

MCP: adatbiztonság

Ez az oldal azt írja le, hogy az [MCP hozzáférés](#) használatakor **milyen adat hagyja el a rendszert**, mi védi a hozzáférést, és mit érdemes a cégnek eldöntenie a bevezetés előtt.

A legfontosabb: az adat elhagyja a rendszert

<note warning>Az MCP kapcsolat lényege, hogy egy **külső AI-alkalmazás** kérdezi az eVIR-t. Amit az AI lekérdez, az **átkerül az AI szolgáltatójához** — ugyanúgy, mintha a felhasználó kimásolná a képernyőről és beillesztené egy chatbe.

Az eVIR technikai védelmei azt szabályozzák, **ki mit kérdezhet le**; azt nem tudják megakadályozni, hogy a lekérdezett adat az AI szolgáltatójánál feldolgozásra kerüljön.</note>

Emiatt a bevezetés **nem csak technikai döntés**. Érdemes a cégnek előre tisztáznia:

- melyik AI-szolgáltató elfogadható (hol tárol, mit tanít az adatból, milyen szerződéssel),
- mely felhasználók kapjanak MCP privilégiumot,
- személyes adatot tartalmazó lekérdezések (partneradatok, TMS, dokumentumok) esetén az adatvédelmi tájékoztató lefedi-e ezt az adattovábbítást.

A felhasználónak ezért kell az engedélyezéskor **adattovábbítási nyilatkozatot** elfogadnia. A nyilatkozat verziózott: ha a szövege változik, a felhasználóknak újra el kell fogadniuk.

Amit az eVIR oldala garantál

- **Jogosultsági kötés.** Minden hívás annak a felhasználónak a nevében fut, aki engedélyezte, és ugyanazon a jogosultság-ellenőrzésen megy át, mint a webes felület. Amihez a felhasználónak nincs joga, azt az AI sem éri el — **a jogosultsági kör szűkíthet, de sosem bővít.**
- **Nincs törlés.** Egyetlen funkció sem tud törölni, semmilyen formában. Az írás piszkozat és megjegyzés szintű.
- **Nincs szabad lekérdezés.** Az AI egy rögzített funkciólistából választ, szabad SQL nincs — lásd [Elérhető funkciók](#).
- **Nincs tömeges kinyerés.** Minden lekérdezés kötelező sorlimittel fut, a válasz mérete korlátozott, és a hívásszám percenként korlátozott.
- **A dokumentumok tartalma nem megy ki.** A dokumentumkeresés csak metaadatot ad vissza; a fájl letöltése a felületen, bejelentkezve történik. A privátnak jelölt dokumentumok nem jelennek meg.
- **Teljes naplózás.** Minden hívás — a jogosultság hiánya miatt elutasított is — bekerül a [hívásnaplóba](#).

Amit a hozzáférés véd

- **Az AI-alkalmazás soha nem látja a jelszót.** A felhasználó a saját eVIR-bejelentkezésén megy át (jelszó-szabályok, naplózás, zárolás, kétlépcsős azonosítás — mind érvényes), az alkalmazás csak egy utólag visszavonható kulcsot kap.
- **Nyers kulcs nem kerül az adatbázisba**, csak annak egyirányú lenyomata. Egy elloptott adatbázis-mentésből tehát nem lehet működő hozzáférést visszaállítani.
- **A hozzáférési kulcs rövid életű** (alapértelmezés: 8 óra), a megújító kulcs pedig **rotálódik**: minden használatkor új születik, a régi azonnal érvénytelen.
- **Újrahasznált megújító kulcs = riasztás.** Ha ugyanazt a kulcsot kétszer használják fel — ez elloptott kulcsra utaló jel —, a rendszer a **teljes láncot** visszavonja.
- **A kulcs példányhoz kötött.** Egy hozzáférési kulcs nem használható másik eVIR példányon.
- **Csak előre bejegyzett címre lehet visszatérni** az engedélyezés után, és a kérés-visszatérés párosítás kriptográfiailag kötött — így egy engedélyt nem lehet máshová eltéríteni.

- **Az MCP privilegium minden hívásnál ellenőrzésre kerül.** Elvétele **azonnal** megszünteti a felhasználó összes élő hozzáférését.

Mi kerül naplóba és mi nem

- Naplóba kerül: időpont, felhasználó, alkalmazás, funkció, szűrőfeltételek, a visszaadott sorok száma, futásidő, hiba, IP cím.
- **Nem** kerül naplóba: a válasz tartalma, és a szabad szövegű bemenetek (megjegyzés-szövegek) — azokról csak a hossz látszik. A hibaüzenetekből a kulcsnak látszó értékek kimaszkolásra kerülnek.

Részletesen: [MCP hívásnapló](#).

Ajánlott gyakorlat

1. **Adj MCP privilegiumot szűken**, csak azoknak, akiknek tényleg kell.
2. **Kezdd csak olvasás körrel.** Írási kört akkor engedélyezz, ha a piszkozat-készítés tényleg része a munkafolyamatnak.
3. **Nézd át rendszeresen** a [kliensek](#) és a [kiadott hozzáférések](#) listáját — ismeretlen alkalmazás vagy régóta nem használt kapcsolat: tiltás, illetve visszavonás.
4. **Kilépő munkatársnál** a felhasználó tiltása mellett vedd el az MCP privilegiumot is, vagy vond vissza a hozzáféréseit.
5. **Rögzítsd a napló megőrzési idejét** a cég adatkezelési szabályzatában — a napló automatikusan nem törlődik.
6. **A hozzáférés kizárólag HTTPS-en** üzemeltethető.

Kapcsolódó oldalak:

- [eVIR MCP szerver \(áttekintés\)](#)
- [Elérhető funkciók \(toolok\)](#)
- [MCP hívásnapló](#)
- [Telepítés és üzemeltetés](#)
- [Jogosultsági rendszer](#)

From:

<https://doc.evir.hu/> - **eVIR tudásbázis**

Permanent link:

https://doc.evir.hu/doku.php/evir:rendszer:ai_mcp:adatbiztonsag

Last update: **2026/08/28 14:32**

