

Hívatlan hallgatóság? A felhőalapú AI veszélyei és lokális megoldások a gyakorlatban

2026. 09. 08. 11:00

MKIK Prompt Aréna

HUN · 40 perc

**Gál Tamás**

Alapító · SafeScribe

Gál Tamás, a SafeScribe alapítója és technológiai vezérigazgatója szerint a szervezeteknek túl kell lépniük az AI-ról szóló hype-en, hogy kritikusan értékeljék az adatvédelmet, a szuverenitást és a felhőalapú és helyi AI-megoldások közötti architekturális különbségeket.

MIRŐL VOLT SZÓ

Gál Tamás kiemeli, hogy a modern mesterséges intelligencia szolgáltatások, mint például a találkozó összefoglalók, összetett adatfeldolgozást igényelnek, ahol a hangfelvételeket külső szerverekre küldik elemzésre nagy nyelvi modellek által. Hasonlóságot von a közösségi média korához, megjegyezve, hogy míg a felhasználók egykor önként osztottak meg személyes tartalmakat, az AI most belső gondolatokat és „vibe kódolást” beszélgetéseket rögzít külső kérés nélkül. Például a felhasználók gyakran osztanak meg érzékeny kódnaplókat vagy személyes adatokat olyan modellekkel, mint a Claude vagy a Gemini, anélkül, hogy tudatában lennének annak, hogy ezeket az adatokat harmadik felek dolgozzák fel.

A prezentáció a felhőalapú és a helyi AI közötti különbséget vizsgálja, hangsúlyozva, hogy a helyi megoldások teljes adat-szuverenitást kínálnak azáltal, hogy az összes feldolgozást privát hardveren végzik. Gál Tamás bemutatja, hogy egy helyi transzkripció rendszer összefoglalókat és feladatlistákat generálhat anélkül, hogy bármilyen adat elhagyná a belső infrastruktúrát. Például egy helyi beállítás futtat egy Mac Mini M4-en 32 GB RAM-mal, hogy érzékeny banki biztonsági megbeszéléseket kezeljen. Ezek az elemek együttesen azt jelentik, hogy a felhő és a helyi AI közötti választás stratégiai architekturális döntés, amely a szükséges ellenőrzési és biztonsági szinttől függ.

KIEMELT MEGÁLLAPÍTÁSOK

- A felhőalapú mesterséges intelligencia szolgáltatások gyakran akár 30 napig is tárolják az adatokat, még ideiglenes csevegési funkciók használata esetén is.
- A Microsoft Teams vállalati licencelése nem feltétlenül védi az adatokat, ha külső résztvevők személyes ügyleteket használnak.
- A helyi AI modellek finomhangolhatók javított átiratokon, hogy jobban megértsék az adott iparág szaknyelvét.

ÜZLETI HATÁS

A vállalati hatás középpontjában a kockázatkezelés és az üzemeltetési hatékonyság áll, különösen az EU AI-törvényének és az általános adatvédelmi rendeletnek (GDPR) való megfelelés tekintetében. A helyi AI alkalmazásával a vállalatok elkerülhetik az adat-helyben tartózkodással járó jogi bonyolultságokat és az „flex routing” kockázatait, amikor az adatokat automatikusan nem EU-beli adatközpontokba helyezik át. Ez a megközelítés lehetővé teszi egy olyan zárt vállalati tudásbázis létrehozását, ahol a belső interakciók, például jogi egyeztetések vagy műszaki előírások objektíven rögzíthetők és kereshetők, anélkül, hogy a védett információkat harmadik fél szolgáltatóknak kellene kiadni.

KÖVETKEZTETÉS

Gál Tamás azzal zárja, hogy felszólítja a szervezeteket, hogy fontolják meg egy döntési mátrix használatát, amely a következőket méri: az adatok érzékenysége, hozzáférhetősége és a lehetséges szivárgás következményei, mielőtt kiválasztanák az architektúrát. Azt javasolja, hogy a vállalatok értékeljék ki, hogy teljes mértékben ellenőrizni akarják-e az adatáramlást, vagy elfogadják a felhő kényelmét. A végső tanulság az, hogy a legfontosabb tényező nem az, hogy egy vállalat mit kérhet az AI-től, hanem hogy mit hajlandó megosztani vele.

Uninvited Listeners? The Risks of Cloud- Based AI and Practical Local Solutions

2026. 09. 08. 11:00

Prompt Arena

HUN · 40 perc

**Tamás Gál**

founder · SafeScribe

Tamás Gál, founder and CTO of SafeScribe, argues that organizations must move beyond the hype of AI to critically examine how data is processed, stored, and controlled during interactions with large language models.

WHAT WAS DISCUSSED

Tamás Gál explains that modern AI interactions, such as "vibe coding" or using tools like ChatGPT, Gemini, and Claude, involve sharing internal thoughts and code without explicit requests for data collection. He highlights three primary channels of interaction: text, audio, and imagery, noting that audio is becoming increasingly prominent as users seek automated meeting summaries and task lists. For example, a user might share a private corporate meeting's audio with an AI to receive an instant summary and action items.

The presentation contrasts cloud-based AI with local AI solutions, emphasizing that cloud services often involve complex data routing and third-party access. Tamás Gál demonstrates that local AI can run on consumer hardware, such as a Mac Mini M4, to ensure that sensitive data never leaves the organization's infrastructure. These elements suggest that choosing between cloud and local architectures is a strategic decision based on the need for data sovereignty and security. For example, a local setup allows for the creation of a private knowledge base from internal meetings and documents without exposing them to external servers.

KEY TAKEAWAYS

- Cloud AI services may route data to different geographic regions automatically through features like flex routing.
- Local AI models can run on standard hardware like a Mac Mini M4 to maintain 100% data privacy.
- The EU AI Act focuses on risk management and transparency rather than strictly limiting data processing to the European Union.

BUSINESS IMPACT

The practical application of these technologies involves a decision matrix for companies to evaluate data sensitivity, access rights, and the consequences of potential leaks. By implementing local AI, organizations can build objective knowledge bases that eliminate disputes over meeting details and provide a secure way to handle sensitive information like bank security incidents. This approach allows for a healthy mix of cloud frontier models for general tasks and local models for proprietary data, potentially reducing long-term costs and risks.

CONCLUSION

Tamás Gál concludes by urging the audience to consider not just what they can ask AI, but what they are willing to tell it. He recommends that organizations evaluate their specific needs and security requirements to decide whether to adopt cloud or local architectures. He encourages a conscious approach to AI adoption where data control remains a primary priority.