

Pilot to Control

Függőségi, kontroll- és kilépési térkép azoknak, akik AI-t bevezetnek

Dr. Kopasz János · AI Summit Budapest 2026 · Future Lab · v1, 2026. szeptember 7. — Tájékoztató anyag, nem jogi tanácsadás. A határidők a 2026. szeptember 7-i állapotot tükrözik.

Kinek szól: deployer — aki más AI-rendszerét saját szervezetében használja: vezetőnek, beszerzésnek, IT-nak, jognak. **Miért:** nem terméket vettünk, függőséget vettünk — és a kontrollt nem lehet kiszervezni.

1 • Észlelés — két szervezeti ábra

A board az első ábrát látja: minden doboznak van vezetője, és van egy AI-leltár a jóváhagyott rendszerekről. A cégben négy kategória működik:

- **Jóváhagyott** — amit tudatosan vettünk és bevezettünk.
- **Beágyazott** — ami a CRM-mel, a HR-rendszerrel, a böngészővel, a frissítéssel érkezett; senki nem „vette”.
- **Árnyék** — amit a kolléga a saját eszközén használ, céges adattal.
- **Ügynök** — ami maga hív eszközöket, hoz részdöntéseket, és jogosultsága van rendszerekhez.

Leltár mind a négyre; minden tételhez egy nevesített gazda (nem „IT / Legal / Business”). A kérdés, amit a boardnak fel kell tennie: **ki felel a második ábráért?**

2 • Öt kérdés — ujjszámolással

1. Milyen AI-rendszereket használunk ténylegesen?
2. Milyen adathoz férnek hozzá?
3. Mit tehetnek emberi jóváhagyás nélkül?
4. Kik állnak mögöttük harmadik félként?
5. Egy incidens után 24 órán belül rekonstruálni tudjuk, mi történt?

Ha mind az ötre nincs válasz, akkor még nincs AI governance. Csak AI van.

3 • Amit valójában megvettünk — szerződéses ellenőrzőlista

A számlán	Amit valójában vettünk	Mit kérjünk a szerződésbe
Alapmodell	csendben változik	változásértesítés előre; verziórögzítés vagy rollback; a beépített kontrolljaink túlélnek a frissítést
Felhő · régió	joghatóság	adatrezidencia, feldolgozási régió, támogatási hozzáférés helye
Vállalati adat · RAG	kint van	mire használható, tanításra nem; törlés és visszaadás; titoktartás a modellszolgáltató felé is
API · gépi identitás	tág mandátum	a jogosultság ne legyen nagyobb, mint a belső üzleti felhatalmazás; scope, lejárát, napló
Vendor · subprocessor	nem auditált	lista, értesítés a változásról, kifogásolási és auditjog
Frissítési jog	náluk	mi számít lényeges változásnak; ki dönt; tesztidőszak
Ár · funkció · modell	bármikor módosul	felmondási jog lényeges változásnál; funkció-megszűnés kezelése
Kilépés · hordozhatóság	nincs a papíron	export formátum, határidő, támogatás, adattörlés igazolása

Tétel: nyolc, plusz a függőség. A szállító „AI compliant” nyilatkozata rá vonatkozik, nem ránk: **a compliance nem öröklődik a licenccel.**

4 • Éles művelet — ami a kapcsolótábláról hiányzik

- **Ki kapcsolja le?** Nevesített személy, elérhető hétvégén is; a leállítás technikailag lehetséges és kipróbált.
- **Mi a fallback?** Emberi vagy korábbi folyamat, ami átveszi; mennyi időre.
- **Ki tud kilépni?** A kilépés nem szándék, hanem képesség: export, alternatíva, szerződéses jog.
- **Érdemi emberi döntés** ott, ahol a döntés jelentős hatással van emberre (GDPR 22. cikk): a döntés naplózva, a döntő nevesítve, a felülbírálás lehetséges. „Jelen volt egy ember” nem elég — az Uber-ügy erről szólt.
- **24 órás rekonstrukció:** mely modell, mely verzió, mely adat, mely jogosultság, mely emberi jóváhagyás — a naplókából, nem emlékezetből.

5 • A jog rétegei — deployerként

- **AI Act, ami már él:** AI-jártassági kötelezettség (4. cikk); tiltott gyakorlatok; átláthatóság — a chatbotnak meg kell mondania, hogy gép, a szintetikus tartalmat jelölni kell (50. cikk). **Ami később él:** a magas kockázatú rendszerek deployeri kötelezettségei (26. cikk; Annex III → 2027. december 2.; Annex I → 2028. augusztus 2.).
- **GDPR:** jogalap, adatvédelmi hatásvizsgálat, 22. cikk; a szállító mint adatfeldolgozó vagy önálló adatkezelő — tisztázva.
- **Munkajog és HR:** toborzás és szűrés, teljesítményértékelés, a munkavállalók ellenőrzésére alkalmas eszköz bevezetésénél az üzemi tanács jogai; diszkrimináció; a munkavállalói használat szabálya.
- **Üzleti titok:** a védelem feltétele az észszerű intézkedés. Ha bárki bemásolhat bármit egy külső eszközbe, és nincs szabály, a titok jogi minősége is elveszhet (2018. évi LIV. törvény).
- **Akadálymentesítés:** ha a chatbot fogyasztói felület része (webshop, banki, hírközlési), 2025. június 28. óta akadálymentességi követelmény alá esik.
- **Szerződés és termékfelelősség:** 2026. december 9-től a szoftver és az AI termék; a deployer igényérvényesítő lehet — de ha saját néven adja tovább, providerré válik.
- **NIS2:** az első magyar auditciklus tanulsága a hatóság közleménye szerint: a rendszerek dokumentáltsága gyakran hiányos. A határnap nem azonos a működési képességgel.
- **Vezetői felelősség:** a gondos eljárás dokumentálva. „A kolléga írta be a promptot” nem védekezés: kifelé a cég felel a teljes kárért; a munkavállalótól gondatlanság esetén legfeljebb négyhavi távolléti díj követelhető.

6 • Négy réteg — ettől lesz védhető egy AI-döntés

A szabályzat kimondja. A kontrollt, a gazdát, a tilalmakat. • **A szerződés kikényszeríti.** A szállítóval és a munkavállalóval szemben is. • **A technika végrehajtja.** Jogosultság, napló, leállítás. • **A bizonyíték megmutatja.** Hogy tényleg működött — a biztosító, a vevő, a hatóság és a bíróság nyelvén.

A szabályokat el lehet halasztani. A felelősséget nem. A kontrollt pedig nem lehet kiszervezni. • drkj.hu