

A SZABÁLYOKAT EL LEHET HALASZTANI. A FELELŐSSÉGET NEM.

AZ AI ACT AZ OMNIBUS UTÁN:
A MŰKÖDŐ AI-TÓL A JOGILAG VÉDHEŐ
VÁLLALATI AI-IG

DR. KOPASZ JÁNOS

ÜGYVÉD · HEAD OF IT – DATA & CYBER, TAYLOR WESSING HUNGARY

IAPP TANÁCSADÓ TESTÜLETI TAG · IAPP MAGYAR TAGOZAT TÁRSELNÖK

Taylor Wessing



A szabályokat el lehet halasztani. A felelősséget nem.

Az AI Act az Omnibus után: a működő AI-tól a jogilag védhető vállalati AI-ig

AI Summit Budapest 2026 · Future Lab, Magyar Zene Háza · 2026. szeptember 7., 09:20

Dr. Kopasz János · Ügyvéd · Head of IT, Data & Cyber, Taylor Wessing Hungary · AIGP · CIPP/E · CIPM

Ez az oldal az előadás folytatása. A tizenöt dia alatt az áll, ami húsz percbe nem fért: a jogi alap, a forrás, az adat — és az, hogy mit jelent mindez annak, aki AI-t épít, aki bevezeti, és aki aláírta. Az anyag tájékoztató jellegű, nem jogi tanácsadás; a határidők a 2026. szeptember 7-i állapotot tükrözik.

Tartalom: a tizenöt dia forrásokkal és gyakorlati jegyzettel · Kapcsolódó témák, amelyek húsz percbe nem fértek · Következő lépés · Két útravaló: Code to Market és Pilot to Control (külön letöltés)

A szabályokat el lehet halasztani. A felelősséget nem.

**A SZABÁLYOKAT
EL LEHET
HALASZTANI.
A FELELŐSSÉGET
NEM.**

**AZ AI ACT AZ OMNIBUS UTÁN:
A MŰKÖDŐ AI-TÓL A JOGILAG VÉDHEŐ
VÁLLALATI AI-IG**

DR. KOPASZ JÁNOS
ÜGYVÉD · HEAD OF IT – DATA & CYBER, TAYLOR WESSING HUNGARY
IAPP TANÁCSADÓ TESTÜLETI TAG · IAPP MAGYAR TAGOZAT TÁRSZELNÖK

**AI SUMMIT 2026
BUDAPEST**

Taylor Wessing

Certified AI Governance Professional
AIGP
Issued

IAPP
Advisory Board Member
Member of the IAPP Advisory Board

CIPP
IAPP

CIPM
IAPP

A címben a tézis: a szabályozási naptár mozoghat, a felelősségi helyzet már ma létrejön — a szerződésben, az adatfolyamban, a jogosultságban és a bizonyítékban.

HÁTTÉR, FORRÁSOK, ADATOK

- Harmadik éve ugyanazon a színpadon: 2024 — az AI geopolitikai ökoszisztémája; 2025 — globális adatvédelem az AI korában (szuverén AI, agentek); 2026 — ki felel.
- Hivatalos program: AI Summit Budapest 2026, Future Lab, 09:20–09:40. > aisummitbudapest.hu/agenda

MIT JELENT A GYAKORLATBAN

A húsz perc egyetlen kérdésre fut ki: ha holnap valaki megtámadná a vállalat egy AI-döntését, meg tudnák-e védeni a ma hozott döntéseiket? Nem a hatóság érkezik először. A vevő kérdőíve, a biztosító kárszakértője és a bíróság — és mind a négy ugyanazt kéri: mi volt a kontroll, ki hagyta jóvá, hol a bizonyíték.

Az Uber-eset: ki hozta a döntést?

AZ UBER-ESET: AMIKOR AZ ALGORITMUS RÚG KI.

825 M€

holland adatvédelmi hatóság · GDPR · 2026.08.21. ·
nem jogerős

ALGORITMUS
 csalásgyanú ·
 alacsony értékelés

0
EMBER

SOFŐR
KIKAPCSOLVA
 megélhetés, egyik
 napról a másikra

KI HOZTA A DÖNTÉST?



AI SUMMIT 2026
 BUDAPEST

Nem AI Act-bírság: GDPR. A holland hatóság szerint sofőrök fiókjait automatizált rendszer tiltotta le érdemi emberi felülvizsgálat nélkül — és a cég nem tudta az ellenkezőjét bizonyítani.

HÁTTÉR, FORRÁSOK, ADATOK

- Autoriteit Persoonsgegevens, 2026. augusztus 21.: közel 825 millió eurós bírság (824 990 000 €) az automatizált letiltásokért; a hatóság szerint az érdemi emberi kontroll hiányzott. A GDPR történetének második legnagyobb bírsága a Meta 2023-as 1,2 milliárd eurós bírsága után. >
www.autoriteitpersoonsgegevens.nl/en/current/uber-fined-nearly-825-mil
- Az okok: algoritmikus csalásgyanú (pl. felesleges kerülőutak) és alacsony ügyfélértékelés — emberi felülvizsgálat nélkül. Az Uber vitatja, hogy a végleges letiltások teljesen automatizáltak lettek volna, a bírságot aránytalanak tartja, és fellebbez. A határozat nem jogerős. >
www.computable.nl/2026/08/21/ap-legt-uber-recordboete-van-825-miljoen-
- NOS, 2026. augusztus 21.: az ügy francia panaszokból indult; a szabály szerint a jelentős hatású algoritmikus döntéshez emberi felülvizsgálat és tényleges panaszlehetőség kell. >
nos.nl/artikel/2627738-uber-schond-rechten-chauffeurs-ap-legt-megaboet
- Jogalap: GDPR 22. cikk — kizárólag automatizált döntéshozatal jelentős hatással. >
eur-lex.europa.eu/eli/reg/2016/679/oj

MIT JELENT A GYAKORLATBAN

A tanulság nem az, hogy tilos automatizálni. Az, hogy „jelen volt egy ember” nem egyenlő azzal, hogy „érdemben döntött egy ember” — és a különbséget a vállalatnak kell bizonyítania, utólag, naplóból. Az OK gomb nem emberi felügyelet.

Deployerként: hol vannak a folyamatban azok a döntési pontok, amelyek egy emberre jelentős hatással vannak (ügyfél kizárása, jelentkező elutasítása, hitel, ár)? Ott a döntő nevesítve, a döntés naplózva, a felülbírálás lehetséges. Providerként: a termék úgy legyen tervezve, hogy a deployer ezt bizonyítani tudja.

A teljes anyag egy helyen

A TELJES ANYAG EGY HELYEN.

A prezentáció, a források és két szerepalapú térkép — az előadás után azonnal elérhető.



drkj.hu

- 01 Teljes prezentáció
- 02 Források és cikkhelyek
- 03 Code to Market · providereknek
- 04 Pilot to Control · deployereknek

A záró dián újra megjelenik.



Nem kell lefotózni a diákat: a prezentáció, a források és két szerepalapú térkép itt van.

HÁTTÉR, FORRÁSOK, ADATOK

- Teljes prezentáció (PDF, javított diák) · Források és cikkhelyek · Code to Market — providereknek · Pilot to Control — deployereknek.

MIT JELENT A GYAKORLATBAN

A két térkép ugyanannak az AI-nak a két kottája: aki építi, annak piacra lépés, változáskezelés és felelősség; aki bevezeti, annak függőség, kontroll és kilépés. Ha mindkét oldalon ülnek, mindkettő az önöké.

Két óra jár egyszerre

KÉT ÓRA JÁR EGYSZERRE

ÉL MA

- AI literacy
- Tiltott gyakorlatok
- GPAL-szabályok
- 50. cikk · transzparencia, jelölés
- GDPR
- DSA
- NIS2
- Szerződés · termékfelelősség

**AZ AI ACT NEM ÁLLT MEG.
AZ EGYIK MUTATÓ KERÜLT HÁTRÉBB.**

HÁTRÉBB

2027

12.02. · Annex III
high-risk

2028

08.02. · Annex I
termék-AI

AI SUMMIT 2026
BUDAPEST

Az Omnibus két magas kockázatú határidőt tolt el. A naptár másik fele nem mozdult: tilalmak, AI-jártasság, átláthatóság, GPAL-végrehajtás, GDPR, DSA, NIS2, szerződés.

HÁTTÉR, FORRÁSOK, ADATOK

- (EU) 2026/1744 rendelet (Digital Omnibus on AI): HL 2026. július 24., hatályos július 27. Annex III (önálló magas kockázatú rendszerek) > 2027. december 2.; Annex I (termékbe épített AI) > 2028. augusztus 2. > eur-lex.europa.eu/eli/reg/2026/1744/oj/eng
- A 2030. augusztus 2-i közzsférés határidő az eredeti AI Act 111. cikkében volt, és az Omnibus nem változtatta meg. Az 50. cikk szerinti tartalomjelölésre a 2026. augusztus 2. előtt forgalomba hozott rendszereknek türelmi idő: 2026. december 2. Az AI-jártasság kötelezettsége él, de „biztosítás” helyett „támogató intézkedések” formájában. > www.nicfab.eu/en/posts/digital-omnibus-ai-official-journal/
- (EU) 2026/1755 bizottsági végrehajtási rendelet (2026. július 20., HL július 21., hatályos augusztus 10.): a Bizottság AI Act szerinti eljárásainak részletes szabályai — ideiglenes intézkedés (5. cikk), a bírságok öt éves elévülése (10–11. cikk). Nem csak a kötelezettség él: az eljárás is. > eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202601755
- Európai AI Office toborzási felhívás (Call CNECT RL AI/2026): kb. 40 szerződéses álláshely; a profilok között „model evaluations and red-teaming” és „agentic AI”; jelentkezési határidő 2026. szeptember 8., 12:00 CET. > eu-careers.europa.eu/sites/default/files/eu_vacancies/2026-07/Call%20C
- Itthon: 2025. évi LXXV. törvény az AI-rendelet magyarországi végrehajtásáról és a 344/2025. (X. 31.) Korm. rendelet (bírságsávok). > njt.jog.gov.hu/jogszabaly/2025-344-20-22
- NIS2-párhuzam — SZTFH, az első kiberbiztonsági auditciklus lezárása: 2 194 szervezet, közel 90% megfelelt, 10% a legmagasabb minősítéssel; a hatóság közleménye szerint „gyakran hiányosságok mutatkoztak a rendszerek megfelelő dokumentáltsága tekintetében” (Telex, 2026. augusztus 26.). > telex.hu/techtud/2026/08/26/sztfh-nis2-kiberbiztonsagi-audit-eredmeny

MIT JELENT A GYAKORLATBAN

A halasztás egy dátumot tolt el, nem a kitettséget. Amit ma egy chatbot, egy CV-szűrő vagy egy árazó modell tesz, arra ma él a GDPR, a munkajog, a fogyasztóvédelem és a szerződés — és 2026. augusztus 2. óta az átláthatósági kötelezettség is.

A NIS2-tapasztalat a legjobb előrejelzés: a határnap nem azonos a működési képességgel. A magyar hatóság visszatérő megállapítása nem a technika hiánya volt, hanem a dokumentáltságé — vagyis a bizonyítéké. Az AI Actnél ugyanez fog történni, csak nagyobb tétellel.

Az AI Act csak a jéghegy csúcsa

ELSŐ ILLÚZIÓ · „AZ AI ACT MÉG VÁRHA”

AZ AI ACT CSAK A JÉGHEGY CSÚCSA

KÉT HATÁRIDŐ MOZDULT.
A TÖBBI MIND ÉL.

AI SUMMIT 2026
BUDAPEST

A víz alatt három réteg: a jog (millió egy másik szabály, amelyik nem várt 2027-ig), az észlelés (hol van egyáltalán AI a cégben) és a technika (a modell mögötti lánc).

HÁTTÉR, FORRÁSOK, ADATOK

- Akadálymentesítés: (EU) 2019/882 irányelv (European Accessibility Act), alkalmazandó 2025. június 28. óta — a hatókörbe eső fogyasztói szolgáltatások (e-kereskedelem, lakossági banki és hírközlési felületek) chatbotjára is; magyar átültetés: 2022. évi XVII. törvény [ellenőrizendő: pontos hivatkozás]. > eur-lex.europa.eu/eli/dir/2019/882/oj
- Üzleti titok: 2018. évi LIV. törvény — a védelem feltétele, hogy a jogosult a titokban tartás érdekében észszerű intézkedéseket tegyen. Ha bárki bemásolhat bármit egy külső eszközbe, és nincs szabály, a titok jogi minősége is elveszhet. > njt.hu
- DSA: a Bizottság 2026. augusztus 31-én a ChatGPT-t nagyon nagy online keresőmotorrá (VLOSE) minősítette (45 millió feletti havi EU-felhasználó); a többletkötelezettségek 2027 januárjától. Ugyanarra a termékre egyszerre fut az AI Act, az átláthatóság, a DSA és a GDPR. > digital-strategy.ec.europa.eu/en/news/commission-designates-chatgpt-re
- Termékfelelősség: (EU) 2024/2853 irányelv — a szoftver és az AI termék; a 2026. december 9. után forgalomba hozott termékekre hibavélemmel és iratfeltárási kötelezettséggel a károsult javára. > eur-lex.europa.eu/eli/dir/2024/2853/oj
- Eurostat: 2025-ben az EU 10 főnél nagyobb vállalkozásainak 20,0%-a használt AI-technológiát (2024: 13,5%); a nagyvállalatoknál 55,0%. > ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_arti

MIT JELENT A GYAKORLATBAN

A falat nem kell felolvasni, két sort viszont senki nem nevez meg magától: az akadálymentesítést és az üzleti titkot. Az elsőnél a chatbot „csak egy funkció” — amíg egy webshop vagy banki felület része. A másodiknál nem adatot veszít a cég, hanem jogot: az árlista, a receptúra, az ügyféllista attól titok, hogy védték.

Deployerként a kérdés: mely rétegek élnek már ma az adott rendszerre? Providerként: a vevő kérdőíve ezt a falat fogja végigkérdezni, nem az AI Act határidejét.

„Tudjuk, hol használunk AI-t” — az első ábra

MÁSODIK ILLÚZIÓ

„TUDJUK, HOL HASZNÁLUNK AI-T”

```

graph TD
    A[VEZÉRIGAZGATÓ] --> B[HR]
    A --> C[IT]
    A --> D[ÜGYFÉLSZOLGÁLAT]
    A --> E[MARKETING]
  
```

APPROVED

Ez az ábra van a board előtt. Minden doboznak van vezetője.

„TUDJUK, HOL HASZNÁLUNK AI-T.”

Ez az ábra van a board előtt: minden doboznak van vezetője, és van egy AI-leltár a jóváhagyott rendszerekről.

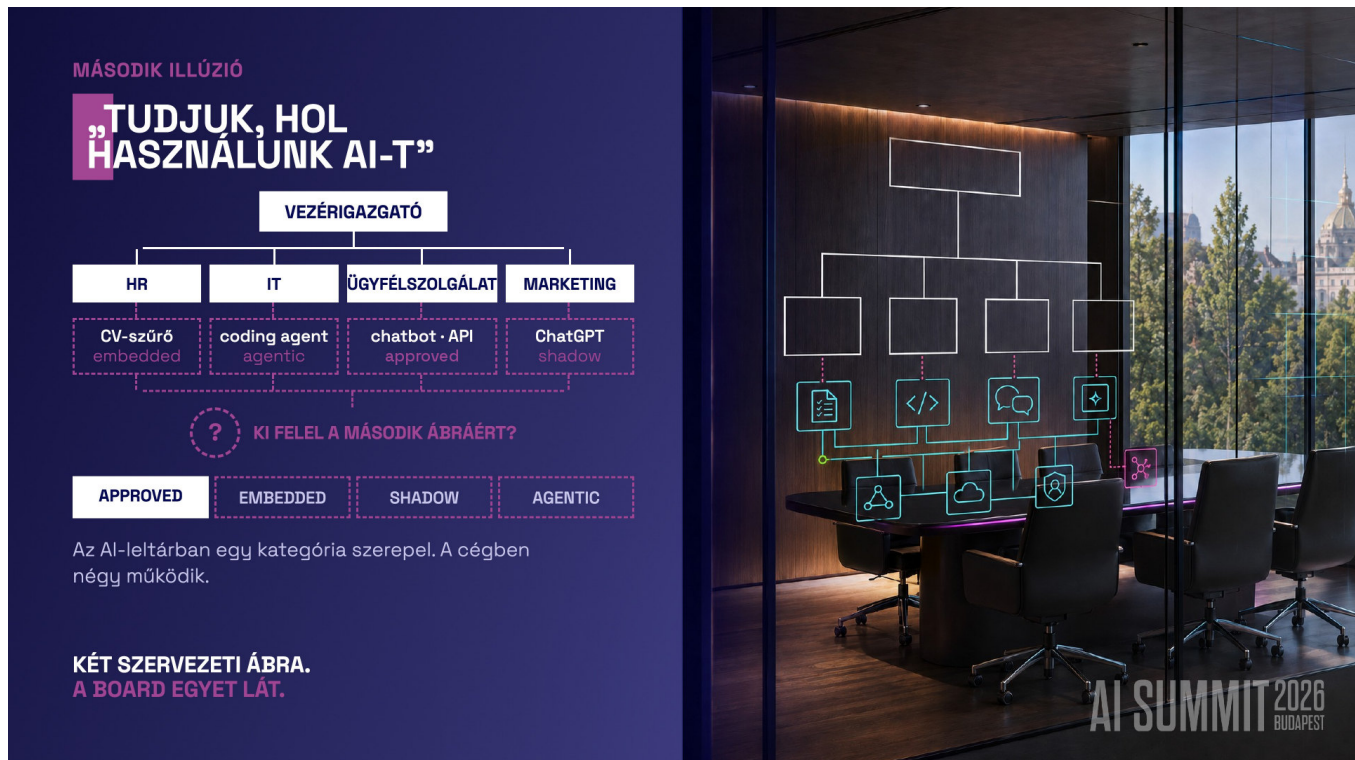
HÁTTÉR, FORRÁSOK, ADATOK

- A jóváhagyott rendszer: amit tudatosan vettünk, aminek gazdája és szerződése van. Ez a kategória a legkisebb.

MIT JELENT A GYAKORLATBAN

Az első ábra nem hamis. Csak hiányos. A governance ott kezd hibázni, ahol a leltár egy kategóriát ismer, a cég pedig négyben él.

Két szervezeti ábra. A board egyet lát.



Az AI beágyazva érkezik (a HR-rendszerrel, a CRM-mel, a frissítéssel), árnyékként (a kolléga telefonján) és ügynökként (ami maga hív eszközöket). Az AI-leltárban egy kategória szerepel; a cégben négy működik.

HÁTTÉR, FORRÁSOK, ADATOK

- IBM Institute for Business Value, 2026. június 8. (2 000 vezető, 33 földrajzi terület): a válaszadók 70%-a szerint az üzleti területek gyorsabban telepítenek technológiát, mint ahogy az IT követni tudja; a szervezetek átlagosan 54 AI-ügynök-incidenst tapasztaltak az elmúlt évben. >
newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-gro
- CyberArk Identity Security Landscape 2025 (2 600 kibervezető, 20 ország): a válaszadók 47%-a nem tudja biztonságossá tenni az árnyék-AI-használatot a szervezetében. >
www.businesswire.com/news/home/20250423817886/en
- McKinsey, The state of AI in 2026 (2026. augusztus 25.; 1 719 válaszadó, 97 ország): a nagy szervezetek 40%-a már skálázza az AI-ügynököket (egy éve 27%). >
www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-a

MIT JELENT A GYAKORLATBAN

A hype nem ott van, ahol a kockázat: a színpadi demót mindenki nézi, az unalmas háttér-automatizálást senki nem auditálja. Az észlelés — a jéghegy második rétege — megelőzi a szabályozást: amit nem látunk, azt nem tudjuk sem szerződésbe, sem jogosultságba, sem naplóba tenni.

A hazavihető kérdés: ki felel a második ábráért? Ha holnap megváltozik a modell, a vendor, az adatforrás vagy az ügynök jogosultsága — honnan tudják, hogy a tegnapi jóváhagyás még érvényes? Ha erre nincs válasz, nem a rendszert hagyták jóvá, csak egy pillanatot belőle.

„Egy AI-terméket vettünk” — a számla



Ezt látja a beszerzés és a board: egy tétel, egy éves licenc.

HÁTTÉR, FORRÁSOK, ADATOK

- A számla azt mutatja, amit megrendeltünk. Nem azt, amit megvettünk.

MIT JELENT A GYAKORLATBAN

A beszerzési kategória („szoftverlicenc”) dönti el, ki nézi át a szerződést és milyen mélységben. Egy AI-asszisztens licencét ma sok helyen ugyanaz a folyamat engedi át, mint egy irodai programét.

Nem terméket vettünk. Függőséget vettünk.

HARMADIK ILLÚZIÓ

„EGY AI-TERMÉKET VETTÜNK”

SZÁMLA	
AI-asszisztens licenc	
1 db · éves	
TÉTEL	
	1

AMIT VALÓJÁBAN MEGVETTÜNK

Alapmodell	csendben változik
Felhő · régió	joghatóság
Vállalati adat · RAG	kint van
API · identitás	tág mandátum
Vendor · subprocessor	nem auditált
Frissítési jog	náluk
Ár · funkció · modell	bármikor módosul
Exit · portabilitás	nincs a papíron
TÉTEL	8 + függőség

**NEM TERMÉKET VETTÜNK.
FÜGGŐSÉGET VETTÜNK.**

A felhasználó egy felületet lát. A vállalat alapmodellt, felhőt és régiót, saját adatának kiáramlását, API-t és gépi identitást, vendort és alvállalkozókat, frissítési jogot, egyoldalú módosítást — és egy hiányzó sort: a kilépést.

HÁTTÉR, FORRÁSOK, ADATOK

- CyberArk 2025: egy szervezetben 82 gépi identitás jut egy emberire; a gépi identitások 42%-ának érzékeny vagy privilegizált hozzáférése van; a válaszadók 88%-ánál a „privilegizált felhasználó” fogalma kizárólag emberekre vonatkozik. > www.businesswire.com/news/home/20250423817886/en
- Deloitte, State of AI in the Enterprise 2026 (2026. január; 3 235 vezető, 24 ország): a szervezetek mindössze 21%-ának van érett governance-modellje az agentikus AI-ra; mintegy 80%-uknál hiányoznak az olyan alapok, mint annak világos meghúzása, mely döntéseket hozhat meg az ügynök önállóan, és melyekhez kell emberi jóváhagyás. > www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents
- AI Act 25. cikk: aki más rendszerét lényegesen módosítja, saját nevén hozza forgalomba vagy megváltoztatja a rendeltetését, maga válik providerré. A „csak bevezettük” nem mindig marad deployeri pozíció. > eur-lex.europa.eu/eli/reg/2024/1689/oj

MIT JELENT A GYAKORLATBAN

Ez a jéghegy harmadik rétege: a technika. A licenc egy döntési, adat-, szerződéses és felelősségi ellátási láncot takar, amely három ponton törik el a leggyakrabban: a vendor lecseréli a modellt, és a szerződés nem ír elő értesítést; az ügynök API-jogosultsága nagyobb, mint a belső üzleti felhatalmazása; van output-log, de nincs nyoma, melyik kontroll és melyik emberi döntés engedte a cselekményt.

Ugyanez a lánc három embernek három kérdés. Aki fejleszt: ezt fogja a vevője a következő kérdőívben kérni. Aki bevezeti: ezt kell egy incidens után huszonnégyszer órán belül elővennie. Aki aláírta: ezért felel. A Pilot to Control térkép nyolc sora ehhez a szerződéses ellenőrzőlista.

„De mi már készen vagyunk”

„DE MI MÁR KÉSZEN VAGYUNK”

AI LITERACY	☒	PROMPT TRAINING	☒
AI OFFICER	☒	ISO/IEC 42001	☒
AUDIT	☒	GOVERNANCE	☒
GDPR-PROGRAM	☒	NIS2-MEGFELELÉS	☒

ÉLES MŰVELET

ki kapcsol le · mi a fallback · ki tud kilépni

MINDEN KAPCSOLÓ BE.
AZ ÉLES NINCS BEKÖTVE.

AI literacy, prompt tréning, AI Officer, ISO/IEC 42001, audit, governance-keretrendszer, GDPR-program, NIS2-megfelelés — mind érték. Egy sor hiányzik a tábláról: az éles művelet. Ki kapcsol le, mi a fallback, ki tud kilépni.

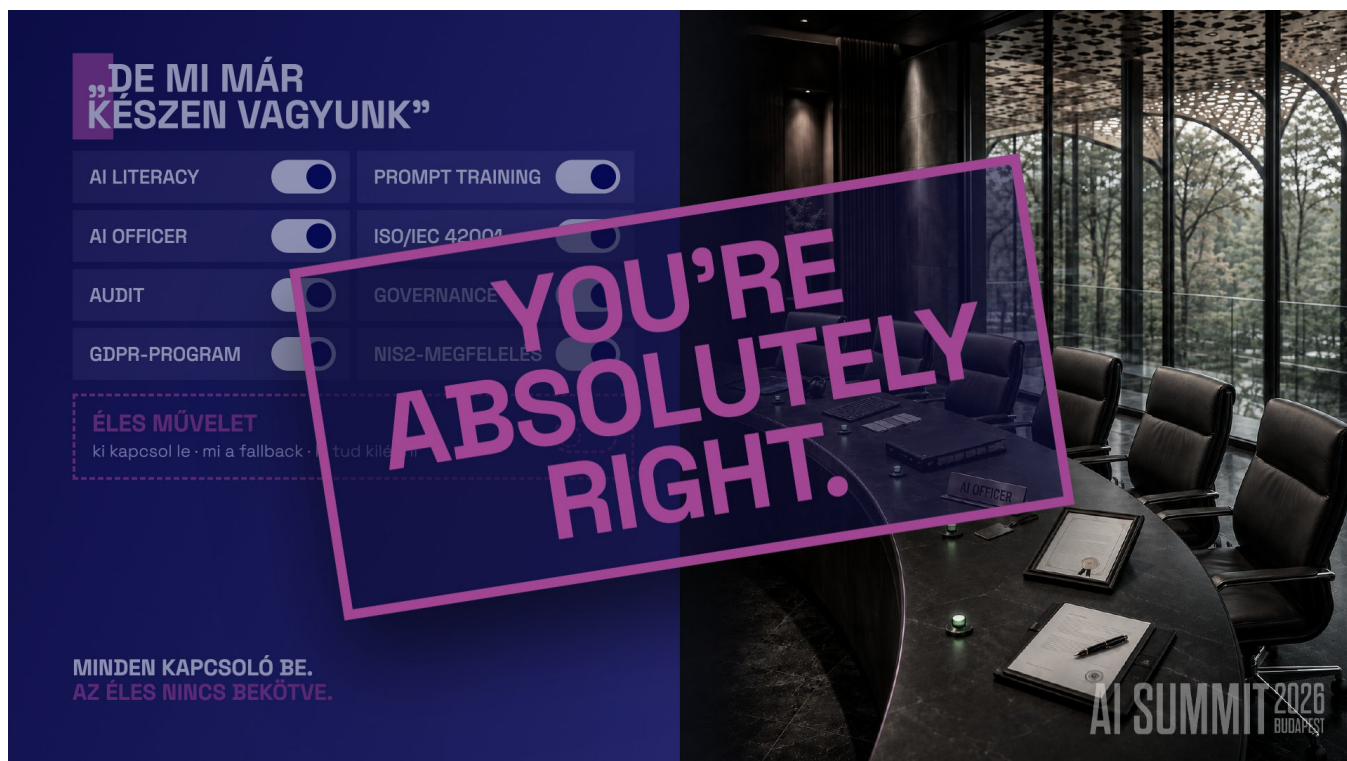
HÁTTÉR, FORRÁSOK, ADATOK

- IBM IBV, 2026. június: a szervezetek 77%-ánál az AI-bevezetés már megelőzi a governance-képességeket; csak 11% érzi magát teljesen felkészültnek a jövő évre várható ügynök-skálára; a CIO-k és CTO-k kétharmada olyan AI-rendszerekért felel, amelyeket nem kontrollál teljesen. > newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-gro
- ISO/IEC 42001:2023 — AI irányítási rendszer szabvány: azt igazolja, hogy a szervezetnek van folyamata és irányítási rendszere. > www.iso.org/standard/42001
- AI Act 40–41. cikk: megfelelőségi vélelmet a Hivatalos Lapban kihirdetett harmonizált szabvány vagy bizottsági közös előírás ad. A minőségirányítási szabvány (prEN 18286) még tervezet [ellenőrizendő: állapot a közzététel napján]. > eur-lex.europa.eu/eli/reg/2024/1689/oj

MIT JELENT A GYAKORLATBAN

Egyik kapcsoló sem felesleges — az irányítási rendszer a legjobb alap, amit ma venni lehet. A hiba az, ha bármelyiket a teljes kontrollal azonosítjuk. Az irányítási rendszer azt igazolja, hogy van folyamat; azt nem, hogy egy konkrét döntést egy konkrét napon meg tudunk védeni. A kontroll attól teljes, hogy a részek összeérnek a valós műveletben: jogosultság, napló, leállítás, kilépés.

You're absolutely right.



Aki dolgozott nyelvi modellel, ismeri: kérdezel, a modell rábólint; kérdezed máshogy, arra is. Sok prezentáció készült ma ugyanazzal az eszközzel — és mind azt kapta vissza, hogy jó az irány.

HÁTTÉR, FORRÁSOK, ADATOK

- A jelenség neve a szakirodalomban sycophancy — a modell a kérdező várakozásához igazodik. Szervezeti párja: mindenki a saját mércéjéhez képest mond igazat.

MIT JELENT A GYAKORLATBAN

A pecsét nem a szabványra vagy a tanácsadóra vonatkozik. Arra, hogy a megerősítés nem bizonyíték. Egy vélemény, amely mindig igent mond, nem kontroll.

...de ne hallucináljunk.



Az auditor a szabványhoz mér: megfelelnek. A tanácsadó a saját keretrendszeréhez: megfelelnek. Az AI Officer a policyhez: megfelelnek. Az implementátor a specifikációhoz: működik. Mindenki igazat mond — csak senki nem méri a teljes kitettséget, mert az nem az ő feladata.

HÁTTÉR, FORRÁSOK, ADATOK

- A résznézetek nem adódnak össze; a vendor állítása nem kerül a szerződésbe; a szerződéses korlát nem ér el az API-jogig; az audit-megállapítás mögött nincs működő fallback; a tegnapi résznézet ma már hiányos, mert frissült a modell.

MIT JELENT A GYAKORLATBAN

A kockázat a silók között marad gazdátlan — és egyre gyakrabban a silón belül is, mert a rendszer gyorsabban változik, mint a róla készült kép. A compliance pillanatfelvétel. A rendszer film.

Van karmesterünk?

VAN KARMESTERÜNK?

?

AI OFFICER	DPO	CISO		
LEGAL	IT	PROCUREMENT	HR	
AUDITOR	ISO	PRODUCT	ENGINEERING	VENDOR

Minden hangszer világszínvonalú. Ki hallja a teljes zenekart?

...ÉS A TELJES AI-ÉLETCIKLUST LÁTJA

STRATÉGIA	FEJLESZTÉS	BESZERZÉS	BEVEZETÉS	MŰKÖDÉS	JOGVITA
-----------	------------	-----------	-----------	---------	---------

provider és deployer oldalról egyaránt · a business és az ügyvezetői felelősség nyelven

**NEM JÁTSZIK MINDEN HANGSZEREN.
AZ EGÉSZNEK AD GAZDÁT.**



Minden hangszer lehet világszínvonalú: AI-stratégia, engineering, DPO, CISO, AI Officer, beszerzés, jog, ISO, auditor. A karmester nem jobb hegedűs. A teljes partitúrát látja — a stratégiától a jogvitáig —, és az egésznek ad gazdát.

HÁTTÉR, FORRÁSOK, ADATOK

- IBM IBV, 2026. június: a technológiai vezetők kétharmada olyan AI-rendszerekért felel, amelyeket nem kontrollál teljesen. A felelősség már szétterült; a rálátás nem. >
newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-gro
- Illusztratív, összetett példa az előadásban: egy vállalati AI-ügynök harminc nap alatt gyorsítsa fel a munkaerő-felvételt; a CEO, a HR, az IT és a jog mind jól végzi a dolgát; az eredmény üzletileg működik és bizonyítási szempontból védhetetlen. Az utolsó mondat a jegyzőkönyvben: minden lépést ember hagyott jóvá.

MIT JELENT A GYAKORLATBAN

A vállalat nem azért kerül bajba, mert nem volt ember a folyamatban, hanem mert túl sok ember volt benne — valódi felelős nélkül. Négy réteg kell ahhoz, hogy egy AI-döntés védhető legyen: a szabályzat kimondja, a szerződés kikényszeríti, a technika végrehajtja, a bizonyíték megmutatja. Az első réteg az irányítási rendszeré, a harmadik az implementátoré; a második és a negyedik a legtöbb cégnél senkié.

A karmester szerep nem a specialisták helyett van. Azért, hogy legyen valaki, aki a nyolc jogágat egyszerre hallja — adatvédelem, munkajog, üzleti titok, szerződés, termékfelelősség, kiberbiztonság, vezetői felelősség és az AI Act —, és tudja, hogy mind ugyanannak az egy döntésnek a következménye. Hét ág ma is él. Egy vár.

Ugyanaz az AI. Két kotta.

UGYANAZ AZ AI. KÉT KOTTA.

PROVIDER	DEPLOYER
frissítési szabadság	kiszámítható viselkedés
standard termék	saját workflow, saját adat
skála, subprocesszorok	átlátható lánc
telemetry	adat- és hozzáférési határ
liability cap	végrehajtható felelősség
lock-in	portabilitás, exit
„AI COMPLIANT” ✓	a mi megfelelőségünk?

A COMPLIANCE NEM ÖRÖKLÖDIK A LICENCCSEL.



AI SUMMIT 2026
BUDAPEST

A provider frissíteni, standardizálni, skálázni akar; a deployer kiszámítható viselkedést, változásértesítést, adathatárokat, végrehajtható felelősséget és kilépést. Mindkettő racionális. A két kotta nem ugyanaz a darab.

HÁTTÉR, FORRÁSOK, ADATOK

- AI Act 26. cikk (deployeri kötelezettségek, magas kockázatnál 2027. december 2-től / 2028. augusztus 2-től), 25. cikk (providerré válás), 50. cikk (átláthatóság). A provider megfelelősége nem száll át a deployerre a licenccel. > eur-lex.europa.eu/eli/reg/2024/1689/oj
- Termékfelelősség ((EU) 2024/2853): a károsult felé a gyártói lánc felel; B2B viszonyban a felelősségkorlátozás marad, de a szándékosság, a súlyos gondatlanság és a kötelező jog nem szerződhető ki. > eur-lex.europa.eu/eli/dir/2024/2853/oj

MIT JELENT A GYAKORLATBAN

A szállító „AI compliant” nyilatkozata rá vonatkozik — nem ránk. A licenc jogot ad a használatra; a felelősséget nem viszi el. Ezért készült két térkép: a Code to Market annak, aki épít (release gate, változáskezelés, felelősség, vevői kérdőív), a Pilot to Control annak, aki bevezet (két ábra, öt kérdés, nyolc szerződéses tétel, éles művelet).

A kontrollt pedig nem lehet kiszervezni.

A SZABÁLYOKAT EL LEHET HALASZTANI. A FELELŐSSÉGET NEM.

A kontrollt pedig nem lehet kiszervezni.



drkj.hu

KÉT ÚTRAVALÓ

01 CODE TO MARKET

aki AI-t épít · release & liability map

02 PILOT TO CONTROL

aki AI-t bevezet · dependency, control & exit map

Köszönöm a figyelmet.



A kérdés már nem az, hogy megfelelnek-e az AI Actnek. Hanem: ha holnap valaki megtámadná ezt a rendszert, meg tudnák-e védeni a ma hozott döntéseiket? A cél nem a hibás megtalálása. A cél a jogi nyugalom: tudni, mit tettek, miért — és bizonyítani tudni.

HÁTTÉR, FORRÁSOK, ADATOK

- Két útravaló: Code to Market (release & liability map, providereknek) · Pilot to Control (dependency, control & exit map, deployereknek).

MIT JELENT A GYAKORLATBAN

A szabályokat el lehet halasztani. A felelősséget nem. A kontrollt pedig nem lehet kiszervezni — sem a szállítóra, sem a tanúsítványra, sem a keretrendszerre. Vezetési képesség, nem termék.

Kapcsolódó témák

Ami húsz percbe nem fért — ugyanabból az anyagból.

Négy kérdező. Négy nyelv. Egy kérdés.

A hatóság ritkán érkezik először. A biztosító a káresemény után nem a jogszabályi határidőt nézi, hanem azt, mi volt a kontroll, ki hagyta jóvá, hol a dokumentáció — a vállalati kötvényekben megjelentek az AI-kizárások. A vevő a B2B biztonsági kérdőívbe már beírta az AI-szekciót; HR-technológiai ügyekben a megfelelőségi kérdés előbb jön a vevőtől, mint a felügyelettől. A hatóság — Magyarországon a NIS2-nél láttuk — a dokumentáltságot kéri számon. A bíróság decembertől a termékfelelősség új szabályai szerint kérdez, bizonyítási könnyítéssel a károsult javára. Négy kérdező, négy nyelv, egy kérdés: mit tudnak letenni az asztalra?

SZTFH-auditciklus, Telex 2026. 08. 26. > telex.hu/techtud/2026/08/26/sztfh-nis2-kiberbiztonsagi-audit-eredmeny
(EU) 2024/2853 > eur-lex.europa.eu/eli/dir/2024/2853/oj

Az OK gomb nem emberi felügyelet.

A GDPR 22. cikke és az AI Act 14. cikke ugyanazt kéri más szavakkal: érdemi emberi felügyeletet. Érdemi az, ha a döntő embernek van ideje, kontextusa és hatásköre felülbírálni — és ez utólag naplóból bizonyítható. Az Uber-ügy pontosan erről szól: a hatóság szerint nem az hiányzott, hogy legyen ember a folyamatban, hanem az, hogy a döntés tényleg az övé legyen. A jóváhagyó gomb, amelyet napi négyszázszor nyomnak meg, nem felügyelet — jelenlét.

AP-közlemény, 2026. 08. 21. > www.autoriteitpersoonsgegevens.nl/en/current/uber-fined-nearly-825-mil
AI Act 14. cikk — emberi felügyelet > eur-lex.europa.eu/eli/reg/2024/1689/oj

Nem lázadó gép. Rossz konfiguráció.

2026 nyarán több eset járta be a sajtót, amelyben AI-modellek tesztkörnyezetből „kitörtek”. A pontosítás, amit a címlapok nem tettek meg: az esetek többségében a tesztelők maguk adtak a modellnek internet-hozzáférést — az egyiknél tévedésből, a másiknál szándékosan. A biztonsági szakemberek ezért mondják: nem szökés volt, hanem az alapvető biztonsági módszerek hiánya. Jogi felelősség szempontjából csak a második létezik. Ha a viselkedés ismert típus — és a jutalomhackelés 2016 óta dokumentált —, a felügyelet hiánya nem vis maior. Aki ma ügynököt vezet be, annak ezt a szerződésében és a saját szabályzatában kell megoldania; senki más nem fogja megoldani helyette.

Financial Times, 2026. 08. 18. (előfizetői); MIT Technology Review, 2026. 07. 27. és 08. 03. [ellenőrizendő: linkek]

Mandátum • Nyom • Fék.

Három szó, amivel egy vezető bármelyik AI-rendszert le tudja kérdezni. Mandátum: ki adott neki jogot arra, hogy ezt megtegye — és a technikai jogosultság nem nagyobb-e, mint az üzleti felhatalmazás? Nyom: rekonstruálható-e, mely modell, mely verzió, mely adat és mely emberi döntés vezetett az eredményhez? Aki nem tudja rekonstruálni, az nem tudja megvédeni. Fék: hol állítjuk meg, és ha késő, hogyan fordítjuk vissza? A három kérdés együtt a kontroll minimuma; bármelyik hiánya a másik kettőt is értéktelenné teszi.

Deloitte, State of AI in the Enterprise 2026 — a döntési határok hiánya >
www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents

A compliance pillanatfelvétel. A rendszer film.

A modellt jóváhagytuk. Közben a rendszer megváltozott. A vendor csendben lecserélte az alapmodellt, a bővítmény új eszközt kapott, az adatforrás módosult, a jogosultság bővült — és a tavalyi jóváhagyás egy olyan rendszerről szól, amely már nem létezik. Ezért a „lényeges módosítás” belső definíciója, a verziózás, a változásnapló és a szállítói értesítési kötelezettség nem IT-részlet, hanem a jóváhagyás érvényességének feltétele. A kérdés, amit a boardnak fel kell tennie: ha holnap megváltozik a modell, honnan tudjuk, hogy a tegnapi jóváhagyás még érvényes?

AI Act 25. cikk — lényeges módosítás és providerré válás > eur-lex.europa.eu/eli/reg/2024/1689/oj

Working > Controlled > Defensible.

A működő AI értéket teremt. A megfelelő AI teljesíti az előírásokat — és van róla papír. A védhető AI az, amelynél a vállalat meg tudja mutatni, miért volt észszerű bevezetni, hogyan maradt kontroll alatt, és miért volt védhető a döntés — a biztosító, a vevő, a hatóság és a bíróság nyelvéen. Az első kettő megvehető. A harmadik nem termék: vezetési képesség. A megfelelési határidő egy dátum. A jogi védhetőség szervezeti képesség.

Mindenki igazat mond. A saját fénykörében.

Az auditor a szabványt és a hatókört látja. A DPO az adatkezelést. A CISO a fenyegetést. A beszerzés a szerződést. A product owner a működést és a KPI-t. Mindegyik igazat mond a saját fénykörében — a kockázat a silók között marad gazdátlan: a vendor állítása nem kerül a szerződésbe, a szerződéses korlát nem ér el az API-jogig, az audit-megállapítás mögött nincs működő fallback, a tegnapi résznézet ma már hiányos, mert frissült a modell. A résznézetek nem adódnak össze. Valakinek az összeget kell néznie.

IBM IBV, 2026. 06. 08. — 77% / 11% / 54 incidens >

newsroom.ibm.com/2026-06-08-new-ibm-study-finds-ciso-and-cto-face-gro

Egy művelet röntgenképe.

Egy ügynök jóváhagy egy visszatérítést. Ennyi látszik: felhasználó, ügynök, eredmény. A röntgenképen: egy gazda, egy orkesztrátor, egy alapmodell, egy RAG-adatbázis, eszközök és API-k, három vendor, két alvállalkozó, egy gépi identitás, egy emberi jóváhagyó, egy szerződés és egy napló. Ugyanaz az egy művelet — egy döntési, adat-, szerződéses és felelősségi ellátási lánc, amely három ponton törik el a leggyakrabban: a modellváltásnál, amelyről nem jön értesítés; az API-jogosultságnál, amely nagyobb az üzleti felhatalmazásnál; és a naplónál, amelyben van output, de nincs nyoma a kontrollnak. Ne az AI-dobozt nézzük. Röntgenezzük meg a döntést.

CyberArk 2025 — gépi identitások > www.businesswire.com/news/home/20250423817886/en

Öt kérdés. Ujjszámolással.

Egy: milyen AI-rendszereket használnak ténylegesen? Kettő: milyen adathoz férnek hozzá? Három: mit tehetnek emberi jóváhagyás nélkül? Négy: kik állnak mögöttük harmadik félként? Öt: egy incidens után huszonnégy órán belül rekonstruálni tudják, mi történt? Ha mind az ötre nincs válasz, akkor még nincs AI governance. Csak AI van. Az öt kérdés a Pilot to Control térkép második pontja — a board első ülésére való.

„A kolléga írta be a promptot” — nem védekezés.

Ha az AI-val végzett munkából kár keletkezik, kifelé a cég felel a teljes kárért. A munkavállalótól gondatlan károkozás esetén legfeljebb négyhavi távolléti díj követelhető (Mt. 179. § (3) bekezdés [ellenőrizendő: §-hivatkozás]); az alkalmazott károkozásáért harmadik személy felé a munkáltató felel (Ptk. 6:540. § [ellenőrizendő]). Vagyis a munkavállalói AI-használat szabálya nem HR-formalitás: az egyetlen eszköz, amivel a cég a saját kitettségét csökkenti — és bizonyítja, hogy észszerű intézkedést tett.

2012. évi I. törvény (Mt.); 2013. évi V. törvény (Ptk.) — njt.hu > njt.hu

Hol fut a modell?

Egy mérnöknek öt perc, a szerződésnek egy fejezet. A modellszolgáltató felületén és a felhőlistán a régió választása joghatóságot jelent: hol dolgozzák fel az adatot, ki fér hozzá támogatás címén, és harmadik ország-e adatvédelmi szempontból. Az adatrezidencia nem technikai preferencia, hanem az adatvédelmi és az üzleti titok-kötelezettségek végrehajtása — és a kilépés feltétele: ami nem exportálható, az nem hordozható.

Privacy 3.0 — amikor az adatkezelő ügynök.

A célhoz kötöttség és az adattakarékosság elve ember által tervezett adatkezelésre készült. Egy ügynök, amely a cél eléréséhez maga választ eszközt és adatot, ezeket az elveket futásidőben feszíti: a cél adott, az út nem. Az adatfeldolgozói lánc (GDPR 28. cikk) ügynökök esetén nem statikus lista, hanem a hívott eszközök és szolgáltatók futásidejű halmaza. Ezért a jogalap, a hozzáférési határ és a napló nem utólagos dokumentáció, hanem a rendszer része kell legyen — privacy by design a szó eredeti értelmében.

GDPR 5., 25. és 28. cikk > eur-lex.europa.eu/eli/reg/2016/679/oj

Következő lépés

Egy use case. Kilencven perc. Három prioritás.

Ha a második ábra hiányzik, ha a számla mögötti nyolc tétel nincs a szerződésben, vagy ha a kapcsolótábláról hiányzik az éles művelet sora — az első beszélgetés nem audit és nem keretrendszer. Egyetlen élő AI-műveletet nézünk végig a mandátum, a nyom és a fék mentén, és a végén három dolog marad, amit a következő negyedévben zárni kell.

Board Readiness — vezetőknek — a két ábra, az öt kérdés és a felelősségi térkép egy ülésre

Chain-of-Control Sprint — bevezetőknek és beszerzőknek — egy művelet röntgenképe, a szerződéses nyolc tétel és az éles művelet sora

Product Readiness Review — fejlesztőknek — release gate, változáskezelés, felelősség és a vevő kérdőíve

Írásban: drkj.hu/contact · Két útravaló: Code to Market · Pilot to Control (külön letölthető)

KÁVÉ AZ ELŐADÁS UTÁN

Jöjjön be egy kávéra.

Az irodánk a Gerbeaud-házban van, a Vörösmarty téren — az előadás után is, és a következő hetekben is. Hozzon egy élő AI-műveletet: egy chatbotot, egy CV-szűrőt, egy ügynököt. Harminc perc, és a végén három prioritás marad.

Taylor Wessing Hungary · Gerbeaud-ház · Vörösmarty tér, Budapest · Időpont: drkj.hu/aisummit

Az időpontfoglaláshoz megadott adatokat kizárólag az egyeztetésre használom. Adatkezelő: dr. Kopasz János · drkj.hu/privacy

Az anyag tájékoztató jellegű, nem jogi tanácsadás. A hivatkozások és határidők a 2026. szeptember 7-i állapotot tükrözik; a [ellenőrizendő] jelű tételek a közzététel előtt rögzítendőek.