

MADLA Ai

NAŠE DATA | NAŠE PRAVIDLA | NAŠE BUDOUCNOST

PRO IT ŘEDITELE A BEZPEČNOSTNÍ MANAŽERY

TECHNICKÁ ARCHITEKTURA A BEZPEČNOST

MADLA Ai – první česká multiplatforma AI pro stát a firmy. Z čeho se skládá, kudy tečou data, kde zůstávají a jak je chráníme.

OBSAH

01 Shrnutí
02 Architektura ve vrstvách
03 Tok dat a suverenita
04 Varianty nasazení
05 Bezpečnost I – identita, izolace, šifrování, audit
06 Bezpečnost II – obrana, zálohy, řízení modelů
07 Soulad s předpisy a provoz
08 Otevřeni spolupráci a kontakt

01 — SHRNUTÍ

SUVERÉNNÍ AI, KTEROU LZE PROVOZOVAT TAM, KDE DATA NESMÍ VEN.

Nejde o jednoho chatbota. Je to tým AI odborníků, který práci udělá a sám si ji zkontroluje.

MADLA Ai spojuje české úřední zdroje, vlastní LLM bránu, vyhrazené GPU v Česku a stovky specializovaných agentů do jedné platformy. Tento dokument popisuje její architekturu ve vrstvách, tok dat, varianty nasazení a technická i organizační bezpečnostní opatření. Ke každé schopnosti uvádíme stav: co je v provozu, co připravujeme a co nasadíme po dohodě.

NAŠE DATA

Data organizace leží na serverech v EU, nebo celá na serveru zákazníka za jeho firewallem (připravujeme). Na serveru zákazníka jde ven jen dotaz do rejstříku, v cloudu i dotazy na komerční modely.

NAŠE PRAVIDLA

Role, dvoufázové ověření a auditní záznam. Kontrolor u agentních úloh. Rozhodnutí vždy zůstává na člověku.

NAŠE BUDOUCNOST

Vlastní LLM brána a vyhrazené GPU v Česku. Vlastní český model, který dotrénujeme na evropském superpočítači LUMI.

125	2 004	790	2 232	10
MCP SERVERŮ	NÁSTROJŮ	AGENTŮ	SKILLS	OBOROVÝCH GENERÁLŮ

HLAVNÍ BODY PRO IT A BEZPEČNOST

IZOLACE ORGANIZACÍ V DATABÁZI

Data firem a úřadů oddělená řádkovou bezpečností. Při chybě se přístup odepře.

AUDITNÍ ZÁZNAM

Záznamy provázané kontrolními součty – dodatečnou úpravu odhalí ověření řetězce.

ZÁLOHY

Pravidelné šifrované zálohy mimo server s neměnitelným zámkem, cíle obnovy ve smlouvě.

IDENTITA A PŘÍSTUP

Dvoufázové ověření, role, zakládání účtů z firemního adresáře (SCIM 2.0).

AKTIVNÍ OBRANA

Blokování útočníků na hlavních serverech platformy, aplikační firewall a detekce za běhu.

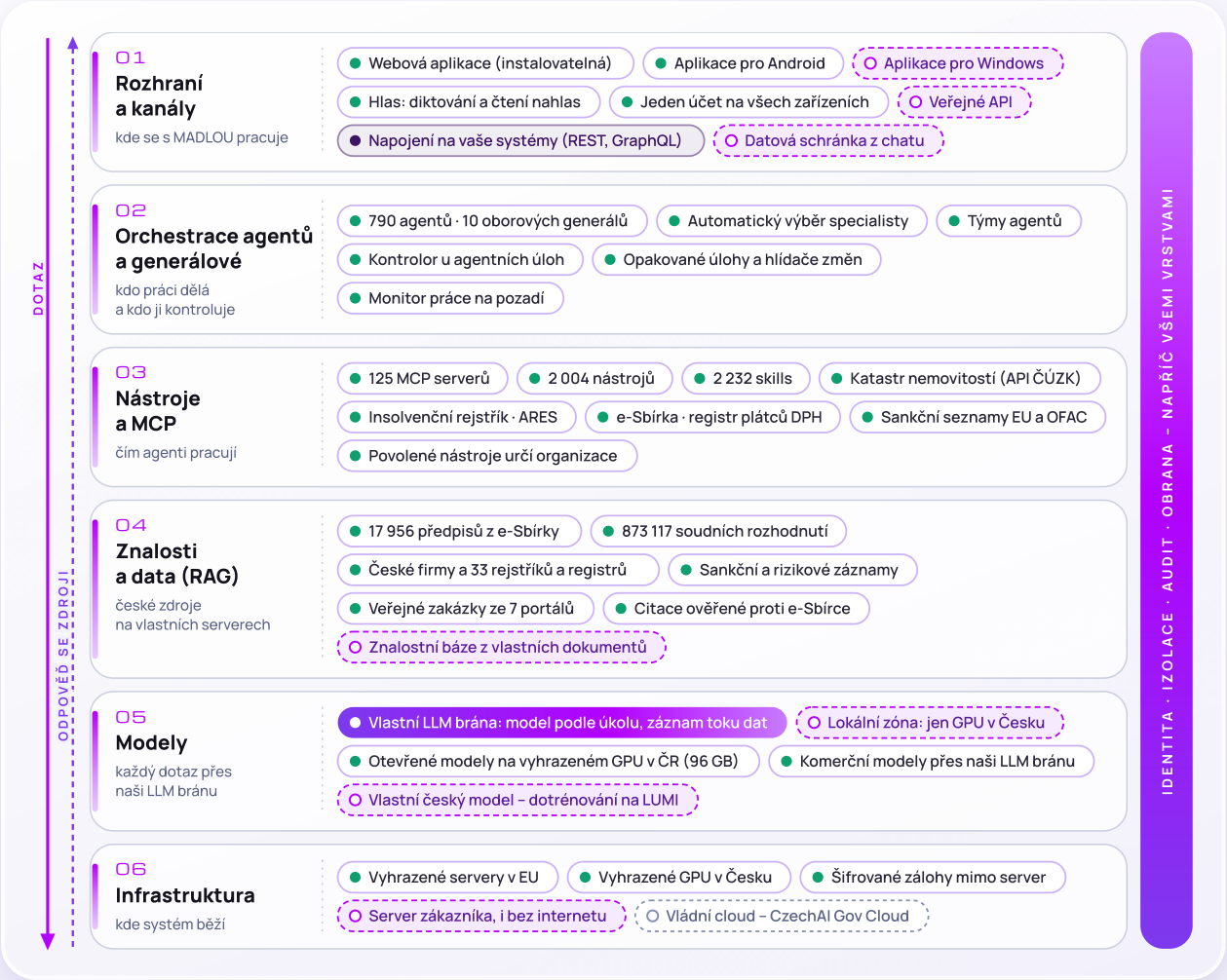
ŘÍZENÍ MODELŮ

Každý dotaz přes vlastní LLM bránu. Organizace volí povolené úrovně modelů a nástroje.

02 — ARCHITEKTURA

ŠEST VRSTEV, JEDNA PLATFORMA.

Dotaz prochází shora dolů, odpověď se vrací i se zdroji. Bezpečnost a audit platí ve všech vrstvách.



JAK ČTEME STAV — V PROVOZU · PŘIPRAVUJEME · PO DOHODĚ · NA ZAKÁZKU

PROČ VRSTVY

Každá vrstva má jednu odpovědnost a lze ji nasadit jinde: rozhraní v cloudu, data i modely u zákazníka. Logika agentů se při změně modelu nemění.

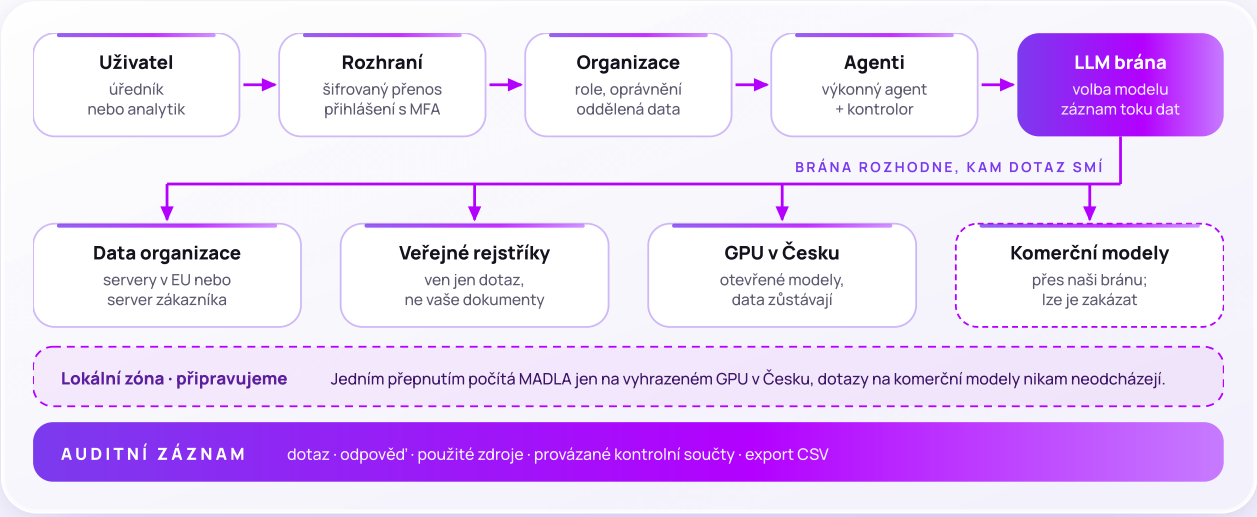
PROČ VLASTNÍ DATA

Rozdíl nedělá jen model, ale přístup k ověřeným datům. V našem benchmarku Skutek 2026 (971 českých pracovních úloh) dosáhl celý stack MADLY skóre 0,81, nejlepší z testovaných světových modelů s webem 0,55. Počty v diagramu k 28. 11. 2026, předpisy v platném i historickém znění.

03 — TOK DAT

KUDY DATA TEČOU A KDE ZŮSTÁVAJÍ.

Suverenita není slib, ale vlastnost architektury: o místě dat rozhoduje zvolené nasazení a pravidla organizace.



ÚDAJE	CLOUD MADLA V EU	SERVER ZÁKAZNÍKA ○ PŘIPRAVUJEME
Konverzace a soubory	na serverech v EU	v budově zákazníka, za jeho firewallem
Výpočet modelu	vyhrazené GPU v Česku; komerční modely přes naši bránu – organizace je může zakázat	model běží za firewallem zákazníka
Dotazy do veřejných rejstříků	odchází jen dotaz, ne dokumenty	jen dotaz a jen s povolením; provoz jde i bez internetu
Zálohy	šifrované, mimo produkční server, v EU	u zákazníka
Auditní záznam	v instanci organizace, export CSV	u zákazníka

SUVERENITA V PRAXI

- Úřední a firemní data jsou uložena jen ve zvoleném místě provozu: v EU, nebo v budově zákazníka.
- Organizace sama určí, které úrovně modelů a skupiny nástrojů smí její lidé používat. Zpracování výhradně na GPU v Česku zaručí lokální zóna (připravujeme).
- Vlastní LLM brána eviduje, kudy data tečou. Dohledatelnost toku dat je samostatná disciplína našeho benchmarku Skutek 2026.

04 — NASAZENÍ

TŘI VARIANTY NASAZENÍ.

Stejná platforma, stejní agenti. Liší se jen to, kde stojí hardware a kdo ho spravuje.

A — V PROVOZU

CLOUD MADLA V EU

Firemní prostor organizace ve sdílené platformě v EU, data oddělená v databázi. Vyhrazená instance na zakázku.

- zálohy, audit, šifrování a aktualizace zajišťujeme my
- modely na vyhrazeném GPU v Česku a komerční modely přes naši bránu
- start bez nákupu hardwaru

B — PŘIPRAVUJEME

SERVER ZÁKAZNÍKA

MADLA ve vaší budově, za vaším firewallem.

- provoz i v síti odpojené od internetu
- ven jde jen dotaz do veřejného rejstříku, a jen s povolením
- sestavy Kompakt, Medium, Big Box a Max (až 128 GB paměti GPU)
- 10 let aktualizací

C — PO DOHODĚ

VLÁDNÍ CLOUD

CzechAI Gov Cloud – sdílená národní AI infrastruktura.

- jeden stack pro tisíce úřadů, vlastní instance pro resort i kraj
- napojení na ISZR, datové schránky, eGON a základní registry
- pro celostátní nasazení od prvního dne

	A · CLOUD V EU	B · SERVER ZÁKAZNÍKA	C · VLÁDNÍ CLOUD
Kde leží data	servery v EU	budova zákazníka	státní infrastruktura
Kdo zajišťuje provoz	provozovatel MADLY	IT zákazníka, s naší podporou	centrálně pro všechny resorty
Připojení k internetu	ano	není nutné	podle bezpečnostní politiky státu
Modely	GPU v Česku + komerční přes bránu	model za firewallem zákazníka	katalog AI agentů a centrální znalostní báze

ZKUŠEBNÍ PROVOZ

Před nasazením lze MADLU vyzkoušet na naší infrastruktuře v EU s modely na GPU v Česku – s účty, rolemi a dvoufázovým přihlášením. Po skončení smažeme data z provozu ihned; lhůtu smazání ze šifrovaných záloh sjednáme ve smlouvě.

05 — BEZPEČNOST I

IDENTITA, IZOLACE, ŠIFROVÁNÍ, AUDIT.

Kdo smí dovnitř, čí data vidí, jak jsou chráněná a co po sobě každý krok zanechá.



IDENTITA A PŘÍSTUP

- Dvoufázové ověření: autentizační aplikace, kód e-mailem, záložní kódy. Organizace ho může nařídit všem.
- Role: vlastník, správce, člen a auditor; oddělení.
- Zakládání a rušení účtů z firemního adresáře (SCIM 2.0).
- Přehled přihlášených zařízení a odhlášení všude.
- Přístup podpory jen se svolením: 1–72 h, jen čtení, se záznamem.
- Jednotné přihlášení SSO (SAML, OIDC).
  PŘIPRAVUJEME

IZOLACE ORGANIZACÍ

- Firemní prostor oddělený od osobního.
- Data organizací oddělená v databázi řádkovou bezpečností.
- Aplikace běží pod rolí, která ochranu nemůže obejít. Kontext organizace se ověřuje u každého čtení i zápisu.
- Při chybě kontextu se přístup odepře (fail-closed).
- Oddělené vývojové prostředí pro každého uživatele.

ŠIFROVÁNÍ

- Šifrovaný přenos (HTTPS).
- Přístupové údaje k napojeným systémům (konektory MCP) uložené šifrovaně.
- Zálohy šifrované veřejným klíčem.

AUDIT A ZÁZNAMY

- Auditní záznam provázaný kontrolními součty; dodatečnou úpravu odhalí ověření řetězce.
- Záznam dotazů, odpovědí a použitých zdrojů; export CSV.
- Nastavitelná doba uchování dat.
- Systémové záznamy 90 dní a audit operačního systému.

06 — BEZPEČNOST II

OBRANA, ZÁLOHY, ŘÍZENÍ MODELŮ.

Útoky blokujeme, podezřelé chování hlásíme a výstupy AI kontrolujeme dřív, než je uvidí člověk.



AKTIVNÍ OBRANA A DETEKCE

- Automatické blokování útočníků na hlavních serverech platformy; zákazy sdílené mezi servery během minut.
- Webový aplikační firewall s virtuálními záplatami známých zranitelností (CVE).
- Detekce podezřelého chování za běhu s hlášením správcům do několika minut.
- Hlídání odchozího provozu databází.
- Centrální sběr a vyhodnocení bezpečnostních událostí (SIEM).
- Noční antivirové kontroly hlavních serverů a noční kontrola zabezpečení.

ZÁLOHY A OBNOVA

- Šifrované zálohy mimo produkční server.
- Trezor záloh s neměnitelným zámkem: 14 dní zálohu nelze změnit ani smazat.
- Cíle obnovy (RPO, RTO) sjednáme ve smlouvě.
- Sledování dostupnosti klíčových služeb a automatický restart procesů.

ŘÍZENÍ MODELŮ A OCHRANA PROTI ZNEUŽITÍ AI

- Každý dotaz jde přes vlastní LLM bránu: zvolí model pro úkol a eviduje tok dat.
- Organizace volí povolené úrovně modelů a skupiny nástrojů. Při výpadku může brána použít záložní model.
- Kontrolor u agentních úloh. Kontrolní skupina (oponent, hlídač čísel, sběrač důkazů, kontrola reality): připravujeme.
- Citace ověřené proti platnému znění e-Sbírky; lhůty počítané podle zákona, ne odhadem.
- Úvahy modelu se uživateli nezobrazují, odpověď má jednotnou identitu MADLY.
- Člověk rozhoduje: MADLA připravuje podklady, rozhodnutí je na úřednících.

1-72 h	14 dní	90 dní
přístup podpory jen se svolením	neměnitelný zámek záloh	uchování systémových záznamů

07 — SOULAD A PROVOZ

SOULAD S PŘEDPISY, PROVOZ A MONITORING.

MADLA je postavena tak, aby organizacím pomáhala plnit jejich povinnosti – ne aby je za ně přebírala.

GDPR
Osobní údaje

POSTAVENO S OHLEDEM · PODPORUJE

Data v EU, nebo celá u zákazníka. Role a oprávnění, nastavitelná doba uchování, smazání účtu (lhůtu smazání ze záloh sjednáme ve smlouvě), auditní záznam. Mimo EU může jít jen obsah dotazů na komerční modely; seznam subdodavatelů dodáme s nabídkou.

NIS2
Kybernetická bezpečnost

POSTAVENO S OHLEDEM · PODPORUJE

Provoz za firewallem zákazníka, i bez internetu (připravujeme). Role, dvoufázové ověření, které organizace může nařídit všem, záznam každého dotazu a odpovědi. Aktivní obrana, detekce, pravidelné šifrované zálohy, cíle obnovy ve smlouvě.

AI Act
Nařízení o umělé inteligenci

POSTAVENO S OHLEDEM · PODPORUJE

Člověk má poslední slovo. Odpovědi se zdroji a citacemi, kontrolor u agentních úloh, dohledatelnost v záznamech. Vzdělávání uživatelů: AI akademie a certifikace.

> Dokument popisuje technická a organizační opatření platformy. Není certifikací ani právním posouzením; soulad konkrétního nasazení posuzuje jeho provozovatel. Podklady pro posouzení bezpečnosti dodáme spolu s nabídkou.

PROVOZ A MONITORING

DOSTUPNOST
Sledování dostupnosti klíčových služeb a automatický restart procesů. Cíle obnovy (RPO, RTO) dohodneme ve smlouvě.

INCIDENTY
Hlášení správcům do několika minut a řízení incidentů.

VYDÁNÍ
Každé vydání se nasazuje s připraveným návratem k předchozí verzi a hlídají ho noční testy.

AKTUALIZACE
U serveru zákazníka 10 let aktualizací.

PODPORA
Přístup podpory k datům jen se svolením zákazníka, časově omezený a zaznamenaný.

ZÁLOHY
Pravidelné šifrované zálohy, cíle obnovy ve smlouvě.

08 — SPOLUPRÁCE

JSME OTEVŘENI SPOLUPRÁCI.

MADLA je platforma, na kterou se dá napojit. Rádi ji rozvineme s úřady, integrátory, distributory, výzkumem i zahraničními partnery.



S KÝM A JAK

STÁTY A ÚŘADY
Celostátní nasazení ve zvolené variantě: cloud v EU, server úřadu (připravujeme), nebo vládní cloud (po dohodě).

NA ZAKÁZKU
INTEGRÁTOŘI
Napojení MADLY na vaše systémy přes REST, GraphQL a webhooky.

NA ZAKÁZKU
FIRMY A VÝVOJÁŘI
Právník AI jako služba pro vaše agenty; weby a AI chatboty na zakázku.

V PROVOZU
DISTRIBUTOŘI A PARTNEŘI
Partnerský program MADLY pro ty, kdo platformu nabízejí dál.

PŘIPRAVUJEME
VÝZKUM
Dotrénování vlastního českého modelu na evropském superpočítači LUMI.

ZAHRANIČNÍ PARTNEŘI
Web v 8 jazycích, aplikace v češtině, angličtině a čínštině; státní verze pro Německo, Rakousko a Slovensko.

JAK ZAČÍT

01
Úvodní schůzka
Projdeme vaše bezpečnostní požadavky, variantu nasazení a napojení na vaše systémy.

02
Podklady k bezpečnosti
Podklady pro posouzení bezpečnosti dodáme spolu s nabídkou.

03
Zkušební provoz
Na naší infrastruktuře v EU s modely na GPU v Česku – s účty, rolemi a dvoufázovým přihlášením.

04
Nasazení
Ve zvolené variantě: cloud v EU, server zákazníka (připravujeme) nebo vládní cloud (po dohodě).

EVROPSKÁ SPOLUPRÁCE VE VÝPOČTU

EuroHPC JU přidělila 21. 9. 2026 po posouzení žádosti výpočetní čas na evropském superpočítači LUMI (Finsko). Na něm dotrénujeme vlastní český model.



KONTAKT

JSME OTEVŘENI SPOLUPRÁCI - OZVĚTE SE.

Rádi projdeme vaše bezpečnostní požadavky, variantu nasazení a napojení na vaše systémy. Podklady pro posouzení bezpečnosti dodáme spolu s nabídkou. Ukázky předvedeme na schůzce. Přehled 14 programů pro stát a 131 funkcí v 16 oblastech najdete v katalogu MADLY.

TECHNICKÉ A BEZPEČNOSTNÍ DOTAZY

ceo@czechai.io

NA WEBU

stat3.czechai.io

Přehled MADLA Ai

PROVOZOVATEL

A&L Prime s.r.o. (provozovatel CzechAI)
IČO 24009245 · Zámostní 1155/27, 710 00 Ostrava
Spisová značka C 101676 vedená u Krajského soudu v Ostravě

NAŠE DATA | NAŠE PRAVIDLA | NAŠE BUDOUCNOST

MADLA Ai