3. BLOK · AI, DATA A AGENTI

Vaše data zůstávají u vás. Plnohodnotná AI pro odvětví, kde je bezpečnost dat absolutní priorita

Artur Bergman · KnowYourData

Zápis z přednášky na konferenci IIČR 2026

Informace, inteligence a čas na rozhodnutí · 19. 11. 2026 · CEVRO Univerzita, Praha
AFCEA Česká pobočka, pracovní skupina PS07 Intelligence · CRIK při CEVRO Univerzitě
Stav 20. 11. 2026 · https://iicr.afcea.cz/zaznelo/



3. BLOK · AI, DATA A AGENTI

Artur Bergman

KnowYourData

Vaše data zůstávají u vás. Plnohodnotná AI pro odvětví, kde je bezpečnost dat absolutní priorita

---

Artur Bergman, spoluzakladatel a CEO startupu PactusAI, vystoupil jako zástupce domácích dodavatelů softwaru s umělou inteligencí. Podle něj je datová suverenita součástí kognitivní suverenity. Smluvní ochrana dat nestačí, rozhoduje technická kontrola nad tím, kde model běží. Kvalitní otevřené modely dnes lze provozovat na vlastní nebo evropské infrastruktuře.

Datová suverenita jako součást kognitivní suverenity

Řečník se představil jako spoluzakladatel a generální ředitel startupu PactusAI a uvedl, že na konferenci zastupuje dodavatele a startupy, které vyvíjejí software založený na umělé inteligenci. Ve firmě podle něj chápou datovou suverenitu jako součást kognitivní suverenity. Věří, že společnosti, které budou datově suverénní a s daty budou zacházet obezřetně, vytvářejí cestu k silnější a serióznější budoucnosti.

Jako výchozí problém uvedl zjištění, že až 80 % zaměstnanců firem, které zakazují nástroje jako ChatGPT nebo Claude, je přesto používá. Zaměstnavatel pak ztrácí přehled o tom, kam data tečou, a nad daty úplně ztrácí kontrolu.

Pět důvodů pro suverénní řešení

Prvním důvodem je mlčenlivost. Zaměstnance, subdodavatele nebo znalce lze smluvně zavázat a kontrolu vymáhat. Nelze ale smluvně zavázat ani kontrolovat poskytovatele vašich poskytovatelů, kteří jim dodávají jazykové modely. Pro řadu odvětví podle řečníka smluvní ochrana nestačí a často to říká i zákon. Datově obezřetná firma by se proto měla opírat především o technickou ochranu: pokud jazykový model a celý software běží u ní nebo v kontrolovatelném prostředí, je ochrana mnohem účinnější.

Druhým důvodem je prevence vynucených aktualizací a nestability produktů. Pokud dodavatel používá rozhraní cizího jazykového modelu a model se bez vědomí zákazníka změní, nemusí to být pro zákazníka správná cesta, i kdyby byl nový model kvalitnější nebo měl víc parametrů. Zákazník ztrácí kontrolu nad stabilitou výstupů, na které je zvyklý, ať jde o analýzy, nebo smlouvy, a to se může promítnout do celé firmy. Společnosti podle řečníka potřebují předvídatelnost a jistotu.

Třetím důvodem je ekonomika. Dodavatel, který má subdodavatele jazykových modelů a ti zase další dodavatele, uvrhává zákazníka do takzvaného vendor lock-inu. Jakékoli zdražení kdekoli v řetězci se objeví na faktuře a firma ho pak promítne do cen pro vlastní klienty. Kromě slabé pozice závislého zákazníka to snižuje konkurenceschopnost vůči firmám, které provozují datově obezřetnější řešení samy a jsou cenově nezávislé.

Čtvrtým důvodem je geopolitická dostupnost technologií. Řečník připomněl, že před několika měsíci americká administrativa v tehdy bezprecedentním kroku zakázala přístup k vybraným jazykovým modelům. Tím vznikl precedent: modely, které dodavatelé využívají přes rozhraní, lze vypnout a

systémy na nich postavené pak přestanou fungovat. Zmínil také případy, kdy se poskytovatelé jazykových modelů dostali na sankční seznam, a jako třetí geopolitické riziko digitální daň, která souvisí s ekonomickou stránkou věci.

Pátým důvodem je podpora českých startupů a firem, které technologii vyvíjejí doma. Ta podle řečníka posiluje národní suverenitu a zároveň zajišťuje, že data klientů zůstávají v zemi a neodcházejí do zahraničí.

Suverénní neznamená horší

Nejčastější námitkou, kterou firma slýchá, je, že suverénní řešení je horší. To podle řečníka už dlouho neplatí. Modely, které byly zveřejněny před několika měsíci, už tehdy zvládaly 99 % rutinních úkonů, které jeho tým pravidelně dělá. Právě takové modely se po několika měsících uvolňují jako modely s otevřenými vahami nebo jako open source. Modely, které tým v létě nadchly, dnes umí spustit na vlastní infrastruktuře.

Čtyři způsoby nasazení

Nejpřísnější a nejrobustnější je nasazení on-premise. Firmy si skládají vlastní technologický stack, kupují grafické karty a budují infrastrukturu přímo u sebe. Je to nejbezpečnější možnost, ale vstupní náklady jsou poměrně vysoké.

Druhou častou možností je cloud zákazníka, například AWS, Azure nebo Google Cloud, s podmínkou, že je hostován v Evropské unii. Třetí, podle řečníka zásadní možností jsou lokální datová centra, která po celé Evropě přibývají a provozuje je stát nebo soukromé subjekty. Jako velkého hráče uvedl České radiokomunikace, se kterými má PactusAI partnerství. Taková centra dávají zákazníkům prostor provozovat vlastní infrastrukturu pod vlastní kontrolou, data nikam neodcházejí a třetí strany se k nim snadno nedostanou. Čtvrtou možností je provoz u samotného poskytovatele softwaru, který je pak zpracovatelem dat. Minimem musí být hostování v EU.

Obezřetnost dovnitř a otázky pro dodavatele

Vedle těchto objektivních podmínek řečník zmínil i opatření uvnitř organizace: dobře nastavená oprávnění v lokálně provozovaných systémech, dobře ošetřené přihlašování a identity uživatelů a auditní záznam aktivity. Logováním nemyslel dohled nad každým krokem zaměstnanců, ale možnost sledovat, jak často a jak dlouho systém používají. Splnění objektivních i vnitřních požadavků označil za základní pilíře ochrany dat.

Téma se podle něj netýká jen regulovaných odvětví, jako je bankovnictví, pojišťovnictví, zdravotnictví, developerské projekty nebo advokacie, odkud má PactusAI řadu klientů. Zájem o bezpečnost dat vidí i u malých a středních podniků, na které se nevztahuje NIS2 ani DORA. Pro ně, protože mají jednodušší nákupní proces, formuloval šest otázek na dodavatele: kde modely fyzicky běží, jak dlouho se uchovávají vstupy a výstupy, zda dodavatel trénuje na datech zákazníka, kdo jsou jeho subdodavatelé a kde sídlí, jakým právem se smlouva řídí a kdo rozhoduje o změně verze modelu. Dodavatelé, kteří nejsou datově obezřetní, budou podle řečníka mlžit nebo dávat neuspokojivé odpovědi a řešením je pak datová suverenita. S odkazem na předřečníka Martina Uhra a jeho poznámku o lenosti uzavřel, že stačí chtít: možnost volby má každý.

Dotazy: velikost firmy, návratnost a role státu

Moderátorka se zeptala, od jak velké firmy dává vlastní provoz smysl, protože si neumí představit, že by si server pro kvalitní umělou inteligenci postavila doma pod stůl. Podle řečníka nejde o velikost firmy, ale o priority. Vstupní náklady už nejsou takovou překážkou jako před několika měsíci. Nemusí to být hned tak levné jako ChatGPT za 20 eur, ale lze si pořídit vlastní instanci Azure s volbou umístění a Nvidia už vyrábí cenově dostupnější grafické karty pro stolní počítače.

Na doplňující otázku, zda existuje jednoduchá metodika, jak spočítat, že se to vyplatí, řečník odpověděl, že odpověď je subjektivní a má tři roviny: jak citlivá data firma má a jak moc nechce, aby do nich někdo nahlížel, jak ji investice na určitou dobu finančně omezí a jaký princip firma zastává. Pro malou firmu nebo jednotlivce může být přínosem i jen dobrý pocit, že data nikdo nečte. Čím větší firma a čím citlivější data, tím je přínos zřetelnější.

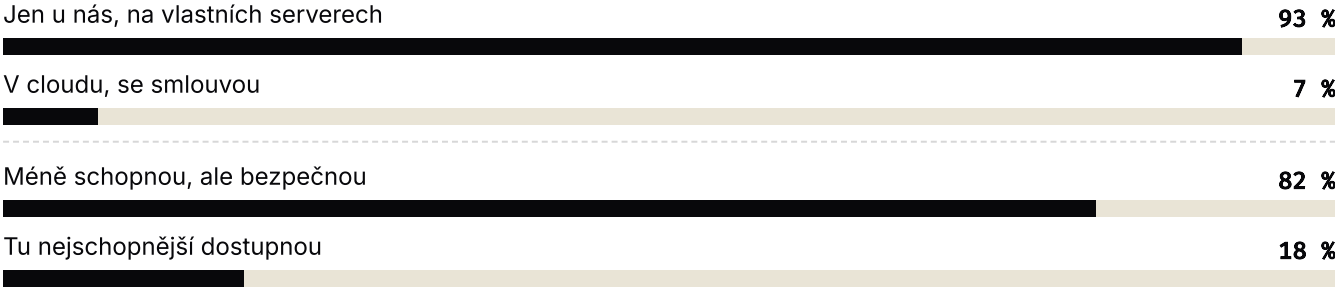
Moderátor Jakub Bareš se zeptal, co by měl stát v této oblasti dělat, včetně regulace, v době agentních útoků na digitální infrastrukturu. Řečník uvedl, že je zastáncem spíše menší regulace a minimalistického státu. Pomoci by podle něj mělo vzdělávání: podobně jako u zákazů nástrojů ve firmách, které 80 % zaměstnanců stejně obchází, nefunguje nařizování. Klíčem je vzdělaná společnost, ve které lidé sami pochopí, proč je téma důležité, místo aby jim to někdo vnucoval. Dodal, že až o data přijdou, bude to bolet.

Co z přednášky plyne pro stát

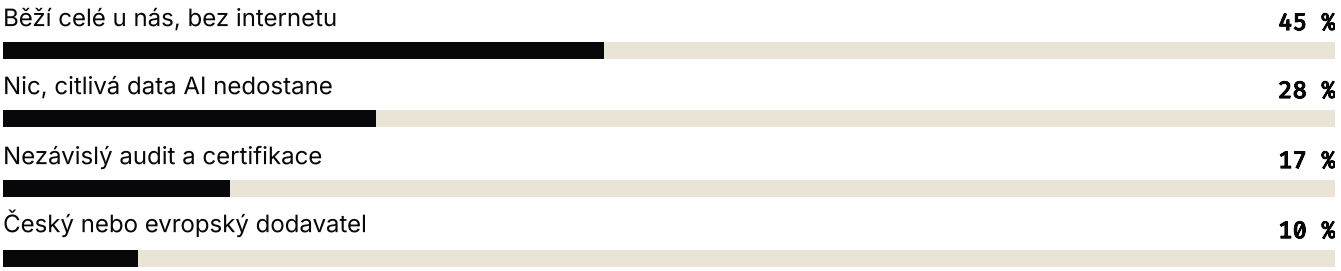
- Smluvní ochrana dat u dodavatelů umělé inteligence nestačí, protože se nevztahuje na jejich poskytovatele jazykových modelů. Rozhoduje technická kontrola nad tím, kde model a software běží.
- Americký zákaz přístupu k vybraným jazykovým modelům a sankční seznamy podle řečníka ukazují, že systémy postavené na zahraničních rozhraních lze vypnout. Jde o geopolitické riziko dostupnosti, ke kterému se přidává digitální daň.
- Podpora českých startupů a firem, které vyvíjejí umělou inteligenci doma, podle řečníka posiluje národní suverenitu a udržuje data v zemi.
- Lokální datová centra (řečník uvedl České radiokomunikace) a hostování v EU umožňují provozovat otevřené modely pod vlastní kontrolou. Hostování v EU označil za minimum.
- Místo regulace řečník doporučil, aby stát podporoval vzdělávání. Zákazy nástrojů nefungují, protože je většina zaměstnanců obchází.

Co řekl sál

Jakou AI pustit na nejcitlivější data? `n = 28, kompas: dvě osy`



Co by vás přesvědčilo pustit AI na nejcitlivější data vaší organizace? n = 29



Otázky ze sálu poslané přes aplikaci

- Jake modely doporučujete aby zákazník provozoval lokálně ? Úroveň lokálních modelů zatím nedosahuje kvality top modelů. Také modely které je možné provozovat často jsou vyvinuté v Číně. Jaké má současný zákazník v EU možnosti?

Zápis pořadatelů ze strojového přepisu, ne autorizovaný text řečníka. Citace zveřejníme až po schválení řečníkem. Opravy: ps07@afcea.cz.

Čtení pořadatelů, ne společné stanovisko řečníků. Zápisy vycházejí ze strojového přepisu konference, ankety vyjadřují názor sálu, ne reprezentativní průzkum. Citace řečníků zveřejníme až po jejich schválení. Opravy a dotazy: ps07@afcea.cz. Volně k použití s uvedením zdroje „IICR 2026, AFCEA Česká pobočka“. Více na https://iicr.afcea.cz/zaznelo/