.

Letošní diskuse zároveň ukázaly, že s rostoucím počtem digitálních služeb nabývá na významu jejich bezpečnost. Veřejná správa čelí phishingu, zneužití přihlašovacích údajů, útokům na informační systémy i riziku manipulace s elektronickými dokumenty. Důvěryhodnost digitálního dokumentu proto nelze řešit pouze v okamžiku jeho podpisu. Je třeba ji budovat a chránit během celého jeho životního cyklu.

### BEZPEČNOST ZAČÍNÁ U PŘIHLÁŠENÍ, NE U PODPISU

Život elektronického dokumentu začíná mnohem dříve, už v okamžiku, kdy se zaměstnanec přihlásí do počítače nebo informačního systému, ve kterém dokument vzniká, upravuje se či schvaluje. Je zásadní vědět, kdo s ním skutečně pracuje. Pokud organizace nedokáže spolehlivě ověřit identitu uživatele už při vstupu do systému, může být následně zpochybněna důvěryhodnost všech dalších kroků.

Samotné uživatelské jméno a heslo dnes již neposkytují dostatečnou úroveň ochrany. Směrnice NIS2 proto mezi opatření k řízení kybernetických rizik řadí také využití vícefaktorového nebo průběžného ověřování identity, je-li to s ohledem na charakter organizace a vyhodnocená rizika vhodné.

Na tuto potřebu reaguje platforma GITRIX, kterou I.CA nabízí ve spolupráci s technologickým partnerem. Jde o komplexní řešení pro správu digitálních identit a vícefaktorové ověřování uživatelů. Identitu lze potvrdit kombinací několika nezávislých faktorů – například čipové karty a PINu nebo prostřednictvím mobilní aplikace.

Jedna čipová karta přitom nemusí sloužit pouze k přihlášení do systému. Může zároveň fungovat jako zaměstnanecký průkaz, prostředek pro vstup do budov, evidenci docházky, identifikaci ve stravovacím systému nebo bezpečný přístup do VPN. Několik samostatných karet a přihlašovacích prostředků tak lze nahradit jediným centrálně spravovaným nosičem identity.

Výhodou je také jednodušší správa celého životního cyklu identity. Při ztrátě karty, odchodu zaměstnance nebo změně jeho pracovní role lze přístupy rychle zablokovat a příslušná oprávnění či certifikáty zneplatnit.

I.CA je exkluzivním partnerem pro karty STARCOS v České republice a dokáže zajistit celé řešení – od volby vhodné kombinace čipových technologií přes personalizaci karty až po nahrání certifikátů a napojení na systémy organizace.

### CERTIFIKÁTY POD KONTROLOU

Bezpečnost digitálního prostředí však nestojí pouze na identitě uživatelů. Stejně důležitá je správa technologických certifikátů, které využívají servery, aplikace a další prvky IT infrastruktury.

S rostoucím počtem digitálních služeb přibývá také certifikátů, které je nutné evidovat, sledovat a včas obnovovat.



*Zdroj: Obrázek byl vygenerován AI*

Opomenutí jediného z nich přitom může vést k nedostupnosti služby nebo komplikacím v provozu informačních systémů. GITRIX proto umožňuje certifikáty centrálně evidovat a sledovat, automatizovat jejich obnovu a distribuci a poskytovat správcům přehled napříč celou infrastrukturou. Organizace tak získává kontrolu nejen nad identitami uživatelů, ale také nad technologickými identitami svých systémů.

## DŮVĚRA PROVÁZÍ DOKUMENT CELOU JEHO CESTOU

Ověřená identita uživatele a bezpečná infrastruktura tvoří základ, na který navazují další služby vytvářející důvěru. Elektronický podpis umožňuje ověřit identitu podepisující osoby a integritu dokumentu. Elektronická pečeť dokládá původ a integritu dokumentu vydaného organizací. Kvalifikované časové razítko pak prokazuje, že konkrétní data existovala v dané podobě v určitém čase.

Tyto nástroje provázejí elektronický dokument během celé jeho cesty – od vzniku nebo doručení přes ověření, zpracování a schválení ve spisové službě až po jeho odeslání občanovi či jiné organizaci.

Tím však jeho životní cyklus nekončí. Stejně důležité je zajistit dlouhodobou důvěryhodnost dokumentu při archivaci. Nestačí uchovat pouze jeho čitelnost. I po mnoha letech musí být možné doložit jeho původ a integritu a ověřit platnost elektronických podpisů, pečetí a časových razítek.

Právě zde se jednotlivé technologie propojují do jednoho celku. I.CA nabízí kvalifikované certifikáty, elektronické pečetě, časová razítka, vzdálené služby RemoteSign a RemoteSeal i nástroje pro ověřování a dlouhodobou archivaci elektronických dokumentů.

Jednotlivá řešení lze integrovat přímo do spisových služeb, agendových informačních systémů i portálů veřejné správy. Potřebné bezpečnostní a důvěryhodné procesy tak mohou probíhat na pozadí, aniž by zbytečně zatěžovaly uživatele. Ten se může soustředit především na samotnou agendu. Důvěra v digitálním prostředí totiž nevzniká jedním podpisem. Začíná už spolehlivým ověřením identity uživatele, pokračuje bezpečnou prací s dokumentem a jeho elektronickým podpisem či pečetí a končí až ve chvíli, kdy dokážeme jeho důvěryhodnost prokázat i po mnoha letech.

„S rostoucím počtem digitálních služeb se zvyšují také požadavky na jejich ochranu a důvěryhodnost. Naším cílem je zajistit, aby bylo možné každý důležitý elektronický dokument a digitální úkon spolehlivě ověřit dnes i s odstupem mnoha let," uzavírá Boris Kučera, obchodní ředitel segmentu veřejné správy, První certifikační autorita, a.s.


Boris Kučera,
ředitel odboru pro státní správu a samosprávu

Alexandr Jakobe,
obchodní manažer pro partnerský prodej

# Od spisové služby k digitálnímu ekosystému:

## Jak propojené systémy mění fungování veřejné správy

***Konference e-government 20:10 v Mikulově opět potvrdila svou pozici jednoho z nejvýznamnějších setkání odborníků na digitalizaci veřejné správy. Diskutovalo se o kybernetické bezpečnosti, legislativních změnách, umělé inteligenci i budoucnosti informačních systémů. Jedním z témat byla také otázka, jak budovat digitální prostředí organizací tak, aby jednotlivé systémy netvořily izolované celky, ale fungovaly jako jeden propojený organismus.***

Právě tomu se ve své přednášce Platforma GINIS – od atestované spisové služby k digitálnímu ekosystému věnoval Ladislav Mazač, ředitel sekce Strategický a projektový management společnosti Gordic. Jeho vystoupení nabídlo pohled na digitalizaci, která nekončí pořízením jednotlivých aplikací, ale stojí na jejich vzájemné provázanosti.

### ATESTACE JAKO SOUČÁST ŠIRŠÍ ZMĚNY

Významnou část prezentace věnoval Ladislav Mazač atestované elektronické spisové službě. Gordic se stal prvním dodavatelem v České republice, jehož řešení získalo atestaci. Podle něj je však splnění legislativních požadavků pouze jedním krokem na cestě k modernímu digitálnímu prostředí.

Přechod na atestovanou spisovou službu totiž neznamená jen nasazení nové verze systému. Do projektu vstupují historická data, návaznosti na další agendové aplikace i změny integračních rozhraní. Většina organizací navíc již elektronickou spisovou službu provozuje a disponuje vlastními procesy a dlouhodobě budovanými vazbami na další systémy. Úspěšná implementace proto vyžaduje připravenost celého informačního prostředí, nikoliv pouze samotné spisové služby.

### SPISOVÁ SLUŽBA JAKO PÁTEŘ ORGANIZACE

Jednou z hlavních myšlenek přednášky bylo přirovnání informačního systému organizace k lidskému organismu. Mazač označil spisovou službu za pomyslnou páteř, která propojuje ostatní části celku.

Vedle spisové služby však organizace využívají ekonomické systémy, personalistiku, mzdové agendy, registry i další specializované aplikace. Pokud fungují odděleně, vznikají duplicity dat, složité integrační vazby i vyšší náklady na správu. Proto Gordic vnímá GINIS nikoli jako soubor samostatných aplikací, ale jako platformu se společným technologickým základem. Jednotlivé části systému mohou využívat společná data, workflow, správu uživatelů i vazby na služby eGovernmentu.

Takový přístup přináší jednodušší správu, omezuje vznik nejednotných dat a snižuje množství integračních rozhraní, která musí organizace dlouhodobě provozovat. Významnou roli hraje i bezpečnost. Sdílené prostředí umožňuje efektivněji využívat zálohování, monitoring nebo další bezpečnostní mechanismy napříč celou platformou.

### UMĚLÁ INTELIGENCE JAKO PODPORA ROZHODOVÁNÍ

Významným tématem letošního ročníku byla také umělá inteligence. Podle Ladislava Mazače může ve veřejné správě pomáhat například při třídění podání, kontrole jejich úplnosti nebo přípravě podkladů pro další zpracování. Společnost Gordic proto rozvíjí platformu AIG 2.0 Agenda, která má podobné funkce postupně přenášet přímo do prostředí GINIS.



Současně však zaznělo důležité upozornění: umělá inteligence nemá nahrazovat odborný úsudek pracovníků veřejné správy. Jejím úkolem je především odbourávat rutinní činnosti, urychlovat práci s informacemi a poskytovat podporu při rozhodování.

## DIGITALIZACE JAKO CELEK

Vystoupení v Mikulově tak přineslo širší poselství než pouze informace o nových funkcionalitách nebo legislativních požadavcích. Spisová služba, ekonomické systémy, personální agenda či umělá inteligence bývají často řešeny odděleně. V každodenní praxi však pracují se stejnými daty, dokumenty i uživateli.

O úspěchu digitalizace proto nerozhoduje počet nasazených aplikací, ale schopnost jednotlivých systémů spolupracovat. Právě vytváření funkčních digitálních ekosystémů označil Ladislav Mazač za jednu z klíčových podmínek efektivní veřejné správy.

„Technologické trendy a digitalizace jsou nezadržitelné. Nebojujte proti nim," uvedl v závěru své přednášky. Na tuto myšlenku navázal výzvou, která vystihla hlavní sdělení celého vystoupení: budovat fungující ekosystémy jako propojené celky a hledat cesty ke spolupráci namísto vytváření dalších izolovaných řešení.

Myšlenky, které v Mikulově zazněly, tak nepředstavují jen technologickou vizi, ale stále více i praktickou potřebu moderní veřejné správy. Digitalizace totiž není o jednotlivých aplikacích. Je především o tom, jak je dokážeme propojit do funkčního celku.

GORDIC

# SPOLEHLIVÁ IT INFRASTRUKTURA jako pevný základ digitální veřejné správy

***Digitalizace veřejné správy klade na informační technologie stále vyšší nároky. Úřady a instituce potřebují sítě, které fungují spolehlivě, IT prostředí chráněné před kybernetickými hrozbami a nástroje, díky nimž mohou jejich týmy efektivně spolupracovat. Společnost Collapo se moderním IT řešením pro veřejnou správu věnuje již od roku 2016.***

## Veřejná správa a nároky na moderní IT

Instituce státní správy a samosprávy dnes řeší úkol, který se týká téměř každého úřadu: zajistit, aby jejich IT prostředí bylo spolehlivé, bezpečné a připravené na další rozvoj. Na stabilitě sítí a datových center závisí každodenní agenda, služby pro občany i komunikace mezi pracovišti. Současně roste význam ochrany dat a systémů před kybernetickými útoky a neoprávněným přístupem. Pro veřejnou instituci proto není důležitá jen samotná technologie, ale především partner, který ji umí navrhnout, zavést a dlouhodobě spravovat.

## Collapo: spolehlivý partner pro IT projekty

Collapo se zaměřuje na řešení v oblasti informačních technologií. Své projekty staví na zkušeném týmu profesionálů a důrazu na kvalitu.

Cílem je dodávat řešení, která jsou efektivní a dlouhodobě udržitelná. Hlavním zaměřením společnosti je již od roku 2016 veřejná správa.

## Čtyři oblasti, které tvoří ucelené IT prostředí

Portfolio Collapo pokrývá klíčové oblasti, na nichž stojí fungování moderní instituce:

**Síťová infrastruktura.**

Collapo nabízí komplexní řešení v oblasti návrhu, implementace a správy síťových systémů. Ty zajišťují spolehlivost, bezpečnost a vysoký výkon.

**Bezpečnostní řešení.**

Řešení v oblasti síťové bezpečnosti chrání IT prostředí před kybernetickými hrozbami, útoky a neoprávněným přístupem.

**Nástroje pro spolupráci.**

Platformy pro týmovou práci zjednodušují a zefektivňují týmovou práci bez ohledu na vzdálenost.

**Datová centra a cloud.**

Řešení pro správu, monitoring a optimalizaci datových center zajišťují jejich vysoký výkon, bezpečnost a efektivitu.

## Zkušenosti z prostředí státní správy a samosprávy

Collapo dlouhodobě spolupracuje s institucemi státní správy a samosprávy. Mezi jeho reference patří:

Ministerstvo vnitra České republiky

Ministerstvo spravedlnosti České republiky

Policie České republiky

Hasičský záchranný sbor České republiky

Digitální a informační agentura

Úřad pro ochranu hospodářské soutěže

Státní zemědělská a potravinářská inspekce

Institut postgraduálního vzdělávání ve zdravotnictví

Asociace krajů České republiky

Kraj VysočinaInstitucím, které hledají partnera pro rozvoj své IT infrastruktury, tak Collapo nabízí spojení technologické odbornosti se zkušenostmi z prostředí veřejné správy.

## Certifikovaný partner Cisco

Collapo je certifikovaným partnerem společnosti Cisco se specializacemi Collaboration, Services a Networking. V této roli navrhuje, implementuje a spravuje podnikové sítě, kolaborační platformy a datová centra, včetně řešení kybernetické bezpečnosti.
Technickou podporu a konzultace zajišťuje tým certifikovaných specialistů CCIE a CCNP.

## Na čem stojí spolupráce

Spolupráce se společností Collapo stojí na čtyřech principech:

- individuální přístup ke každému projektu;
- důraz na kvalitu a inovativní řešení;
- odborné know-how a zkušenosti z oboru;
- spolehlivost a férové jednání.

Institucím, které hledají partnera pro rozvoj své IT infrastruktury, tak Collapo nabízí spojení technologické odbornosti se zkušenostmi z prostředí veřejné správy.

collapo

Viktor Gyönyör
obchodní ředitel, Collapo
viktor@collapo.com

IS4 security
Feel Real Trust

VENDOR REPRESENTATIVE COMPANY

ČESKÁ REPUBLIKA · SLOVENSKO

# Bezpečnost veřejné správy stojí na partnerech, na které se dá spolehnout.

Zastupujeme světové výrobce kybernetické bezpečnosti. S certifikovanými partnery chráníme úřady, města, kraje i státní instituce.

CHANNEL! Awards 2025

**Distributor s přidanou hodnotou roku 2024 i 2025**

Ocenění jsme získali dva roky po sobě a hlasovali o něm partneři.

IT produkt

**IT produkt roku 2026**

Bitdefender GravityZone Business Security Enterprise – počtvrté za pět let.

## S čím vám můžeme pomoci

Útočníci stále častěji zneužívají legitimní nástroje a tradiční ochrana je nemusí včas odhalit. Proto vybíráme řešení, která chrání data i přístupy, odhalují útoky bez malwaru a zjednodušují správu. Zákazníkům pomáháme s nasazením i jejich efektivním využitím.

### Bitdefender

IT PRODUKT ROKU 2026

Bitdefender GravityZone spojuje prevenci, EDR/XDR a řízení rizik v jedné platformě. GravityZone PHASR pomocí AI dynamicky omezuje zneužitelné nástroje a akce podle chování uživatele, čímž snižuje útočnou plochu a pomáhá zastavit i útoky bez malwaru.

www.bitdefender.cz

### hexnode

Hexnode spojuje UEM, správu identit a zabezpečení endpointů v jedné platformě. Umožňuje centrálně spravovat zařízení, aplikace a aktualizace, vynucovat bezpečnostní politiky a podmíněný přístup a pomocí XDR rychleji odhalovat a řešit hrozby napříč firemním prostředím.

www.hexnode.cz

### netwrix

Firmy potřebují vědět, kde mají citlivá data, kdo s nimi pracuje a jak zabránit jejich úniku. Netwrix Endpoint Protector kombinuje DLP, kontrolu zařízení, eDiscovery a šifrování, aby chránil data na koncových bodech před nechtěným i úmyslným únikem – online i offline.

www.netwrix.cz

### miniOrange

miniOrange řeší roztříštěnou správu identit a přístupů napříč cloudem i vlastní infrastrukturou. Spojuje SSO, MFA, správu životního cyklu uživatelů, CIAM, PAM a UEM, takže organizace mohou centrálně řídit přístupy i zařízení, omezit bezpečnostní rizika a zjednodušit správu i audit.

www.miniorange.cz

### endian

Endian chrání IT i OT sítě před útoky a riziky vzdáleného přístupu. Spojuje UTM firewall, segmentaci, VPN a Zero Trust přístup k jednotlivým systémům se schvalováním a záznamem relací. Organizacím tak pomáhá zabezpečit kanceláře, výrobu i kritickou infrastrukturu a plnit požadavky NIS2 a IEC 62443.

www.endian.cz

## Domluvte si nezávaznou konzultaci

Naskenujte QR kód nebo navštivte
**www.is4security.cz**


**IS4 security s.r.o.**

Jordánská 391, 198 00 Praha 9

+420 245 501 800

info@is4security.cz

ORACLE

# AI nad veřejnými daty pod kontrolou.

## Oracle koncept pro bezpečnou veřejnou správu v éře generativní inteligence



### Oracle pro státní správu

Šest principů bezpečnostního modelu pro data, která vstupují do světa AI.

1. Méně komplexity, méně bezpečnostních hranic.
2. AI přichází k datům. Data zůstávají pod kontrolou.
3. Ochrana funguje přímo v databázi.
4. RAG, prompty a agenti získávají jen oprávněný přístup.
5. Stejný model ochrany v datacentru, cloudu i multicloudu.
6. Suverenita dat a regulatorní připravenost pro EU.

AI agent musí v databázi jednat jen v rámci svých oprávnění.

### AI otevírá nové cesty k citlivým datům

Rychlé nasazení RAG, agentů a přirozeného jazyka přináší hodnotu, ale i nové riziko. Ochrana dat přímo v databázi proto musí zůstat účinná nezávisle na tom, jaká AI nebo aplikační vrstva je právě používá.

### Veřejná správa potřebuje ochranu, která rozumí kontextu

Nestačí filtrovat výstupy AI. Oprávnění AI agentů musí odpovídat tomu, kdo data požaduje, proč je potřebuje a jak citlivá jsou. Tím lze bezpečně rozvíjet digitální a AI služby bez oslabení ochrany údajů.

### Bezpečnostní principy Oracle

**Jednotná datová platforma zjednodušuje bezpečný rozvoj digitálních služeb:** Organizace chrání různé typy dat i AI scénáře společnými pravidly. Snižuje tím provozní složitost, riziko nekonzistentních kontrol i čas potřebný pro zavádění nových služeb. Správci dat nebudují nový model ochrany pro každou aplikaci.

**AI pracuje s daty tam, kde jsou již chráněna:** RAG a AI Agenti běží v bezpečnostním kontextu databáze a využívají existující datové kontroly místo vytváření neřízených kopií informací. Organizace volí cloudový, privátní nebo hybridní model podle svých požadavků.

**AI agent jedná pouze v mezích oprávnění konkrétního uživatele:** Agent nesmí získat širší přístup než jeho zadavatel. Databáze sama rozhoduje, k jakým datům má zadavatel přístup – AI agent pracuje s jeho identitou a oprávněním. Bezpečnostní politika je oddělena od aplikační logiky. Pravidla zůstávají centrálně řiditelná, auditovatelná a nezávislá na jednotlivých aplikacích.

**Privátní AI a datová suverenita:** Private AI Services Container umožňuje provozovat modely a AI služby uvnitř bezpečnostního perimetru organizace a v izolovaném prostředí. Oracle EU Sovereign Cloud umožňuje volit model nasazení podle regulace i požadavků na evropskou datovou suverenitu.

### Důvěryhodná AI stojí na ochraně dat, ne pouze na kontrole dotazů a odpovědí.

AI agent přináší hodnotu jen tehdy, když přistupuje k datům v jasně vymezených hranicích a v kontextu identity konkrétního uživatele.

# ŽÍT VÍC *Premium*



Hodně jste toho dokázali. Zasloužíte si bankéře, který naslouchá vašim plánům a otevře dveře příležitostem.
S námi se komfort stává standardem.
Ať jde o spoření, promyšlené investování, nebo pohodlí na cestách. Začněte žít prémiově.

S investováním je spojené i riziko.

ČSOB Premium

Premium linka +420 499 900 900 | www.csobpremium.cz