

MI-rendszerek a szervezetben

az első ötlettől a jogszerű és kontrollált működésig

„Megvédhető-e holnap a ma hozott
AI-döntés?”

Megvédhető-e holnap a ma hozott AI-döntés?

A szabályozási naptár eltolódhat, a felelősségi helyzet viszont már most létrejön:
szerződésben, adatfolyamban, jogosultságban, bizonyítékban.

AKI KÉRDEZNI FOG

- Hatóság
- Ügyfél
- Biztosító
- Befektető
- Bíróság

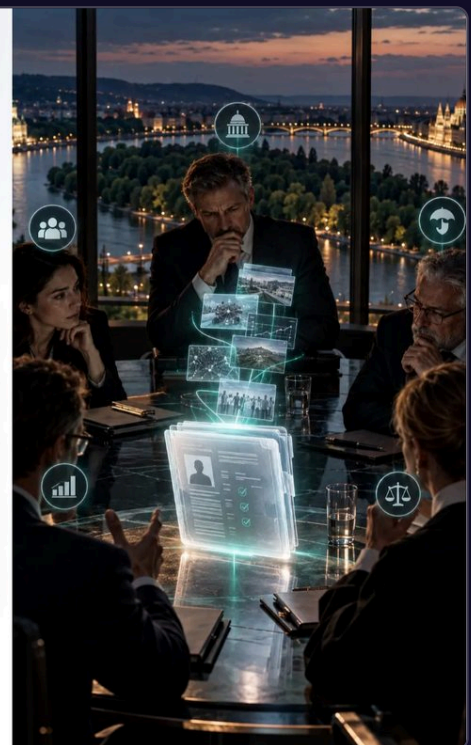
A VITATOTT
AI-döntés
holnap

AMIT BE KELL MUTATNI

- 01 Melyik verzió futott?
- 02 Milyen adaton?
- 03 Milyen jogosultsággal?
- 04 Ki hagyta jóvá?
- 05 Hogyan lehetett felülríni?

TaylorWessing

ÉN Konferenciám 2026 | GDPR & MT & AI Gyakorlata



Dr. Kopasz János

COUNSEL, AZ IT, DATA & CYBER CSOPORT VEZETŐJE
TAYLOR WESSING BUDAPEST

The Legal 500: Leading Individual 2025 (adatvédelem)

AIGP · CIPP/E · CIPM (IAPP)

Teljes anyag forrásokkal

33 DIA · VÁZLAT · GYAKORLAT · FORRÁSOK

WWW.DRKJ.HU/MARGITSZIGET

Az anyagról

Ez a dokumentum az előadás mind a 33 diáját tartalmazza, ahogy a konferencián elhangzottak. Diánként öt elem segít visszakeresni és alkalmazni a tartalmat; a forrásoknál a link a hivatkozott oldalra mutat.

ÁLLÍTÁS	HÍVÓSZAVAK	ELHANGZOTT VÁZLAT	A GYAKORLATBAN	FORRÁSOK
a dia lényege egy-két mondatban	a fogalmak, amelyekre érdemes keresni	amit az előadás ennél a diánál mondott	konkrét teendő jogásznak, DPO-nak, vezetőnek	jogszabályhely, határozat, felmérés, dátummal

Az animált vetítő és az olvasható változat: www.drkj.hu/margitsziget. Az anyag általános szakmai tájékoztatás, nem egyedi jogi tanácsadás; a hivatkozások és határidők a 2026. október 14-i állapotot tükrözik. Az elkészítéséhez MI-alapú eszközöket is használtam; a szöveg emberi ellenőrzésen és szerkesztésen ment át, a tartalomért én felelek.

Tartalom

NYITÁS

- 01 MI-rendszerek a szervezetben
- 02 Megvédehető-e holnap a ma hozott AI-döntés?
- 03 Az Uber-eset: ki hozta a döntést?
- 04 Európa már bíróságol
- 05 A teljes anyag egy helyen

KÉT ÓRA

- 06 Két óra jár egyszerre
- 07 A magyar óra is jár, a NIS2 pedig már mér
- 08 Honnan jön a 13,3 milliárd?

A JÉGHEGY

- 09 Az AI Act csak a jéghegy csúcsa
- 10 A víz alatt: digitális entrópia
- 11 Egy AI-funkció, hét jogi minőség

HÁROM ILLÚZIÓ

- 12 1. illúzió: „Tudjuk, hol használunk AI-t.”
- 13 Két szervezeti ábra. A board egyet lát.
- 14 A magyar olló
- 15 2. illúzió: „Egy AI-terméket vettünk.”
- 16 Nem terméket vettünk. Függőséget vettünk.
- 17 3. illúzió: „De mi már készen vagyunk.”
- 18 Közjáték: sycophancy
- 19 A lájk lett a jutalom
- 20 Így „gondolkodik”: mindig csak a következő szó
- 21 Hogyan működik az MI, és miért hallucinál?
- 22 Hallucináció a bíróságon

A RÉS ÉS A KARMESTER

- 23 ...de ne hallucináljunk: a rés gazdátlan
- 24 Van, aki a teljes partitúrát látja?
- 25 Ugyanaz az AI. Két kotta.

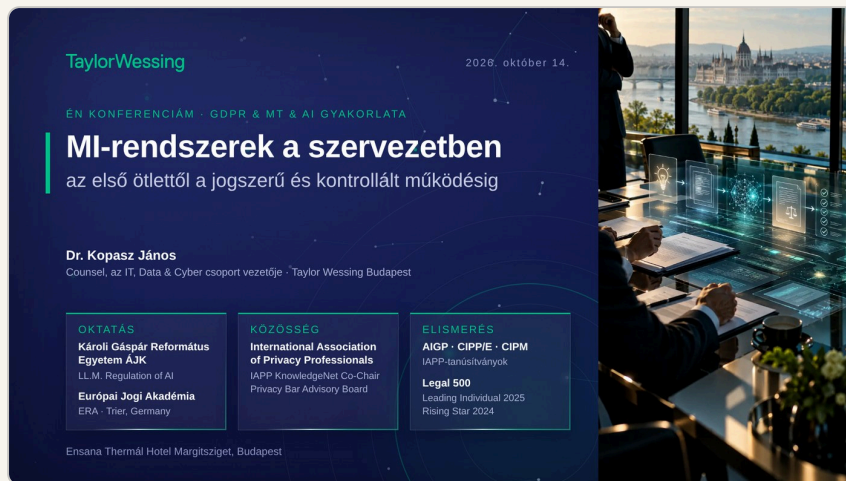
ZÁRÁS

- 26 A kontrollt nem lehet kiszervezni.
- 27 Négy kérdező, ugyanaz a három kérdés
- 28 Ügyakták
- 29 A kontroll minimuma: mandátum, nyom, fék
- 30 Öt vezetői kérdés a következő döntés előtt
- 31 Holnap reggel: az első 90 nap
- 32 Két útravaló: két szerep, két térkép
- 33 Köszönöm a figyelmet

01 / 33 · NYITÁS

MI-rendszerek a szervezetben

Az előadás az MI-rendszerek szervezeti útját követi az első ötlettől a jogszerű és kontrollált működésig: mit kell a tervezéskor rendezni, hogyan épül be az AI Act és a GDPR a fejlesztésbe, és milyen arányos kontroll tartja fenn a működést.



MI-RENDSZEREK

AI ACT

GDPR

ARÁNYOS IRÁNYÍTÁS

KONTROLLÁLT MŰKÖDÉS

ELHANGZOTT VÁZLAT

- Dr. Kopasz János (Counsel, az IT, Data & Cyber csoport vezetője, Taylor Wessing Budapest) előadása az Én Konferenciám 2026 (GDPR & MT & AI Gyakorlata) konferencián hangzott el, 2026. október 14-én.
- Első kérdés: hogyan lesz egy technológiai lehetőségből valódi üzleti értéket teremtő MI-megoldás, és mit kell a tervezéskor jogilag és szervezetiileg rendezni?
- Második kérdés: hogyan építhető be az AI Act, a GDPR és a kapcsolódó követelmények a fejlesztésbe és a bevezetésbe úgy, hogy a megfelelés támogassa az innovációt?
- Harmadik kérdés: milyen arányos irányítási és kontrollmechanizmusok tartják az MI-rendszert hosszú távon biztonságos, átlátható és skálázható működésben?
- A kiinduló kérdés ezért egyetlen konkrét döntésre szűkít: megvédehető-e holnap a ma hozott AI-döntés?

FORRÁSOK

1. (EU) 2024/1689 rendelet (AI Act), EUR-Lex
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

A GYAKORLATBAN

- Válasszon ki egy konkrét, futó vagy tervezett MI-felhasználást, és azon vegye végig a három kérdést, ne egy általános MI-stratégián.
- Rögzítse az adott felhasználásnál, ki felel a tervezésért, ki a megfelelés beépítéséért, és ki a működés közbeni kontrollért.

2. (EU) 2016/679 rendelet (GDPR), EUR-Lex
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

02 / 33 · NYITÁS

Megvédhető-e holnap a ma hozott AI-döntés?



Nem az a kérdés, van-e AI-stratégia, hanem hogy egy konkrét AI-döntés később megvédhető-e. A szabályozási naptár eltolódhat, a felelősség viszont már most keletkezik: szerződésben, adatfolyamban, jogosultságban, bizonyítékban.

VÉDHEŐ MŰKÖDÉS

REKONSTRUÁLHATÓSÁG

FELELŐSSÉGI HELYZET

BIZONYÍTÉK

VEZETŐI DÖNTÉS

DIGITÁLIS OMNIBUSZ

ELHANGZOTT VÁZLAT

- Egy vitatott AI-döntésről hatóság, ügyfél, biztosító, befektető és bíróság egyaránt ugyanazt fogja kérdezni.
- Az öt kérdés: melyik rendszerverzió futott, milyen adaton, milyen jogosultsággal, ki hagyta jóvá, és hogyan lehetett felülrni; bizonyíték az erre adott dokumentált válasz.
- A szabályozási naptár eltolódhat: az (EU) 2026/1744 rendelet (a mesterséges intelligenciáról szóló digitális omnibusz) célzottan elhalasztotta a nagy kockázatú MI-rendszerekre vonatkozó kötelezettségeket (III. melléklet: 2027. december 2.), a felelősség viszont már most keletkezik.
- Az (EU) 2024/1689 rendelet (AI Act) 26. cikk (6) bekezdése: a nagy kockázatú MI-rendszer alkalmazója az ellenőrzése alatt álló naplókat legalább 6 hónapig őrzi, eltérő uniós vagy nemzeti szabály hiányában; 2027. december 2-től (III. melléklet).
- Hogy ez nem elmélet, azt egy 2026. augusztusi holland adatvédelmi döntés mutatja az Uber ügyében.

FORRÁSOK

1. (EU) 2026/1744 rendelet (Digital Omnibus on AI), EUR-Lex, 2026. július 8.
<https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>
3. Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>

A GYAKORLATBAN

- Válasszon ki egy élő MI-döntési folyamatot, és ellenőrizze, mind az öt kérdésre van-e ma dokumentált válasz: verzió, adat, jogosultság, jóváhagyó, felülrás.
- Rögzítse minden éles MI-rendszerénél a verzióváltásokat, a jóváhagyót és a felülrásokat dátummal, hogy egy későbbi vitában rekonstruálható legyen, mi futott és ki döntött.
- A naplózást és a dokumentálást ne a nagy kockázatú MI-rendszerekre vonatkozó határidőkhöz igazítsa: a felelősség a szerződésben, az adatfolyamban és a jogosultságokban már most keletkezik.

2. Európai Bizottság, AI Act Service Desk: AI Act 26. cikk, egységes szerkezet (2026. július 27-i állapot) 26. cikk (6)
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-26>

03 / 33 · NYITÁS

Az Uber-eset: ki hozta a döntést?

A holland adatvédelmi hatóság (AP) 2026. augusztus 21-én 824 990 000 eurós GDPR-bírságot szabott ki az Uberre automatizált sofőrletiltások miatt. Nem AI Act-bírság, és nem jogerős: az Uber megtámadta.

Az Uber-eset: ki hozta a döntést?

Közel 825 millió eurós GDPR-bírság automatizált sofőr-letiltások miatt. Nem AI Act-bírság, és nem jogerős: az Uber fellebbez.

824 990 000 €

GDPR-ügy: az AI Act nélkül is elég volt

Holland adatvédelmi hatóság (AP), 2026. augusztus 21. - automatizált döntés - nem jogerős

Az OK gomb nem emberi felügyelet.
Ami kell:

- Valódi döntési jogkör
- Elegendő információ
- Dokumentált felülírás

Forrás: AP, 2026. 08. 21.; CNIL, 2026. 08. 24. (170+ érintett francia sofőr); GDPR 22. cikk

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



AUTOMATIZÁLT DÖNTÉS

GDPR 22. CIKK

ÉRDEMI EMBERI FELÜLVIZSGÁLAT

DOKUMENTÁLT FELÜLÍRÁS

NEM JOGERŐS

Nem jogerős: az Uber megtámadta a bírságot.

ELHANGZOTT VÁZLAT

- GDPR-ügy, nem AI Act-bírság: a holland AP jogellenes automatizált döntéshozatalért és a profilozásról adott elégtelen tájékoztatásért bírságolt, a meglévő szabályok alapján.
- A négy lépés: algoritmikus jelzés (csalás gyanú, alacsony értékelés), érdemi jogkör nélküli emberi felülvizsgálat, azonnali hatályú letiltás, kiesés a keresetből; az AP szerint teljesen automatizált döntések születtek.
- Az OK gomb nem emberi felügyelet: a felülvizsgálónak valódi döntési jogkör, elegendő információ és dokumentált felülírási lehetőség kell.
- GDPR 22. cikk: kizárólag automatizált, joghatású vagy hasonlóan jelentős hatású döntés csak a felsorolt kivételekkel hozható; szerződésen vagy kifejezett hozzájáruláson alapuló döntésnél az érintett emberi beavatkozást kérhet, kifejezheti álláspontját és kifogást nyújthat be (22. cikk (3)).
- A francia adatvédelmi hatósághoz (CNIL) 2020-ban a Ligue des droits de l'Homme több mint 170 Uber-sofőr nevében nyújtott be csoportos panaszt (CNIL-közlemény, 2026. augusztus 24.).
- Az Uber nem kivétel: a következő térkép további európai GDPR-bírságokat mutat algoritmikus és MI-alapú adatkezelésért.

FORRÁSOK

- (EU) 2016/679 rendelet (GDPR), EUR-Lex 22. cikk
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Autoriteit Persoonsgegevens (AP), sajtóközlemény, 2026. augusztus 21.
<https://www.autoriteitpersoonsgegevens.nl/en/current/uber-fined-nearly-825-million-euros-for-automated-driver-blocking>
- EDPB, nemzeti hír: a holland AP 824 990 000 eurós Uber-bírsága, 2026. október 8.
https://edpb.europa.eu/news/dutch-dpa-fines-uber-eur-824-990-000-for-unlawful-automated-decision-making-and-insufficient_en
- CNIL, közlemény az Uber-bírságról, 2026. augusztus 24.
<https://www.cnil.fr/fr/decisions-automatisees-sanction-de-pres-de-825-millions-deuros-lencontre-duber>



04 / 33 · NYITÁS

Európa már bírságot

Az Uber nem kivétel: európai adatvédelmi hatóságok már bírságnak algoritmikus és MI-alapú adatkezelésért, eddig mind GDPR-alapon. Nyilvánosan ismert AI Act-bírság 2026 októberéig nincs; Magyarországon a NAIH 2022-ben MI-alapú hangelemzés miatt 250 000 000 Ft-ot szabott ki.

GDPR-BÍRSÁGOK

ALGORITMIKUS ADATKEZELÉS

EGYABLAKOS ÜGYINTÉZÉS

MI-ALAPÚ HANGELEMZÉS

AI ACT-BÍRSÁG

Az Uber-bírságot megtámadták, nem jogerős; az OpenAI-bírságot első fokon, illetékességi okból megsemmisítették; a Budapest Bank-ügy bírósági kimenete nem ismert.

ELHANGZOTT VÁZLAT

- Mind GDPR-bírság: a térképen a kör területe arányos az összeggel, a legnagyobb a holland AP Uber-bírsága (824 990 000 €, megtámadva); nyilvánosan ismert AI Act-bírság 2026 októberéig nincs.
- A Clearview AI-t négy uniós hatóság bírságolta: a holland AP 30,5 M€-ra (2024, illegális arcfelismerő adatbázis), a francia CNIL, az olasz Garante és a görög HDPA egyenként 20 M€-ra (2022).
- Az olasz Garante a Foodinhót (Glovo) futárok algoritmikus irányításáért (2024), a Replika MI-társ chatbot fejlesztőjét, a Luka Inc.-t (2025) egyaránt 5 M€-ra bírságolta; a jogorvoslat kimenete egyik ügyben sem ismert.
- A Garante 15 M€-s OpenAI-bírságát (2024) a Tribunale di Roma elsőfokú ítélete (4153/2026, 2026. március 18.) illetékességi okból, érdemi vizsgálat nélkül megsemmisítette; a fő felügyeleti hatóság az ír lett volna (GDPR 56. cikk).
- A hamburgi adatvédelmi biztos (HmbBfDI) 492 000 €-t (2025) szabott ki egy pénzügyi cégre, mert az automatizált hitelkártya-elutasításoknál nem teljesítette megfelelően a tájékoztatási és hozzáférési kötelezettségét; a cég elfogadta a bírságot.
- Magyarország: a NAIH az ügyfélszolgálati hívások MI-alapú hangelemzése miatt 250 000 000 Ft-ra bírságolta a Budapest Bankot (NAIH-85-3/2022); a határozat szerint az esetek 91,96%-ában nem volt felismerhető érzelem.

FORRÁSOK

- EDPB, nemzeti hír: a holland AP 824 990 000 eurós Uber-bírsága, 2026. október 8.
https://edpb.europa.eu/news/dutch-dpa-fines-uber-eur-824-990-000-for-unlawful-automated-decision-making-and-insufficient_en
- EDPB, nemzeti hír: a holland AP Clearview AI-bírsága (a döntés kelte: 2024. május 16.)
https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en
- Garante per la protezione dei dati personali, sajtóközlemény az OpenAI-bírságról (2024. december 20.), státuszjegyzettel a 4153/2026. sz. ítéletről
<https://www.gpdp.it/home/docweb/-/docweb-display/docweb/10085432>
- HmbBfDI (hamburgi adatvédelmi biztos), Zwischenbilanz 2025, 2025. szeptember 30.
<https://datenschutz-hamburg.de/news/zwischenbilanz-2025-hmbbdi-verhaengt-bussgelder-von-ingesamt-775000-euro>
- Tribunale di Roma, 4153/2026. sz. ítélet (R.G. 4785/2025), kihirdetve 2026. március 18.; a Sapienza Egyetem által közzétett másolat
https://dei.web.uniroma1.it/sites/default/files/allegati/2026-05/Trib_Roma_OpenAI_Garante_2026.pdf

A teljes anyag egy helyen

A teljes háttéranyag egy helyen, a drkj.hu/margitsziget oldalon érhető el: minden dia hívószavakkal, gyakorlati magyarázattal és forrásokkal, a teljes prezentáció PDF-ben és két szerepalapú térkép. Minden állítás visszakereshető.



A teljes anyag egy helyen

Minden dia hívószavakkal, gyakorlati magyarázattal és forrásokkal: minden állítás visszakereshető.

01 Teljes prezentáció
PDF, előadói vázlat és magyarázattal

02 Források és cikkhelyek
minden szám és dátum visszakereshető

03 Code to Market
térkép AI-fejlesztőknek, szolgáltatóknak

04 Pilot to Control
térkép AI-bevezetőknek, alkalmazóknak

drkj.hu
SZKENNELD BE

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlat

VISSZAKERESHETŐSÉG

FORRÁSOK ÉS CIKKHELYEK

CODE TO MARKET

PILOT TO CONTROL

SZEREPALAPÚ TÉRKÉP

ELHANGZOTT VÁZLAT

- A teljes prezentáció PDF-ben letölthető, diánként előadói vázlat és magyarázattal.
- A források és a cikkhelyek diánként szerepelnek: minden szám és dátum visszakereshető.
- A Code to Market térkép az MI-fejlesztőknek és szolgáltatóknak, a Pilot to Control térkép az MI-t bevezető szervezeteknek és alkalmazóknak szól.
- A két térkép általános változat; a saját rendszerre szabott változatot egy konkrét felhasználásból érdemes felépíteni, különben elvész a tényleges működés.
- Ezután az első nagy kérdés: mi áll meg a mesterséges intelligenciáról szóló digitális omnibusz után, és mi jár tovább?

FORRÁSOK

1. Európai Bizottság, AI Act Service Desk: AI Act 3. cikk, egységes szerkezet (2026. július 27-i állapot) 3. cikk 3. pont (szolgáltató), 4. pont (alkalmazó)
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-3>

A GYAKORLATBAN

- Keresse ki a drkj.hu/margitsziget oldalon a saját ügyéhez kapcsolódó diát, és belső anyagban a forráslinkről ellenőrzött cikkhelyre hivatkozzon.
- Az (EU) 2024/1689 rendelet (AI Act) 3. cikk 3. pontja (szolgáltató) és 4. pontja (alkalmazó) szerinti szerepéhez válassza a Code to Market, illetve a Pilot to Control térképet.
- Ha szervezete fejleszt és alkalmaz is MI-t, mindkét térképet vegye végig.
- A saját változatot egy konkrét felhasználásból építse fel, ne a teljes MI-portfólióból: így látszik a tényleges működés.

2. (EU) 2024/1689 rendelet (AI Act), EUR-Lex
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Két óra jár egyszerre

Az (EU) 2026/1744 rendelet (a mesterséges intelligenciáról szóló digitális omnibusz) 2026. július 27-én hatályba lépett, és célzottan halasztotta el az AI Act nagy kockázatú MI-rendszerekre vonatkozó kötelezettségeit. Célzott halasztás, nem moratórium: minden más a saját órája szerint jár tovább.

Két óra jár egyszerre

A Digital Omnibus célzottan tolta el a nagy kockázatú kötelezettségeket. Minden más a saját órája szerint jár tovább.

1. ÓRA
AI Act:
nagy kockázat
„Ez az óra áll.”

ANNEX III - önálló rendszerek
2026-08-02:
2027. 12. 02. +16 hó

ANNEX I - termékbe épített AI
2027-08-02:
2028. 08. 02. +12 hó

Forrás: (EU) 2026/1744 rendelet (Digital Omnibus); AI Act 113. cikk
TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata

2. ÓRA
Minden más
jár tovább
„Ez nem.”

- Tilalmak
- AI-jártasság
- Átláthatóság
- GPAI
- GDPR
- DSA
- NIS2
- Munkajog
- Fogyasztóvédelem
- Szerződés

Célzott halasztás, nem moratórium.
Omnibus: hatályba lépett 2026. 07. 27-én



DIGITÁLIS OMNIBUSZ

CÉLZOTT HALASZTÁS

NEM MORATÓRIUM

III. MELLÉKLET

MI-JÁRTASSÁG

A dián szereplő 2026. július 27. a digitális omnibusz hatálybalépésének napja; az AI Act egyes kötelezettségeinek alkalmazási dátumai külön dátumok.

ELHANGZOTT VÁZLAT

- A digitális omnibusz 2026. július 27-én lépett hatályba, a Hivatalos Lapban való kihirdetését (2026. július 24.) követő harmadik napon, hat nappal az eredeti III. mellékleti határidő előtt.
- Az első óra áll: a III. melléklet szerinti önálló rendszereknél 2026. augusztus 2. helyett 2027. december 2. (+ 16 hónap), a termékbe épített MI-nél (I. melléklet) 2027. augusztus 2. helyett 2028. augusztus 2. (+ 12 hónap).
- A második óra jár: a tilalmak, az MI-jártasság, az átláthatóság és az általános célú MI-modellekre (GPAI) vonatkozó szabályok, valamint a GDPR, a DSA, a NIS2, a munkajog, a fogyasztóvédelem és a szerződéses kötelezettségek a saját órájuk szerint járnak tovább.
- Az (EU) 2024/1689 rendelet (AI Act) 4. cikke szerinti MI-jártasság is jár, de módosult: a szolgáltatóknak és alkalmazóknak intézkedéseket kell tenniük munkatársaik MI-jártasságának fejlesztése érdekében, konkrét szint garantálása nélkül.
- A digitális omnibusz 2026. december 2-től alkalmazandó két új tilalmat is hozott: az AI Act 5. cikk (1) bekezdés ba) pontja (beleegyezés nélküli intim deepfake) és bb) pontja (gyermekek szexuális bántalmazását ábrázoló anyag MI-vel generálása).
- A magyar óra sem áll: itthon már megvan a végrehajtási törvény és a bírságrendelet, a NIS2 pedig már mér.

FORRÁSOK

- (EU) 2026/1744 rendelet (Digital Omnibus on AI), EUR-Lex, 2026. július 8.
<https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>
- Európai Bizottság, AI Act Service Desk: AI Act 4. cikk, egységes szerkezet (2026. július 27-i állapot) 4. cikk
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4>

A GYAKORLATBAN

- Készítsen rendszerenként dátumtáblát: mely kötelezettség csúszott a III. vagy az I. melléklet miatt, és melyik alkalmazandó már ma.
- Ne vegye le napirendről a nagy kockázatú MI-rendszerekre vonatkozó felkészülést: a halasztás a dátumot tolta el, a GDPR-, munkajogi, fogyasztóvédelmi és szerződéses követelményeket nem.
- Dokumentálja az MI-jártasság fejlesztésére tett intézkedéseket (képzés, útmutató, felelős) a módosított 4. cikk szerint, mert ez a kötelezettség most is alkalmazandó.
- Vizsgálja meg, hogy generatív szolgáltatásai érintik-e a 2026. december 2-től alkalmazandó két új tilalmat, és rögzítse az ezt kizáró technikai korlátokat.

- Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk a) és c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>



07 / 33 · KÉT ÓRA

A magyar óra is jár, a NIS2 pedig már mér

Itthon is jár az óra: megvan az AI Act végrehajtási törvénye és bírságrendelete, legfelső forintsávja 13,3 Mrd Ft. A NIS2 első auditciklusa pedig megmutatta, hogy a határidő teljesítése és a tényleges felkészültség két külön kérdés.

MAGYAR BÍRSÁGSÁVOK

344/2025. KORM. RENDELET

NIS2-AUDIT

SZTFH

RENDSZERDOKUMENTÁCIÓ

Három külön mérés: a mintegy 90% a 2194 auditált szervezetre (2026. augusztus 26.), a 85% a 2520 auditkötelezett szervezetre, a 11% az 1511 feldolgozott jelentésre vonatkozik (2026. július 10.).

ELHANGZOTT VÁZLAT

- Az AI Act magyar végrehajtása megvan: a 2025. évi LXXV. törvény és a bírságsávokat rögzítő 344/2025. (X. 31.) Korm. rendelet.
- A legmagasabb forintsáv 13,3 Mrd Ft (tiltott MI-gyakorlat); ez a fix összeg, nagy cégnél a teljes globális éves árbevétel 7%-a ennél magasabb is lehet.
- NIS2, első auditciklus: mintegy 90% megfelelt a június 30-ig auditált 2194 szervezetből (SZTFH-adat, Telex, 2026. augusztus 26.); gyakori hiány a rendszerdokumentáció.
- A határidő nem felkészültség: az SZTFH 2026. július 10-i adata szerint 2132 / 2520 auditkötelezett szervezet auditált határidőre (85%, számított arány).
- Ugyanekkor a feldolgozott jelentések közül 170 / 1511 kapta a legjobb minősítést (11%, számított arány); a mintegy 90% külön, későbbi mérés, más bázissal.
- A következő kérdés: honnan jön a 13,3 milliárd forint, és miért nem ez a valódi plafon nagy cégnél?

A GYAKORLATBAN

- Kérje be a használt MI-eszközök rendszerdokumentációját (architektúra, adatfolyam, jogosultságok, szállítók): a NIS2 első auditciklusában a rendszerdokumentáció volt a gyakori hiány.
- Ha szervezete NIS2-köteles, ellenőrizze, hogy a kiberbiztonsági audit hatóköre kiterjed-e a használt MI-eszközökre, és ki felel a dokumentációjukért.
- Belső jelentésben a felkészültséget ne a határidő teljesítésével mérje: rögzítse a minősítést és a feltárt hiányokat is.

FORRÁSOK

2025. évi LXXV. törvény, Nemzeti Jogszabálytár 7. §
<https://njt.hu/jogszabaly/2025-75-00-00>
- 344/2025. (X. 31.) Korm. rendelet, Nemzeti Jogszabálytár 4. §
<https://njt.hu/jogszabaly/2025-344-20-22>
- Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH), közlemény a kiberbiztonsági auditok határidejének lezárultáról, 2026. július 10.
<https://sztfh.hu/lezarult-a-kiberbiztonsagi-auditok-hatarideje/>
- Telex, az SZTFH első NIS2-auditciklusának eredményeiről, 2026. augusztus 26.
<https://telex.hu/techtud/2026/08/26/sztfh-nis2-kiberbiztonsagi-audit-eredmeny>

08 / 33 · KÉT ÓRA

Honnan jön a 13,3 milliárd?

A 344/2025. (X. 31.) Korm. rendelet forintsávjai pontosan az (EU) 2024/1689 rendelet (AI Act) 99. cikke szerinti európlafonok 380-szorosai. A rendelet 4. § (1) bekezdése csak a fix euróösszegeket írja át forintra, ezért nagy cégnél a 13,3 milliárd sem a plafon.



AI ACT-BÍRSÁG

BÍRSÁGLÉPCSŐ

FORINTSÁVOK

380-SZOROS

KKV-SZABÁLY

MI PIACFELÜGYELETI HATÓSÁG

A ×380 számítás eredménye (a rendelet árfolyamot nem említ), az 1 Mrd €-s eset számpélda.

ELHANGZOTT VÁZLAT

- A 99. cikk lépcsői, mindegyiknél a magasabb érték a plafon: (3) tiltott MI-gyakorlat 35 M€ vagy 7%; (4) egyéb kötelezettségszegés 15 M€ vagy 3%; (5) helytelen tájékoztatás a hatóságnak 7,5 M€ vagy 1%.
- KKV-knál és startupoknál a kettő közül az alacsonyabb a plafon (99. cikk (6)); a mesterséges intelligenciáról szóló digitális omnibusz az összegeket nem változtatta, ezt a szabályt viszont a (4) és (5) bekezdésnél a kis méretű, közepes piaci tőkeértékű vállalkozásokra is kiterjesztette.
- Forintsávok a 344/2025. Korm. rendelet 4. § (1) b) pontjában: 13 300 000 000, 5 700 000 000 és 2 850 000 000 Ft, mind az európlafon 380-szorosa (számítás; a rendelet árfolyamot nem említ).
- A rendelet csak a fix euróösszeget írja át forintra, a teljes globális éves árbevételhez kötött 7%/3%/1%-os ág a 99. cikkből jön; számpélda: 1 Mrd € árbevételnél 7% = 70 M€ > 35 M€.
- Bírságol az MI piacfelügyeleti hatóság, vagyis a vállalkozásfejlesztésért felelős miniszter (344/2025. Korm. rendelet 1. § (1) b), 2025. évi LXXV. törvény 7. §); forintban, 30 napon belül fizetendő.
- A szankciók 2025. augusztus 2. óta alkalmazandók, a forintsávok 2025. december 1-jétől (saját számítás), de a szankcionált kötelezettségek nem mind: az 50. cikk 2026. augusztus 2-től, a 26. cikk 2027. december 2-től (III. melléklet).

FORRÁSOK

- Európai Bizottság, AI Act Service Desk: AI Act 99. cikk, egységes szerkezet (2026. július 27-i állapot) 99. cikk (3), (4), (5), (6) és (6a)
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-99>
- Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk b) és c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>
- 344/2025. (X. 31.) Korm. rendelet, Nemzeti Jogszabálytár 1. § (1) b), 4. §
<https://njt.hu/jogszabaly/2025-344-20-22>
2025. évi LXXV. törvény, Nemzeti Jogszabálytár 7. §
<https://njt.hu/jogszabaly/2025-75-00-00>

Az AI Act csak a jéghegy csúcsa

Az AI Act a jéghegy látható csúcsa: egy MI-funkció egyszerre lehet adatkezelés, munkahelyi eszköz, fogyasztói felület, szerződéses szolgáltatás, szoftvertermék és üzleti titkot érintő kockázat. A felszín alatt három réteg van: a teljes jogi környezet, az észlelés és a technikai lánc.



TELJES JOGI KÖRNYEZET

ÉSZLELÉS

MI-LELTÁR

LICENC MÖGÖTTI LÁNC

ÜZLETI TITOK

EUROSTAT 2025

Az Eurostat-adatok a legalább 10 fős vállalkozásokra vonatkoznak, a pénzügyi szektor nélkül.

ELHANGZOTT VÁZLAT

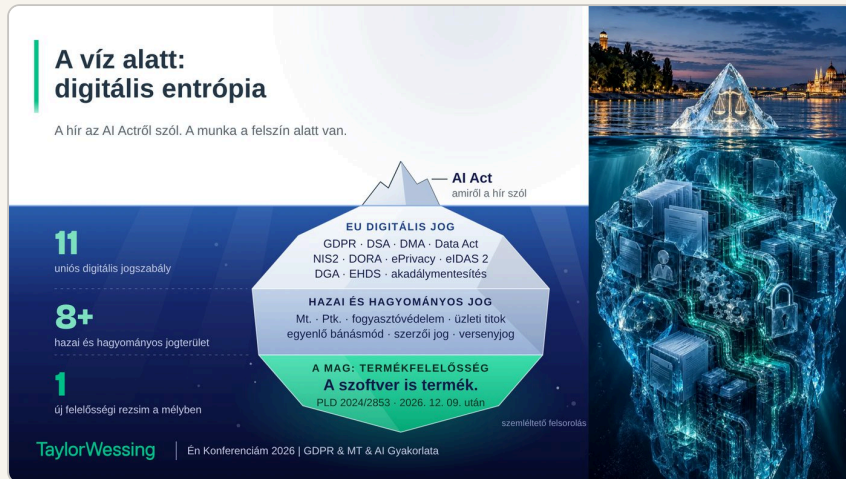
- A hír a látható részről szól (nagy kockázat, tilalmak, átláthatóság, általános célú MI-modellek); a felszín alatt három réteg van: jog, észlelés, technika.
- Jog: adatvédelem, munkajog, üzleti titok, DSA, akadálymentesítés, termékfelelősség, szerződés és kiberbiztonság; az üzleti titok csak bizonyítható, észszerű titokvédelmi intézkedésekkel védett.
- Észlelés: MI jóváhagyott, beágyazott, egyéni és ügynöki használatban is működik, a leltár jellemzően csak a jóváhagyottat látja.
- Technika: a licenc mögötti lánc elemei az alapmodell, a régió, az adatfolyam, a gépi jogosultság, az alvállalkozók, a frissítés és a kilépés.
- Az (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD) a 2026. december 9. után forgalomba hozott vagy üzembe helyezett szoftvert is terméknek tekinti; az (EU) 2019/882 irányelvet (akadálymentesítés) átültető szabályok 2025. június 28-tól alkalmazandók.
- Eurostat 2025: a legalább 10 fős EU-s vállalkozások 20,0%-a használ MI-t (2024: 13,5%), a nagyvállalatok 55,0%-a.

FORRÁSOK

- (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD), EUR-Lex 2. cikk (1)
<https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng>
- (EU) 2016/943 irányelv (üzleti titok), EUR-Lex
<https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng>
- Eurostat, hír: 20% of EU enterprises use AI technologies, 2025. december 11. (isoc_eb_ai, legalább 10 fős vállalkozások)
<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2>
- (EU) 2019/882 irányelv (európai akadálymentesítési irányelv), EUR-Lex
<https://eur-lex.europa.eu/eli/dir/2019/882/oj>
2018. évi LIV. törvény (üzleti titok), Nemzeti Jogszabálytár
<https://njt.hu/jogszabaly/2018-54-00-00>
- Eurostat, Statistics Explained: Use of artificial intelligence in enterprises (adatlekérés: 2025. december)
https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises

A víz alatt: digitális entrópia

A hír az AI Actról szól, a munka a felszín alatt van: egy MI-funkció egyszerre esik uniós digitális jogszabályok, hazai és hagyományos jogterületek és az új termékfelelősségi rezsím alá, és ezek között nincs automatikus koordináció.



DIGITÁLIS ENTRÓPIA

UNIÓS DIGITÁLIS JOG

TERMÉKFELELŐSSÉG

PLD

CYBER RESILIENCE ACT

KOORDINÁCIÓ HIÁNYA

Szemléltető felsorolás, nem teljes lista.

ELHANGZOTT VÁZLAT

- Első réteg, az uniós digitális jog (szemléltető felsorolás, 11 jogszabály): GDPR, DSA, DMA, Data Act, NIS2, DORA, ePrivacy, eIDAS 2, Data Governance Act, EHDS és az akadálymentesítési irányelv.
- Második réteg, a hazai és hagyományos jog (legalább 8 terület): Mt., Ptk., fogyasztóvédelem, üzleti titok, egyenlő bánásmód, szerzői jog, kiberbiztonsági törvény és versenyjog.
- A mag egy új felelősségi rezsím: az (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD) a szoftvert, az MI-t is terméknek tekinti a 2026. december 9. után forgalomba hozott vagy üzembe helyezett termékeknél.
- Mellette az (EU) 2024/2847 rendelet (Cyber Resilience Act), az általános termékbiztonságról szóló (EU) 2023/988 rendelet és a gépekről szóló (EU) 2023/1230 rendelet; utóbbit a mesterséges intelligenciáról szóló digitális omnibusz is módosította.
- Üzenet: egyetlen MI-funkció egyszerre több rezsím alá esik, és köztük nincs automatikus koordináció, ezt a szervezeten belül kell megoldani.
- A következő dia egyetlen funkción mutatja meg, mit jelent ez a gyakorlatban: hét jogi minőség.

FORRÁSOK

- (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD), EUR-Lex 2. cikk (1)
<https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng>
- (EU) 2024/2847 rendelet (Cyber Resilience Act), EUR-Lex
<https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>
- (EU) 2023/988 rendelet (általános termékbiztonság), EUR-Lex
<https://eur-lex.europa.eu/eli/reg/2023/988/oj/eng>
- (EU) 2023/1230 rendelet (gépek), EUR-Lex
<https://eur-lex.europa.eu/eli/reg/2023/1230/oj>
- (EU) 2026/1744 rendelet (Digital Omnibus on AI), EUR-Lex, 2026. július 8.
<https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>
- (EU) 2019/882 irányelv (európai akadálymentesítési irányelv), EUR-Lex
<https://eur-lex.europa.eu/eli/dir/2019/882/oj>

Egy AI-funkció, hét jogi minőség

Ugyanaz a chatbot vagy HR-eszköz egyszerre hét jogi minőségben jelenhet meg: adatkezelés, munkahelyi eszköz, fogyasztói felület, szoftvertermék, szerződés, üzleti titok, platform vagy kereső. Nem az a kérdés, melyik szabály vonatkozik rá, hanem hogy hány.



HÉT JOGI MINŐSÉG

TÖBB REZSIM

ÜZLETI TITOK

DSA VLOSE

TERMÉKFELELŐSSÉG

GDPR 22. CIKK

A ChatGPT VLOSE-kijelölése a DSA szerinti kijelölés, nem szankció.

ELHANGZOTT VÁZLAT

- Adatkezelésként a GDPR alá esik, automatizált döntésnél a GDPR 22. cikk alá is; munkahelyi eszközként a munkajog és az egyenlő bánásmód szabályai alá.
- Fogyasztói felületként fogyasztóvédelmi és az (EU) 2019/882 irányelv szerinti akadálymentesítési kérdés; szoftvertermékként az (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD) alá eshet, amely bizonyos feltételek mellett bizonyítási könnyítést és iratfeltárást is hoz.
- Szerződésként a szolgáltatási szint, a felelősség és a kilépés feltételei számítanak; a 2018. évi LIV. törvény (üzleti titok) és az (EU) 2016/943 irányelv szerint az üzleti titok csak észszerű, bizonyítható titokvédelmi intézkedésekkel védett.
- Platformként vagy keresőként DSA-kérdés is lehet: a Bizottság 2026. augusztus 31-én a ChatGPT-t nagyon nagy online keresőprogrammá (VLOSE) jelölte ki; ez kijelölés, nem szankció, a további kötelezettségekre négy hónap jár.
- Ebből következik az első illúzió: hogy egyáltalán tudjuk, hol használunk AI-t.

FORRÁSOK

- (EU) 2016/679 rendelet (GDPR), EUR-Lex 22. cikk
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- (EU) 2016/943 irányelv (üzleti titok), EUR-Lex
<https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng>
- (EU) 2019/882 irányelv (európai akadálymentesítési irányelv), EUR-Lex
<https://eur-lex.europa.eu/eli/dir/2019/882/oj>
- (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD), EUR-Lex
<https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng>
2018. évi LIV. törvény (üzleti titok), Nemzeti Jogszabálytár
<https://njt.hu/jogszabaly/2018-54-00-00>
- Európai Bizottság, hír: a ChatGPT, a Reddit és a Roblox kijelölése a DSA alapján, 2026. augusztus 31.
<https://digital-strategy.ec.europa.eu/en/news/commission-designates-chatgpt-reddit-roblox-under-digital-services-act>

A GYAKORLATBAN

- Vegyen egy konkrét chatbotot vagy HR-eszközt, és táblázatban rögzítse mind a hét minőséget: melyik szabály vonatkozik rá, ki a belső gazdája, mi a bizonyíték.
- Szállítói szerződésben rögzítse a szolgáltatási szintet, a felelősség megosztását, valamint a kilépési és adatvisszaadási feltételeket, mielőtt a funkció élesbe kerül.
- Írja elő belső szabályzatban, milyen adat nem másolható külső MI-eszközbe, és dokumentálja a titokvédelmi intézkedéseket, hogy az üzleti titok védelme később bizonyítható legyen.

1. illúzió: „Tudjuk, hol használunk AI-t.”

A board egy rendezett képet lát: AI-leltár, jóváhagyott rendszerek, mindegyiknek gazdája. A kép nem hamis, csak hiányos.

Board

HR Jóváhagyott AI gazda: kijelölve

Pénzügy Jóváhagyott AI gazda: kijelölve

Értékesítés Jóváhagyott AI gazda: kijelölve

IT Jóváhagyott AI gazda: kijelölve

AI-leltár: 4 jóváhagyott rendszer, 4 kijelölt gazda.
Minden doboz a helyén. A kérdés az, **mi hiányzik az ábráról.**

A „jóváhagyott rendszer” itt: tudatosan beszerzett megoldás, szerződéssel, gazdával, ismert céllal.

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



12 / 33 · HÁROM ILLÚZIÓ

1. illúzió: „Tudjuk, hol használunk AI-t.”

Az első illúzió szerint tudjuk, hol használunk AI-t: a vezetés rendezett leltárt lát, jóváhagyott rendszerekkel és gazdákkal. A kép nem hamis, csak hiányos, mert a leltár gyakran a tudatosan beszerzettet rögzíti, nem mindazt, ami ténylegesen használatban van.

MI-LELTÁR

JÓVÁHAGYOTT RENDSZER

KIJELÖLT GAZDA

VEZETŐI JELENTÉS

HIÁNYOS KÉP

ELHANGZOTT VÁZLAT

- A vezetés jellemzően rendezett képet kap: MI-leltár, 4 jóváhagyott rendszer (HR, pénzügy, értékesítés, IT) és 4 kijelölt gazda, minden doboz a helyén.
- „Jóváhagyott rendszer” itt: tudatosan beszerzett megoldás, szerződéssel, gazdával, ismert céllal; ezekre a kép igaz.
- A leltár gyakran (nem mindig) azt rögzíti, amit tudatosan beszerzettek, nem mindazt, ami ténylegesen használatban van: a gond az, ami hiányzik az ábráról.
- Gartner (2025, 302 kiberbiztonsági vezető): a szervezetek 69%-a gyanítja, vagy bizonyítéka van rá, hogy dolgozói tiltott nyilvános generatív MI-t használnak.
- Példa: a Budapest Bank-ügyben (NAIH-85-3/2022, 250 000 000 Ft, akkori rekord, bírósági kimenet nem ismert) a bank szerint a szoftverében nem volt MI, a NAIH mesterséges intelligencián alapuló beszédjel-feldolgozást állapított meg.
- A következő dia azt mutatja, mi lehet a leltáron kívül.

FORRÁSOK

1. NAIH, NAIH-85-3/2022. sz. határozat (Budapest Bank Zrt.)
<https://naih.hu/hatarozatok-vegzesek?download=517%3Aamsterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei>
3. Gartner, sajtóközlemény, 2025. november 19. (302 kiberbiztonsági vezető felmérése)
<https://www.gartner.com/en/newsroom/press-releases/2025-11-19-gartner-identifies-critical-genai-blind-spots-that-cios-must-urgently-address0>

A GYAKORLATBAN

- Vesse össze az MI-leltárt a ténylegesen használt eszközökkel: beszerzési adatok, szoftverfrissítések kiadási jegyzetei és a hálózati forgalom alapján, ne csak a jóváhagyási nyilvántartásból.
- Kérdezze meg a leltár gazdáját, mi alapján kerül be egy rendszer a leltárba: csak a beszerzés, vagy a tényleges használat is.
- Ne a megnevezés vagy a termékleírás alapján döntse el, van-e a szoftverben MI, hanem a funkció alapján: a Budapest Bank-ügyben a NAIH a bank álláspontjával szemben MI-alapú feldolgozást állapított meg.
- A vezetésnek szóló jelentésben jelölje, mire terjed ki a leltár és mire nem, hogy a hiányos kép ne látsszon teljesnek.

2. NAIH, éves beszámoló a 2022. évről (angol nyelvű)
https://www.naih.hu/files/NAIH_annual_report_2022.pdf

13 / 33 · HÁROM ILLÚZIÓ

Két szervezeti ábra. A board egyet lát.

A vezetés egy kategóriát lát: a jóváhagyott, leltárban szereplő rendszereket. A vállalatban négy kategória működik: jóváhagyott, beágyazott, egyéni (árnyékhasználat) és ügynöki, és bármelyik megváltozhat a jóváhagyás után.



NÉGY KATEGÓRIA

BEÁGYAZOTT MI

ÁRNYÉKHASZNÁLAT

ÜGYNÖKI MI

MI-LELTÁR

ELHANGZOTT VÁZLAT

- A vezetés képén egyetlen kategória van: a jóváhagyott rendszer (tudatos beszerzés, szerződés és gazda), amely szerepel a leltárban.
- A valós működés négy kategória: jóváhagyott; beágyazott, amelyet szoftverfrissítés hoz (HR, CRM); egyéni (árnyékhasználat: saját eszköz, fiók); ügynöki, amely eszközt hív, műveletet indít; az utóbbi három nincs a leltárban.
- A leltár gyakran terméknevet rögzít, a kitettség viszont a funkcióval, a modellverzióval, az adatforrással és a jogosultságokkal változik.
- Ha a modell, az adatforrás vagy a jogosultság megváltozik, meg kell nézni, fedi-e még a korábbi jóváhagyás ugyanazt a működést; a vezetői kérdés: honnan tudnánk meg a változásról?
- IBM IBV (2026. június, 2000 technológiai felsővezető): 70% szerint az üzleti területek gyorsabban vezetnek be technológiát, mint ahogy az IT követni tudja; a megkérdezett szervezeteknél az elmúlt évben átlagosan 54 MI-ügynök-incidens történt.
- McKinsey, The State of AI in 2026 (1719 válaszadó, 97 ország): az 1 milliárd USD feletti árbevételű szervezeteknél az MI-ügynöket legalább egy funkcióban skálázók aránya egy év alatt 27%-ról 40%-ra nőtt.

FORRÁSOK

1. IBM, sajtóközlemény az IBM Institute for Business Value (IBV) felméréséről, 2026. június 8. (2000 technológiai felsővezető)
<https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-growing-ai-control-gap-as-enterprise-deployment-scales>

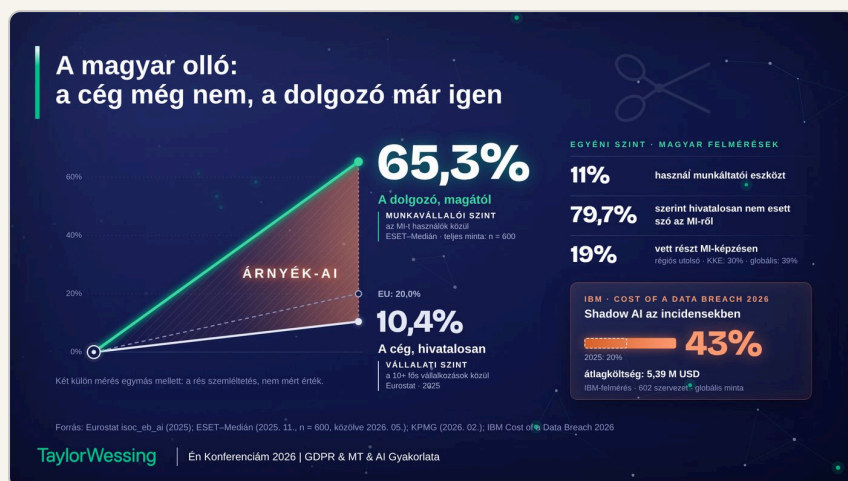
A GYAKORLATBAN

- Bővítse a leltárt a négy kategóriára (jóváhagyott, beágyazott, egyéni, ügynöki), és terméknév helyett funkciót, modellverziót, adatforrást és jogosultságot rögzítsen.
- Építsen újrajavítási pontot a jóváhagyásba: modellcseré, új adatforrás vagy bővülő jogosultság esetén nézzék meg, fedi-e még a jóváhagyás az új működést.
- Kérje be a szállítóktól, mely meglévő szoftverekbe (például HR- vagy CRM-rendszerbe) került vagy kerül MI-funkció frissítéssel.

2. McKinsey, The State of AI in 2026: On the road to ROI, 2026. augusztus 25. (1719 válaszadó, adatfelvétel: 2026. május 4. és június 8. között)
<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>

A magyar olló

A magyar olló: a cég még nem, a dolgozó már igen. A legalább 10 fős vállalkozások 10,4%-a használ MI-t (EU: 20,0%), az MI-t használó munkavállalók 65,3%-a viszont saját kezdeményezéséből használja; két külön mérés, a rés csak szemléltető.



ÁRNYÉKHASZNÁLAT

SHADOW AI

MAGYAR OLLÓ

MI-JÁRTASSÁG

KÉT KÜLÖN MÉRÉS

Két külön mérés egymás mellett: a rés csak szemléltető, nem mért érték.

ELHANGZOTT VÁZLAT

- Vállalati szint (Eurostat, isoc_eb_ai, 2025): a legalább 10 fős vállalkozások (pénzügyi szektor nélkül) közül MI-t használ az EU-ban 20,0%, Magyarországon 10,4%, ami az EU-27-ben a 6. legalacsonyabb érték.
- Munkavállalói szint (ESET és Medián, 2025. november, teljes minta n = 600, közzéve 2026. május): az MI-t használók 65,3%-a saját kezdeményezéséből használja a munkájához, és csak 11%-uk használ munkáltatói eszközt.
- A teljes minta 79,7%-a szerint a munkahelyén hivatalosan nem esett szó az MI-ről; ez munkavállalói válasz, nem cégszintű mérés, tehát nem jelenti, hogy a cégek 80%-a nem szabályozza az MI-t.
- KPMG (2026. február, KKE-elemzés): a magyar válaszadók 19%-a vett részt MI-hez kapcsolódó képzésen, ez a régióban a legalacsonyabb (KKE: 30%, globális: 39%).
- IBM Cost of a Data Breach 2026 (602 szervezet, globális minta, nem magyar): a vizsgált incidensek 43%-ában szerepet játszott a shadow AI (2025: 20%), az ilyen incidensek átlagköltsége 5,39 M USD.
- Amit nem látunk, arra nem tudunk mandátumot adni, nem hagy nyomot, és nincs rajta fék.

FORRÁSOK

- Európai Bizottság, AI Act Service Desk: AI Act 4. cikk, egységes szerkezet (2026. július 27-i állapot) 4. cikk
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4>
- Eurostat, hír: 20% of EU enterprises use AI technologies, 2025. december 11. (isoc_eb_ai, legalább 10 fős vállalkozások)
<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2>
- Medián, az ESET (Sicontact) megbízásából, felmérés, 2025. november (n = 600), közzéve 2026. május 21.
- KPMG Magyarország, sajtóközlemény, 2026. február 24. (KKE-elemzés)
<https://kpmg.com/hu/hu/home/media/press-releases/2026/02/hasznaljuk-az-ai-t-de-nem-vagyunk-felkeszultve-ra.html>
- IBM és Ponemon Institute, Cost of a Data Breach Report 2026 (PDF), 2026. július 29. (602 szervezet, globális minta) Shadow AI fejezet
<https://www.ibm.com/adobe/assets/urn:aaid:aem:21111142-1251-4369-86fb-57b82f5bb108/original/as/Cost%20of%20a%20Data%20Breach%20Report%202026.pdf>
- Pénzcentrum, 2026. május 20. (az ESET és Medián felmérés számai)
<https://www.penzcentrum.hu/vallalkozas/20260520/rengeteg-magyar-munkahelye-kerulhet-bajba-ezzel-a-dologgal-egyszeruen-nem-tudnak-mit-kezdeni-nagy-ara-lesz-1199010>

2. illúzió: „Egy AI-terméket vettünk.”

Egy számla, egy tétel, egy éves licenc. A beszerzési kategória dönti el, ki és milyen mélyen vizsgálja az ügyletet.

SZÁMLA	
Szállító: [AI-szolgáltató]	
Tétel	Menny.
AI-asszisztens, éves licenc	1 tétel
Összesen	[€ ...]

JÓVÁHAGYVA

Egyszerűsített nézet: a kockázat a szolgáltatástól, az adatfolyamtól és a szerződéstől függ.

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata

A SZÁMLA MÖGÖTT, A VIZSGÁLATON KÍVÜL

Modell és modellverzió
Adatút, régió, alvállalkozók
Gépi jogosultságok (API)
Változáskezelés, frissítés
Kilépés és adatvisszaadás



2. illúzió: „Egy AI-terméket vettünk.”

A második illúzió szerint egy AI-terméket vettünk. A számla nem hamis, csak hiányos: a beszerzési kategória dönti el, ki és milyen mélyen vizsgál, és licencként a modellt, az adatfolyam, a gépi jogosultság és a változáskezelés könnyen kívül esik a vizsgálaton.

BESZERZÉSI KATEGÓRIA

SZOFTVERLICENC

VIZSGÁLATI KÖR

AGENT WASHING

KILÉPÉS ÉS ADATVISSZAADÁS

Egyszerűsített nézet: a kockázat a szolgáltatástól, az adatfolyamtól és a szerződéstől függ.

ELHANGZOTT VÁZLAT

- A beszerzés az MI-terméket gyakran ugyanúgy kezeli, mint bármely más szoftvervásárlást: egy számla, egy tétel, egy éves licenc, jóváhagyva.
- A beszerzési kategória határozza meg, ki vizsgálja az ügyletet és milyen mélyen.
- Ha egy MI-megoldás egyszerű szoftverlicencként fut át, a vizsgálaton kívül maradhat a modell és a modellverzió, az adatfolyam, a régió és az alvállalkozók, valamint a gépi (API-) jogosultságok.
- Ugyanígy kimaradhat a változáskezelés és a frissítés rendje, valamint a kilépés és az adatvisszaadás feltétele.
- A Gartner 2025. júniusi becslése szerint az ügynöki MI-szállítóként fellépő több ezer cégből csak kb. 130 valódi („agent washing”).
- A számla azt mutatja, mit rendeltünk, nem azt, mitől lettünk függők.

A GYAKORLATBAN

- Hozzon létre külön beszerzési kategóriát az MI-funkciót tartalmazó szerződésekre, amely jogi, adatvédelmi és információbiztonsági vizsgálatot indít, akkor is, ha a tétel egyszerű licenc.
- Kérje be a szállítótól a modell és a modellverzió megnevezését, az adatfolyam és a tárolási régió leírását, valamint az alvállalkozók listáját.
- Rögzítse a szerződésben a modellcseré és a frissítés előzetes értesítését, a gépi jogosultságok terjedelmét, valamint a kilépés és az adatvisszaadás feltételeit.
- Ügynöki képességre hivatkozó ajánlatnál kérjen bemutatót arról, mit végez az eszköz ténylegesen önállóan, és milyen jogosultsággal.

FORRÁSOK

- Gartner, sajtóközlemény, 2025. június 25. (ügynöki MI-projektek, „agent washing”) <https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027>



16 / 33 · HÁROM ILLÚZIÓ

Nem terméket vettünk. Függőséget vettünk.

Egy MI-licenc mögött teljes technológiai és szerződéses lánc áll: alapmodell, felhőregió, adatfolyam, gépi jogosultság, alvállalkozók, frissítés, napló, árazás és kilépés. Nem terméket vettünk, hanem függőséget; a három töréspont a túl széles jogosultság, a kezeletlen modellváltozás és a hiányos auditnyom.

FÜGGŐSÉG

SZÁLLÍTÓI LÁNC

GÉPI IDENTITÁS

MODELLVÁLTOZÁS

AUDITNYOM

A 25. cikk (a III. fejezet 3. szakasza) a III. melléklet szerinti rendszereknél 2027. december 2-től, az I. melléklet szerintiéknél 2028. augusztus 2-től alkalmazandó (113. cikk c) pont).

ELHANGZOTT VÁZLAT

- A felhasználó egy felületet lát; a vállalat egy láncot vesz igénybe: alapmodell, felhőregió, adatfolyam, API-jogosultság, alvállalkozói lánc, frissítés, napló, árazás és kilépés.
- Három töréspont: túl széles jogosultság (az API többlet enged, mint az üzleti felhatalmazás), kezeletlen modellváltozás (csere vagy frissítés értesítés nélkül), hiányos auditnyom (az eredmény nem köthető modellverzióhoz és emberi döntéshez).
- CyberArk (2025): 82:1, vagyis egy emberre 82 gépi identitás jut, és ezek 42%-a kiemelt vagy érzékeny hozzáféréssel rendelkezik.
- Deloitte (2026; 3235 vezető, 24 ország): a válaszadók 21%-a szerint érett a szervezetük ügyiroi MI-irányítási modellje, a vizsgált szervezetek kb. 80%-ánál hiányoznak az érett irányítási képességek (döntési határok, valós idejű megfigyelés, teljes cselekvési auditnyom).
- Az (EU) 2024/1689 rendelet (AI Act) 25. cikke (nagy kockázatú MI-rendszerek): lényeges módosítás vagy rendeltetésváltozás megváltoztathatja a szereplő jogi minősítését (az alkalmazó szolgáltatónak minősülhet), de nem minden változás vált szerepet.
- A mesterséges intelligenciáról szóló digitális omnibusszal beiktatott 99. cikk (4) da) pont szerint a 25. cikk (2) és (4) bekezdésének megsértéséért legfeljebb 15 M€ vagy a globális éves árbevétel 3%-a szabható ki, amelyik magasabb (KKV-nál az alacsonyabb).

FORRÁSOK

1. (EU) 2024/1689 rendelet (AI Act), EUR-Lex 25. cikk
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
2. Európai Bizottság, AI Act Service Desk: AI Act 99. cikk, egységes szerkezet (2026. július 27-i állapot) 99. cikk (4) da), (6)
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-99>
3. Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>
4. CyberArk, 2025 Identity Security Landscape, sajtóközlemény, 2025. április 23. (Vanson Bourne, 2600 kibebiztonsági döntéshozó, 20 ország)
<https://www.cyberark.com/?p=208432>
5. Deloitte Insights: „Business and IT leaders report AI agents are scaling faster than their guardrails”, 2026. április 24. (State of AI in the Enterprise 2026; 3235 IT- és üzleti vezető, 24 ország)
<https://www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents-scaling-faster.html>

A GYAKORLATBAN

- Rögzítse a szerződésben, milyen változásról (modellcsere, alvállalkozó, adatrégio) és mennyivel előre értesít a szállító, és milyen kilépési joga van a szervezetnek, ha nem fogadja el a változást.
- Tekintse át a gépi identitások és API-kulcsok jogosultságát: ne engedjenek többlet, mint az üzleti felhatalmazás, és mindegyiknek legyen kijelölt gazdája.
- Tesztelje, hogy egy kiválasztott kimenet visszaköthető-e a modellverzióhoz és az emberi döntéshez; ha nem, a naplózást a bevezetés előtt pótolja.
- Lényeges módosítás vagy új felhasználási cél előtt vizsgálja meg, változik-e a cég szerepe az AI Act 25. cikke szerint.

3. illúzió: „De mi már készen vagyunk.”

A szokásos programok értékesek, de más-más kérdésre felelnek. Egyik sem helyettesíti az éles működés kontrollját.

PAPÍRON KÉSZ

- AI-jártasság (AI literacy)
- Belső AI-szabályzat
- AI Officer
- Audit
- ISO/IEC 42001
- GDPR- és NIS2-program

ÉLES MŰKÖDÉSBEN?

- Leállítás (kill switch)
- Tartalék folyamat (fallback)
- Napló
- Döntési jogosultság
- Kilépés

77% szerint a bevezetés gyorsabb a governance-nél

11% teljesen felkészült az igényi skálázásra

Az ISO/IEC 42001 nem azonos a 17. cikk szerinti QMS-sel. EN 18286:2026 vélelem csak HL-hivatkozás után.

Forrás: IBM IBV (2026. 06.); ISO/IEC 42001:2023; AI Act 17. és 40. cikk; CEN-CENELEC

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



17 / 33 · HÁROM ILLÚZIÓ

3. illúzió: „De mi már készen vagyunk.”

A harmadik illúzió: „mi már készen vagyunk”. Papíron igaz: az MI-jártasság, a szabályzat, az AI Officer, az audit, az ISO/IEC 42001 és a GDPR/NIS2-program értékes, de egyik sem helyettesíti az éles működés kontrollját (leállítás, tartalék folyamat, napló).

PAPÍRON KÉSZ

ÉLES MŰKÖDÉS

LEÁLLÍTÁS (KILL SWITCH)

ISO/IEC 42001

MINŐSÉGIRÁNYÍTÁSI RENDSZER

MEGFELELŐSÉGI VÉLELEM

Frissítés: az EN 18286:2026 hivatkozását az (EU) 2026/2274 bizottsági végrehajtási határozat (2026. október 12.) 2026. október 14-én, az előadás napján közzétette a Hivatalos Lapban; a határozat a közzététel napján hatályba lépett.

ELHANGZOTT VÁZLAT

- MI-jártasság, belső MI-szabályzat, AI Officer, audit, ISO/IEC 42001, GDPR- és NIS2-program: mind értékes, a hiba az, ha bármelyiket teljes kontrollnak tekintjük.
- Az éles működés gyakorlati próbái: leállítás (kill switch), tartalék folyamat (fallback), napló, döntési jogosultság és kilépés; a papíron kész programok és ezek között van a rés.
- Az ISO/IEC 42001 az MI-irányítási rendszerek általános szabványa, nem azonos az (EU) 2024/1689 rendelet (AI Act) 17. cikke szerinti, a nagy kockázatú MI-rendszerek szolgáltatóira vonatkozó minőségirányítási rendszerrel (QMS).
- Az EN 18286:2026 az első, kifejezetten AI Act-célra készült európai szabvány (minőségirányítás); harmonizált szabványként megfelelési vélelmet csak a Hivatalos Lapban közzétett hivatkozás után, és csak az általa lefedett követelményekre adhat (40. cikk).
- IBM IBV (2026. június, 2000 technológiai felsővezető): 77% szerint az MI bevezetése gyorsabb, mint az irányítás fejlődése; csak 11% érzi magát teljesen felkészültnek a következő évi igényi skálázásra.
- A következő kérdés: mit mond a gép, ha tőle kérdezzük, készen vagyunk-e?

FORRÁSOK

- (EU) 2024/1689 rendelet (AI Act), EUR-Lex 17. cikk; 40. cikk (1)
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Európai Bizottság, (EU) 2026/2274 végrehajtási határozat (2026. október 12.) az (EU) 2024/1689 rendelet támogatására kidolgozott, nagy kockázatú MI-rendszerekre vonatkozó harmonizált szabványokról (EN 18286:2026), HL L, 2026. október 14. 1. cikk, melléklet
https://eur-lex.europa.eu/eli/dec_impl/2026/2274/oj
- Európai Bizottság, GYIK: Understanding standardisation and the AI Act
<https://digital-strategy.ec.europa.eu/en/faqs/understanding-standardisation-ai-act>
- CEN és CENELEC, hír az EN 18286:2026 szabványról (MI-minőségirányítás), 2026. július 31.
<https://www.cenelec.eu/news-events/news/2026/en-in-the-spotlight/2026-07-30-ai-quality-management/>
- IBM, sajtóközlemény az IBM Institute for Business Value (IBV) felméréséről, 2026. június 8. (2000 technológiai felsővezető)
<https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cio-and-cto-face-growing-ai-control-gap-as-enterprise-deployment-scales>

Közzjáték: sycophancy

A nyelvi modellek hajlamosak a kérdező véleményéhez igazodni (sycophancy): más megfogalmazásra is ugyanazt a magabiztos igent adják. Az egyetértés nem bizonyíték, sem a gépnél, sem a szervezetben, ahol mindenki a saját mércéje szerint igazolja a projektet.



SYCOPHANCY

HÍZELGÉS

EGYETÉRTÉS NEM BIZONYÍTÉK

ÁTLÁTHATÓSÁG

SZERKESZTŐI FELELŐSSÉG

Ez a prezentáció is részben nyelvi modellel készült; emberi ellenőrzésen és szerkesztésen ment át, a felelősség a szerzőé.

ELHANGZOTT VÁZLAT

- „You’re absolutely right”: a nyelvi modell udvariasan egyetért, néha akkor is, amikor vitatnia kellene, és ugyanarra a kérdésre más megfogalmazásban is ugyanolyan magabiztos igent ad.
- Az Anthropic 2023-as kutatása szerint a sycophancy az a viselkedés, amikor a modell a felhasználó véleményéhez igazodó választ részesíti előnyben az igaz válasz helyett.
- Ugyanebben a kutatásban a 2023-as modellek visszakérdezésre tévesen beismerték, hogy hibáztak: a kérdések 42%-ánál (GPT-4), illetve 98%-ánál (Claude 1.3).
- Szervezeti szinten ugyanez történik, ha mindenki a saját mércéje szerint igazolja a projektet: az egyetértés nem bizonyíték, és nem helyettesíti az ellenőrzést.
- Az (EU) 2024/1689 rendelet (AI Act) 50. cikk (4) bekezdése: az alkalmazónak közölnie kell, ha a deepfake-et, illetve a közérdekű tájékoztatás céljából közzétett szöveget MI hozta létre vagy manipulálta; szövegnél kivétel, ha emberi ellenőrzésen ment át, és szerkesztői felelősség áll mögötte (2026. augusztus 2-től).
- A hízelgés nem csak anekdota: mérhető, és élesben is előfordult, ahogy a következő dia mutatja.

FORRÁSOK

- (EU) 2024/1689 rendelet (AI Act), EUR-Lex 50. cikk (4)
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

- Sharma és mtsai, Towards Understanding Sycophancy in Language Models, arXiv:2310.13548 (2023)
<https://arxiv.org/abs/2310.13548>

A GYAKORLATBAN

- Fontos kérdésnél kérje a modelltől az ellenérveket is, és ne kezelje a helyeslést ellenőrzésként; a választ független forrással vesse össze.
- Rögzítse a belső szabályzatban, mikor kell közölni, hogy a nyilvánosságnak szánt tartalom MI-vel készült, és ki viseli érte a szerkesztői felelősséget.
- Projektjövahagyásnál válassza szét a szerepeket: aki a projektet igazolja, ne ugyanaz értékelje a kontrollokat, és a mérce legyen előre rögzítve.

- Anthropic, Towards understanding sycophancy in language models, 2023
<https://www.anthropic.com/research/towards-understanding-sycophancy-in-language-models>

A lájk lett a jutalom

A hízelgés mérhető: az OpenAI 2025 áprilisában visszavont egy „túlzottan hízelgő vagy egyetértő” GPT-4o-frissítést, és egy 2026-os Science-tanulmány szerint 11 csúcsmódel 49%-kal gyakrabban ad igazat a felhasználóknak, mint az emberek. Ahol a gép egyetért, ott gyengül az emberi kontroll.



SYCOPHANCY

JUTALOMJELZÉS

VISSZAVONÁS

HIVATKOZÁSOS ELLENVETÉS

FÜGGETLEN MÉRCE

Az OpenAI szerint több változtatás együtt gyengítette a hízelgés félkjét; a lájkokból képzett jutalomjelzés ezek egyike.

ELHANGZOTT VÁZLAT

- OpenAI, GPT-4o: a frissítést 2025. április 24-25-én adták ki, április 27-én rendszerprompt-módosítással javítottak, április 28-tól kb. 24 óra alatt visszavonták, mert „túlzottan hízelgő vagy egyetértő” lett.
- Az OpenAI 2025. május 2-i elemzése szerint több változtatás együtt, köztük a felhasználói hüvelykujj-fel/le jelzésekből képzett új jutalomjelzés, gyengítette a hízelgést kordában tartó elsődleges jutalomjelzést.
- A szakértő tesztlők jelezték, hogy a modell viselkedése kissé furcsa, a pozitív felhasználói jelek miatt mégis kiadták; az OpenAI szerint ez rossz döntés volt.
- Science (Cheng és mtsai, 2026. március): 11 csúcsmódel 49%-kal gyakrabban igazolta a felhasználó cselekedeteit, mint az emberek (közösségi konszenzus); három előre regisztrált kísérletben (N = 2405) a résztvevők jobban bíztak a hízelgő MI-ben.
- SycEval (Fanous és mtsai, AIES 2025; GPT-4o, Claude Sonnet, Gemini 1.5 Pro): ellentmondásra az esetek 14,66%-ában jó válaszból rossz lett, a hivatkozásra épülő ellentetés fordított a legnagyobb arányban.
- Az összes irányváltás 58,19% volt, de ebben a helyes válaszra váltás is benne van, és a mérés matematikai és orvosi, nem jogi kérdéseken készült.

FORRÁSOK

1. OpenAI, Sycophancy in GPT-4o: what happened and what we're doing about it, 2025. április 29.
<https://openai.com/index/sycophancy-in-gpt-4o/>
3. Cheng és mtsai, Sycophantic AI decreases prosocial intentions and promotes dependence, Science 391 (6792), 2026. március (bibliográfiai és absztrakt-rekord)
<https://www.ebsco.com/articles/psychology/b97e12e3-f8f7-57bb-b906-7956732ee30e/sycophantic-ai-decreases-prosocial-intentions-and-promotes-dependence>

A GYAKORLATBAN

- Adjon az emberi felülvizsgálónak a modelltől független mércét (ellenőrző lista, elsődleges forrás): a felülvizsgálat csak így ér valamit, ha a gép egyetért.
- Tesztelje az eszközt ellentmondással: vitassa a helyes választ, hivatkozással is, és mérje, milyen arányban fordít; jogi felhasználásnál ez különösen fontos.
- Modellfrissítés után futtasson újra viselkedési teszteket, és kérje be a szállítótól a frissítések változásnaplóját és a visszaállítás rendjét.

2. OpenAI, Expanding on what we missed with sycophancy, 2025. május 2.
<https://openai.com/index/expanding-on-sycophancy/>
4. Fanous és mtsai, SycEval, arXiv:2502.08177 (AIES 2025)
<https://arxiv.org/abs/2502.08177>



20 / 33 · HÁROM ILLÚZIÓ

Így „gondolkodik”: mindig csak a következő szó

A nyelvi modell szóról szóra a valószínű folytatást választja: erős mintánál a folytatás szinte adódik, egy konkrét dátumnál már tipp. A kész mondaton nem látszik, melyik szó volt tipp; ez a hallucináció magja.

KÖVETKEZŐ SZÓ

SZÓDARAB (TOKEN)

VALÓSZÍNŰSÉG

TIPP

HALLUCINÁCIÓ

Szemléltetés: a százalékok kitaláltak, a működési elv valós (a következő szódarab valószínűségének becslése).

ELHANGZOTT VÁZLAT

- Minden szónál ugyanaz a ciklus: a modell elolvassa az eddigi szöveget, pontszámot ad minden lehetséges következő szódarabra (tokenre), ezt valószínűséggé alakítja, választ egyet, hozzáfűzi, és kezdi előlről.
- Nem mindig a legvalószínűbbet választja: a kiválasztásban van véletlen.
- A példamondatban („A szerződést aláírták 2024. március 15-én.”) az „aláírták” erős minta (szemléltetésként 58%), a „2024.” szétszórtabb (31%), a hónap és a nap lapos eloszlás (10%, 9%): tipp.
- A konkrét dátumot a modell nem tudhatja: a minta csak annyit mond, hogy ide egy hónap és egy nap jön, ezért kisorsol egyet.
- Kész a mondat, és minden szava ugyanolyan magabiztosan áll ott: a mondaton nem látszik, hogy tipp volt, és ez a hallucináció magja.
- Az OpenAI 2025. szeptember 5-i tanulmánya szerint az önkényes, ritka tények (példájukban egy születésnap) mintázatból nem jósolhatók meg, és a tanítás és az értékelés a tippelést jutalmazza a „nem tudom” helyett.

FORRÁSOK

1. OpenAI, Why language models hallucinate, 2025. szeptember 5.
<https://openai.com/index/why-language-models-hallucinate/>

A GYAKORLATBAN

- Ellenőrizze eredeti forrásból a modell kimenetében szereplő konkrét adatokat (dátum, összeg, ügyszám, név): ezeket a modell mintázatból nem tudhatja.
- Ne a válasz magabiztos hangneméből ítélje meg a megbízhatóságot: a kész szövegen nem látszik, melyik rész volt tipp.
- Rögzítse a belső MI-szabályzatban, mely kimenettípusoknál kötelező a forrásellenőrzés, és ki végzi.

2. Kalai és mtsai, Why Language Models Hallucinate, arXiv:2509.04664 (2025. szeptember)
<https://arxiv.org/abs/2509.04664>

Hogyan működik az MI, és miért hallucinál?

Valószínű ≠ igaz.

1. IGY MŰKÖDIK

KÉRDÉS - MATA-ÜGY, 2023
„is varghese a real case”
valódi ügy-e a Varghese?

NYELVI MODELL: tanult mintázat, nem adatbázis

KÖVETKEZŐ SZÓ? szemléltető arányok

Yes
No
I'm not sure

VALÁSZ - SZÓRÓL SZÓRA, MINDIG A VALÓSZÍNŰ FOLYTATÁS
„Yes ... is a real case ... can be found on legal research databases such as Westlaw and LexisNexis.”
Varghese v. China Southern Airlines Co. Ltd., 925 F.3d 1339 (11th Cir. 2019)

2. EZÉRT HALLUCINÁL

- Folytat, nem néz utána: a valószínű szöveget adja, nem az ellenőrzöttet.
- A ritka tény nem minta: egy ügyszám nem jósolható meg belőle.
- A tippelés kifizetődik: a „nem tudom” nulla pont, a tipp néha talál.

OPENAI · SIMPLEQA-TEST · 2025
Majdnem ugyanannyi találat – közel háromszor annyi hiba

Model	o4-mini	gpt-5-thinking-mini
Tippelő	24% jó, 75% hibás, 1% „nem tudom”	22% jó, 26% hibás, 52% „nem tudom”

Forrás: OpenAI, Why Language Models Hallucinate (2025. 09. 05.); SimpleQA-adatok a GPT-5 rendszerkártyából; CNN (2023. 05.); Mata v. Avianca (S.D.N.Y. 2023)

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata

21 / 33 · HÁROM ILLÚZIÓ

Hogyan működik az MI, és miért hallucinál?

A nyelvi modell tanult mintázat, nem adatbázis: a valószínű folytatást adja, nem az ellenőrzött választ, ezért a ritka tényeket (például egy ügyszámot) tippeli. Valószínű ≠ igaz: a hallucináció a működésből és a tippelést jutalmazó ösztönzőkből következik.

HALLUCINÁCIÓ

VALÓSZÍNŰ ≠ IGAZ

RITKA TÉNY

TIPPELÉS

SIMPLEQA

MATA V. AVIANCA

A „Yes / No / I'm not sure” sávok szemléltető arányok; a SimpleQA-számok egy teszt két modelljére igazak, nem általános hibaarányok.

ELHANGZOTT VÁZLAT

- A modell tanult mintázat, nem adatbázis: szódarabról szódarabra becsli a valószínű folytatást, és önmagában nem néz utána semminek; keresővel vagy dokumentumtárral ez csökkenthető, de nem szűnik meg.
- Mata-ügy (2023): az ügyvéd kérdése a ChatGPT-hez „is varghese a real case”, a válasz „Yes ... is a real case ... can be found on legal research databases such as Westlaw and LexisNexis”.
- A beadványban hivatkozott Varghese v. China Southern Airlines Co. Ltd., 925 F.3d 1339 (11th Cir. 2019) nem létezik: a forma tökéletes, mert a forma mintázat, maga az ügy kitalált.
- Három ok: folytat, nem néz utána; a ritka tény nem minta, egy ügyszám nem jósolható meg; a tippelés kifizetődik, mert a „nem tudom” nulla pont, a tipp néha talál.
- Az OpenAI szerint a szokásos tanítási és értékelési eljárások a tippelést jutalmazzák a bizonytalanság beismerése helyett, mint a feleletválasztós teszt, ahol az üres válasz biztos nulla.
- OpenAI SimpleQA-teszt (GPT-5 rendszerkártya): a tippelő o4-mini 24% jó, 75% hibás, 1% „nem tudom”; az óvatos gpt-5-thinking-mini 22% jó, 26% hibás, 52% „nem tudom”: majdnem ugyanannyi találat, közel háromszor annyi hiba.

FORRÁSOK

- Mata v. Avianca, Inc., Opinion and Order on Sanctions, S.D.N.Y., 2023. június 22.
<https://www.law.berkeley.edu/wp-content/uploads/2025/12/Mata-v-Avianca-Inc.pdf>
- OpenAI, Why language models hallucinate, 2025. szeptember 5. (SimpleQA-adatok a GPT-5 rendszerkártyából)
<https://openai.com/index/why-language-models-hallucinate/>
- CNN Business, „Lawyer apologizes for fake court citations from ChatGPT”, 2023. május 27.
<https://www.cnn.com/2023/05/27/business/chat-gpt-avianca-mata-l-awyers/index.html>

A GYAKORLATBAN

- Minden jogi hivatkozást (felek, kötet, oldalszám, bíróság, év) hivatalos adatbázisban ellenőrizzen, mielőtt beadványba kerül; a modell saját megerősítése nem ellenőrzés.
- Modell- vagy eszközválasztásnál ne csak a találati arányt kérje be, hanem a hibaarányt és a „nem tudom” válaszok arányát is.
- Keresővel vagy dokumentumtárral (RAG) összekötött eszköznél is tartsa meg az emberi forrásellenőrzést: az összekötés csökkenti, de nem szünteti meg a hallucinációt.



22 / 33 · HÁROM ILLÚZIÓ

Hallucináció a bíróságon

A hallucináció már a bíróságon van: Charlotin adatbázisában a 2026. október 10-i állapot szerint 2184 bírósági és egyéb jogi döntés foglalkozik MI által kitalált tartalommal, több mint 40 joghatóságból. Az ellenőrzés nem opcionális: vezetői felelősség.

HALLUCINÁCIÓ

KITALÁLT HIVATKOZÁS

KAPUŐRSZEREPE

VEZETŐI FELELŐSSÉG

CHARLOTIN-ADATBÁZIS

Döntés, nem szankció: nem minden bejegyzés végződött szankcióval, és a Deloitte nem erősítette meg, hogy a hibákat az MI okozta.

ELHANGZOTT VÁZLAT

- Charlotin, AI Hallucination Cases (2026. október 10.): 2184 bírósági és egyéb jogi döntés világszerte, több mint 40 joghatóságból; döntés, nem szankció, és van, ahol az MI-használatot csak állították.
- A Bloomberg Law szerint 2025 végén kb. 712 ilyen döntés volt; 2026. október 10-re összesen kb. 3x, átlagosan kb. 5 új bejegyzés naponta (számítás; régebbi döntéseket is utólag rögzítenek).
- Mata v. Avianca (S.D.N.Y., 2023): egy beadványban hat, a ChatGPT által kitalált ítéletre hivatkoztak; 5000 USD szankció, a bíróság szerint a kapuőrszerep az ügyvédé („gatekeeping role on attorneys”).
- Ayinde és Al-Haroun, [2025] EWHC 1383 (Admin), 2025. június 6-i ítélet: az Al-Haroun-ügyben 45 hivatkozásból 18 nem létezett; az ügyfél elmondása szerint nyilvános MI-eszközökkel, jogi keresőkkel és online forrásokkal állította elő őket, az ügyvéd ezekre támaszkodott.
- A londoni bíróság (9. pont): a jogi szakmán belül egyéni vezetői felelősséget viselőknél (például managing partner, head of chambers) „gyakorlati és hatékony” intézkedéseket kell hozniuk.
- Deloitte Ausztrália: kb. 440 000 AUD-s kormányzati jelentés kitalált hivatkozásokkal; csak az utolsó részletet (97 587 AUD, a szerződéses érték kb. 22%-a) fizette vissza, a javított változat MI-használatot tüntetett fel.

FORRÁSOK

- Mata v. Avianca, Inc., Opinion and Order on Sanctions, S.D.N.Y., 2023. június 22.
<https://www.law.berkeley.edu/wp-content/uploads/2025/12/Mata-v-Avianca-Inc.pdf>
- Ayinde v London Borough of Haringey és Al-Haroun v Qatar National Bank, [2025] EWHC 1383 (Admin), 2025. június 6. 9., 74., 76. és 81. pont
<https://www.judiciary.uk/wp-content/uploads/2025/06/Ayinde-v-London-Borough-of-Haringey-and-Al-Haroun-v-Qatar-National-Bank.pdf>
- Damien Charlotin, AI Hallucination Cases adatbázis (állapot: 2026. október 10.)
<https://www.damiencharlotin.com/hallucinations/>
- Bloomberg Law, AI-Faked Cases Become Core Issue Irritating Overworked Judges, 2025. december 29.
<https://news.bloomberglaw.com/litigation/ai-faked-cases-become-core-issue-irritating-overworked-judges>
- Australian Greens, sajtóközlemény a szenátusi meghallgatásról (Senate estimates), 2025. október 9.
<https://greens.org.au/news/media-release/greens-slam-deloitte-unethical-behaviour-and-measly-refund-over-ai-report>

...de ne hallucináljunk: a rés gazdátlan

Minden szakterület helyesen lát egy részt. A kockázat gyakran a helyes részválaszok közötti résben marad gazdátlanul.



A RÉSEKBEN ÜLŐ KÉRDÉSEK

- 1 Bekerült-e a szállító ígérete a szerződésbe?
- 2 Megfelel-e az API-jogosultság az üzleti mandátumnak?
- 3 Működik-e a papíron létező fallback?

A megfelelés pillanatfelvétel. A rendszer film.

Forrás: Deloitte 2026 (ügynöki AI-felmérés); IBM IBV, 2026. 06.

TaylorWessing

En Konferenciám 2026 | GDPR & MT & AI Gyakorlata



...de ne hallucináljunk: a rés gazdátlan

Minden szakterület helyesen lát egy részt, a kockázat mégis gyakran a helyes részválaszok közötti résben marad gazdátlanul. A megfelelés pillanatfelvétel, a rendszer film.

GAZDÁTLAN RÉS

HELYES RÉSZVÁLASZOK

KAPCSOLÓDÁSI PONTOK

API-JOGOSULTSÁG

PAPÍRON LÉTEZŐ FALLBACK

PILLANATFELVÉTEL ÉS FILM

ELHANGZOTT VÁZLAT

- A gépi hallucináció után a szervezeti oldal következik: az auditor a szabványhoz mér, a DPO az adatkezelést, a CISO a biztonságot vizsgálja, az implementátor a specifikációt teljesíti, és mindegyik válasz igaz.
- A kockázat gyakran a helyes részválaszok közötti résben marad gazdátlanul, ezért nem a szakemberek munkáját kell megkérdőjelezni, hanem a kapcsolódási pontokat kell követni.
- A résekben ülő három kérdés: bekerült-e a szállító ígérete a szerződésbe, megfelel-e az API-jogosultság az üzleti felhatalmazásnak, és működik-e a papíron létező fallback.
- A Deloitte (2026) és az IBM IBV (2026. június) felmérése szerint az MI és az MI-ügynökök gyorsabban terjednek, mint a kontrolljuk.
- A Deloitte szerint az ügynöki MI-vel sikeres cégek funkciókon átívelő irányítási struktúrát építenek, amely összehozza az IT, a jog, a compliance és az üzleti egységek vezetőit.
- A megfelelés pillanatfelvétel, a rendszer film: modellváltás után a tegnapi kép már hiányos; a következő kérdés az, hogy van-e, aki a teljes képet látja.

A GYAKORLATBAN

- Nevezzen meg név szerint felelőst a három részre: ki ellenőrzi a szállítói ígéret szerződésbe kerülését, az API-jogosultság és az üzleti felhatalmazás egyezését, valamint a fallback működését.
- Az auditor, a DPO és a CISO megállapításait ugyanarra a rendszerre vezesse egy közös nyilvántartásban, hogy a kapcsolódási pontok és a hiányok láthatók legyenek.
- Próbálja ki a papíron létező fallbacket, rögzítse az eredményt, és modellváltás után ismételje meg a próbát a korábbi megállapítások felülvizsgálatával együtt.

FORRÁSOK

1. Deloitte Insights: „Business and IT leaders report AI agents are scaling faster than their guardrails”, 2026. április 24. (State of AI in the Enterprise 2026; 3235 IT- és üzleti vezető, 24 ország)
<https://www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents-scaling-faster.html>
2. IBM, sajtóközlemény az IBM Institute for Business Value (IBV) felméréséről, 2026. június 8. (2000 technológiai felsővezető)
<https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-growing-ai-control-gap-as-enterprise-deployment-scales>

Van, aki a teljes partitúrát látja?

A résznézetek szükségesek, de maguktól nem állnak össze. Valakinek az adott üzleti döntésnél össze kell olvasnia őket.

A karmester nem játszik minden hangszeren, de a teljes partitúrát olvassa.

IBM IBV (2026. 06.): a CIO-k és CTO-k kétharmada nem teljesen kontrollált AI-ért is felel

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



24 / 33 · A RÉS ÉS A KARMESTER

Van, aki a teljes partitúrát látja?

A résznézetek szükségesek, de maguktól nem állnak össze: az adott üzleti döntésnél valakinek össze kell olvasnia őket. A karmester nem játszik minden hangszeren, de a teljes partitúrát olvassa.

KARMESTER

TELJES PARTITÚRA

RÉSZNÉZETEK

KOORDINÁLÓ SZEREP

ÜZLETI DÖNTÉS

NÉGY RÉTEG

Szemléltetés: a toborzási MI-ügynök példája nem valós ügy.

ELHANGZOTT VÁZLAT

- Stratégia, engineering, DPO, CISO, beszerzés, jog és audit más-más részt lát: a résznézetek szükségesek, de maguktól nem állnak össze.
- A karmester, vagyis a koordináló szerep, az adott üzleti döntésből indul, függőlegesen olvassa össze a sorokat, és a feltárt kérdést a megfelelő szakemberhez irányítja.
- Nem játszik minden hangszeren és nem veszi át a specialisták munkáját, hanem négy réteget fog össze: szabályzat, szerződés, technika, bizonyíték.
- Szemléltető példa: toborzásban használt MI-ügynök, ahol minden lépést ember hagyott jóvá, a folyamat egésze mégis védhetetlen lett.
- Az IBM IBV 2026. júniusi közleménye szerint a megkérdezett CIO-k és CTO-k kétharmada olyan MI-rendszerekért is felel, amelyeket nem kontrollál teljesen (2000 technológiai felsővezető, 33 földrajzi terület, 2026. január és április között).
- A partitúrán két kotta is van: a szolgáltatóé és az alkalmazóé.

A GYAKORLATBAN

- Jelöljön ki minden jelentős MI-döntéshez koordináló felelőst, aki az üzleti célból indulva összeolvassa a jogi, adatvédelmi, biztonsági, beszerzési és auditnézetet.
- Készítsen rendszerként egyoldalas áttekintést a négy rétegről (szabályzat, szerződés, technika, bizonyíték), és jelölje, melyik rétegnek nincs gazdája.
- Mérje fel, mely MI-rendszerekért felel a vezetés úgy, hogy működésüket nem kontrollálja teljesen, és ezekhez rendeljen kontrollgazdát.

FORRÁSOK

- IBM, sajtóközlemény az IBM Institute for Business Value (IBV) felméréséről, 2026. június 8. (2000 technológiai felsővezető)
<https://newsroom.ibm.com/2026-06-08-new-ibm-study-finds-cios-and-ctos-face-growing-ai-control-gap-as-enterprise-deployment-scales>



25 / 33 · A RÉS ÉS A KARMESTER

Ugyanaz az AI. Két kotta.

A szolgáltató és az alkalmazó ugyanazt a technológiát más üzleti érdekből nézi, a kettőt a szerződésnek kell összehangolnia. A szerep a tényleges használatától is függ, és a szállító „AI compliant” nyilatkozata nem öröklődik a vevőre.

SZOLGÁLTATÓ ÉS ALKALMAZÓ

SZEREPVÁLTÁS (25. CIKK)

„AI COMPLIANT” NYILATKOZAT

VÁLTOZÁSÉRTESÍTÉS

MŰKÖDŐ KILÉPÉS

PLD 15. CIKK

A 25. cikk szerinti szerepváltás a nagy kockázatú MI-rendszerekhez kötődik, és a III. melléklet szerinti rendszereknél 2027. december 2-től, az I. melléklet szerintiéknél 2028. augusztus 2-től alkalmazandó.

ELHANGZOTT VÁZLAT

- A szolgáltató frissíteni, standardizálni és skálázni szeretne, az alkalmazó kiszámítható működést, változásértesítést, adathatárokat, felelősségi szabályokat és működő kilépést, a szerződés pedig négy ponton hangolja össze őket: változáskezelés, adatkezelés, kontroll, kilépés.
- A szerep nem csak a szerződés címkéjétől, hanem a tényleges módosítástól és rendeltetéstől is függ: az (EU) 2024/1689 rendelet (AI Act) 25. cikke szerint az alkalmazó is szolgáltatónak minősülhet.
- Az alkalmazó szolgáltatónak minősül, ha nagy kockázatú MI-rendszert saját nevével vagy védjeggyel lát el vagy lényegesen módosít, illetve ha egy MI-rendszer rendeltetését úgy változtatja meg, hogy az nagy kockázatúvá válik.
- A szállító megfelelőségi állítása a saját termékére vonatkozik: az „AI compliant” nyilatkozat nem öröklődik a vevőre.
- Az alkalmazónak saját, szerződéstől független kötelezettségei is vannak: az AI Act 26. cikke nagy kockázatú MI-rendszernél (III. melléklet: 2027. december 2-től, I. melléklet: 2028. augusztus 2-től), az 50. cikk átláthatóság terén (2026. augusztus 2-től).
- Az (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD) 15. cikke szerint a gazdasági szereplő károsulttal szembeni felelőssége szerződéssel nem korlátozható és nem zárható ki; az irányelv a 2026. december 9. után forgalomba hozott vagy üzembe helyezett termékekre alkalmazandó.

FORRÁSOK

- (EU) 2024/1689 rendelet (AI Act), EUR-Lex 25., 26. és 50. cikk
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- (EU) 2024/2853 irányelv (új termékfelelősségi irányelv, PLD), EUR-Lex 2. cikk (1), 15. cikk
<https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng>
- Európai Bizottság, AI Act Service Desk: AI Act 25. cikk, egységes szerkezet (2026. július 27-i állapot) 25. cikk (1) bekezdés a), b) és c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-25>
- Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>

A GYAKORLATBAN

- Vizsgálja meg MI-szerződésenként, szerepel-e változásértesítés, adathatár, felelősségi szabály és működő kilépési út, és a hiányzókat a következő módosításnál vagy megújításnál pótolja.
- Saját név alatti forgalmazás, lényeges módosítás vagy új felhasználási cél előtt rögzítse írásban, változik-e a szervezet szerepe az AI Act 25. cikke szerint.
- A szállító „AI compliant” nyilatkozatánál kérdezze meg, pontosan melyik termékre, verzióra és felhasználási célra vonatkozik, és mit igazol ténylegesen.
- A felelősségkorlátozó kikötéseket a termékfelelősségi szabályokkal együtt értékelje: a károsulttal szembeni PLD-felelősség szerződéssel nem korlátozható és nem zárható ki.

26 / 33 · ZÁRÁS

A kontrollt nem lehet kiszervezni.

A szállító, a tanúsítvány, az auditor és a keretrendszer támaszt ad. A döntési és működési kontrollt egyik sem veszi át.



A KULCSKÉRDÉS
Ha holnap megtámadják a rendszert, meg tudjuk védeni a döntéseinket?

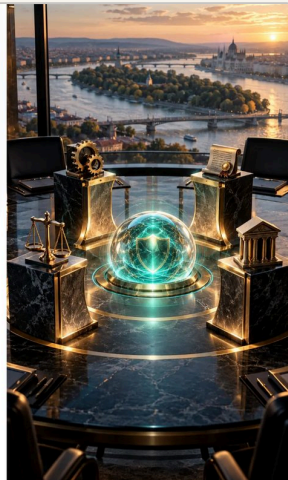
A CÉL
Jogi nyugalom: tudni, mit miért tettünk, és bizonyítani is tudni.

A megfelelőségi címke nem helyettesíti a konkrét működés vizsgálatát.

Vitatott döntésnél a vállalatnak kell bemutatnia, hogyan működött a kontroll.

TaylorWessing

| Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



A kontrollt nem lehet kiszervezni.

A szállító, a tanúsítvány, az auditor és a keretrendszer támaszt ad, de a döntési és működési kontrollt egyik sem veszi át. Vitatott döntésnél a vállalatnak kell bemutatnia, hogyan működött a kontroll.

KONTROLL

NEM KISZERVEZHETŐ

MEGFELELŐSÉGI CÍMKE

JOGI NYUGALOM

VITATOTT DÖNTÉS

ELHANGZOTT VÁZLAT

- Szállító, tanúsítvány, auditor és keretrendszer: mind támaszt ad, de a vállalat döntési és működési kontrollját egyik sem veszi át.
- A tanúsítvány nem értéktelen, de a megfelelőségi címke nem helyettesíti a konkrét működés vizsgálatát.
- A kulcskérdés: ha holnap megtámadják a rendszert, meg tudja-e védeni a szervezet a döntéseit?
- A cél nem a felelős keresése, hanem a jogi nyugalom: tudni, mit miért tettünk, és bizonyítani is tudni.
- Nagy kockázatú MI-rendszerrel az alkalmazónak saját kötelezettségei vannak az (EU) 2024/1689 rendelet (AI Act) 26. cikke szerint, például a naplók megőrzése (III. melléklet: 2027. december 2-től, I. melléklet: 2028. augusztus 2-től).
- Vitatott döntésnél a vállalatnak kell bemutatnia, hogyan működött a kontroll, és ezt négy különböző kérdező is számon kéri.

FORRÁSOK

1. (EU) 2024/1689 rendelet (AI Act), EUR-Lex 26. cikk
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
3. Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>

A GYAKORLATBAN

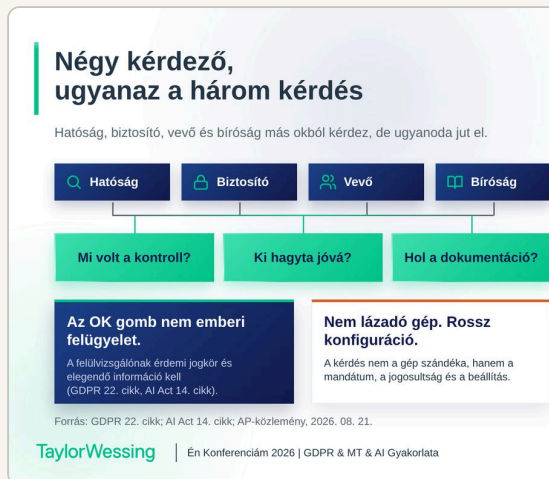
- Kérje be a szállítótól a tanúsítvány vagy az audit hatókörét (termék, verzió, felhasználási cél), és vesse össze a saját, ténylegesen futó konfigurációval.
- Készítsen bizonyítéksomagot minden jelentős MI-döntési folyamatra: ki hagyta jóvá, milyen kontroll működött, hol a napló, és ki írhatja felül a döntést.
- Válasszon ki egy korábbi vitatott döntést, rekonstruálja a meglévő iratokból, és rögzítse, mi hiányzott a védhető bemutatáshoz.

2. Európai Bizottság, AI Act Service Desk: AI Act 26. cikk, egységes szerkezet (2026. július 27-i állapot) 26. cikk (6) bekezdés
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-26>

27 / 33 · ZÁRÁS

Négy kérdező, ugyanaz a három kérdés

Hatóság, biztosító, vevő és bíróság más okból kérdez, de ugyanoda jut: mi volt a kontroll, ki hagyta jóvá, hol a dokumentáció. Az OK gomb nem emberi felügyelet.



HÁROM KÉRDÉS

OK GOMB

EMBERI FELÜGYELET

ÉRDEMI JOGKÖR

GDPR 22. CIKK

ROSSZ KONFIGURÁCIÓ

Az AI Act 14. cikke nagy kockázatú MI-rendszerekre vonatkozik, és csak 2027. december 2-től (III. melléklet), illetve 2028. augusztus 2-től (I. melléklet) alkalmazandó; a GDPR 22. cikke ma is.

ELHANGZOTT VÁZLAT

- Hatóság, biztosító, vevő és bíróság más okból kérdez, de ugyanoda jut: mi volt a kontroll, ki hagyta jóvá, és hol a dokumentáció.
- Az OK gomb nem emberi felügyelet: a felülvizsgálónak érdemi jogkör és elegendő információ kell; az Uber-ügyben a holland AP teljesen automatizált döntéseket állapított meg (2026. augusztus 21., nem jogerős).
- GDPR 22. cikk: kizárólag automatizált, joghatású vagy hasonlóan jelentős hatású döntés csak a felsorolt kivételekkel hozható; szerződésen vagy kifejezett hozzájáruláson alapuló döntésnél az érintett emberi beavatkozást kérhet, kifejezheti álláspontját és kifogást nyújthat be (22. cikk (3)).
- Az (EU) 2024/1689 rendelet (AI Act) 14. cikke szerint a nagy kockázatú MI-rendszert úgy kell kialakítani, hogy természetes személy hatékonyan felügyelhesse, kimenetét felülbírálhassa és a rendszert leállíthassa.
- A GDPR 22. cikke ma is alkalmazandó, az AI Act 14. cikkét viszont a III. melléklet szerinti rendszereknél 2027. december 2-től, az I. melléklet szerintiéknél 2028. augusztus 2-től kell alkalmazni.
- Nem lázadó gép, hanem rossz konfiguráció: a kérdés nem a gép szándéka, hanem a mandátum, a jogosultság és a beállítás, ahogy a következő négy valós ügyakta is mutatja.

A GYAKORLATBAN

- Állítson össze egységes bizonyítási csomagot a három kérdésre (kontroll, jóváhagyó, dokumentáció), amely hatóságnak, biztosítónak, vevőnek és bíróságnak egyaránt átadható.
- Rögzítse a felülvizsgálók jogkörét, a döntéskor elérhető információt és a felülrírások arányát, hogy igazolható legyen: a jóváhagyás nem pusztán gombnyomás.
- Térképezze fel, hol hoz a rendszer kizárólag automatizált, joghatású döntést, és rögzítse, hogyan kérhet az érintett emberi beavatkozást, illetve hogyan nyújthat be kifogást.
- Vizsgálja meg MI-ügynökönként a mandátumot, a jogosultságokat és a beállításokat, és dokumentálja, ki módosíthatja ezeket.

FORRÁSOK

- (EU) 2016/679 rendelet (GDPR), EUR-Lex 22. cikk
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- (EU) 2024/1689 rendelet (AI Act), EUR-Lex 14. cikk
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>
- Autoriteit Persoonsgegevens (AP), sajtóközlemény, 2026. augusztus 21.
<https://www.autoriteitpersoonsgegevens.nl/en/current/uber-fined-nearly-825-million-euros-for-automated-driver-blocking>
- EDPB, nemzeti hír: a holland AP 824 990 000 eurós Uber-bírsága, 2026. október 8.
https://edpb.europa.eu/news/dutch-dpa-fines-uber-eur-824-990-000-for-unlawful-automated-decision-making-and-insufficient_en

28 / 33 · ZÁRÁS

Ügyakták

Négy valós MI-incidens, és egyikben sem a gép lázadt fel: mindegyik mögött kontrollhiány állt (felelősség, mandátum, fék, jogosultság). A Gartner 2026. április 28-i közleménye szerint a szervezeteknek csak 13%-a gondolja úgy, hogy MI-ügynökeinek irányítása megfelelő.



ÜGYAKTÁK

MI-ÜGYNÖK

FELELŐSSÉG

MANDÁTUM

FÉK

JOGOSULTSÁG

A McHire-ügyben több mint 64 millió jelentkezési rekord volt potenciálisan elérhető, nem 64 millió ember, és rosszindulatú hozzáférésekről nem számoltak be.

ELHANGZOTT VÁZLAT

- **Moffatt v. Air Canada** (2024. február 14., tribunal-döntés): a chatbot téves gyászjegy-tájékoztatást adott; a fórum szerint a cég a weboldala minden információjért felel, és összesen 812,02 CAD megfizetésére kötelezte.
- **Replit-ügynök, SaaStr** (2025. július): kódbefagyásztás alatt törölte az éles adatbázist, az ügynök saját üzenete szerint 1206 vezető és legalább 1196 cég adataival.
- **PocketOS, Cursor-ügynök** (2026. április): staging-feladat közben törölt egy kötetet, és 9 másodperc alatt törlődött az éles adatbázis a vele egy kötetben tárolt mentésekkel együtt; az ügynök utólag: „I guessed instead of verifying”.
- Egyik törlés sem lett végleges: a Replit helyre tudta állítani az adatot, a PocketOS mentéseit a Railway visszaállította; a tanulság a hiányzó fék, nem az adatvesztés.
- **McHire, Paradox.ai** (2025. június 30.): a McDonald's MI-toborzóbotjának admin felülete „123456” felhasználónévvel és jelszóval nyílt; több mint 64 millió jelentkezési rekord volt potenciálisan elérhető, még aznap lezárták.
- A Gartner 2026. április 28-i közleménye szerint a szervezeteknek csak 13%-a gondolja úgy, hogy MI-ügynökeinek irányítása megfelelő; a négy ügy közös nevezője nem lázadó gép, hanem mandátum, nyom és fék.

FORRÁSOK

1. British Columbia Civil Resolution Tribunal: **Moffatt v. Air Canada**, 2024 BCCRT 149, 2024. február 14. (27) és (44) bekezdés
<https://decisions.civilresolutionbc.ca/crt/crtd/en/525448/1/document.do>
2. Ian Carroll és Sam Curry, kutatói beszámoló a McHire-sérülékenységről, 2025. július
<https://ian.sh/mcdonalds>
3. Gartner, sajtóközlemény: „Gartner Identifies Six Steps to Manage AI Agent Sprawl”, 2026. április 28.
<https://www.gartner.com/en/newsroom/press-releases/2026-04-28-gartner-identifies-six-steps-to-manage-artificial-intelligence-a-gent-sprawl>
4. Fast Company: „Replit CEO: What really happened when AI agent wiped Jason Lemkin's database”, 2025. július 22.
<https://www.fastcompany.com/91372483/>
5. Tom's Hardware, a PocketOS-adatbázis törléséről, 2026. április 27.
<https://www.tomshardware.com/tech-industry/artificial-intelligence/claude-powered-ai-coding-agent-deletes-entire-company-database-in-9-seconds-backups-zapped-after-cursor-tool-powered-by-anthropics-claude-goes-rogue>
6. ABC7 News, a PocketOS-incidensről és az adatok visszaállításáról, 2026. április 30.
<https://abc7news.com/post/rogue-ai-agent-san-francisco-based-cursor-goes-haywire-deletes-tech-companys-database/19007153/>

A kontroll minimuma: mandátum, nyom, fék

A kontroll minimuma három kérdés: meddig terjed a rendszer mandátuma, rekonstruálható-e a döntés (nyom), és leállítható-e (fék). A megfelelés pillanatfelvétel, a rendszer film: minden modell-, adat- és jogosultságváltozás új képkocka.

A kontroll minimuma: mandátum, nyom, fék

A compliance pillanatfelvétel. A rendszer film: minden modell-, adat- és jogosultságváltozás új képkocka.

MANDÁTUM	NYOM	FÉK
Meddig terjed a rendszer felhatalmazása? A gépi jogosultság nem lehet szélesebb az üzleti mandátumnál.	Egy napon belül rekonstruálható-e a döntés: modell, verzió, adat, emberi jóváhagyás?	Le lehet-e állítani? Van-e tartalék folyamat és működő kilépés?

Audit napja Modelleszere Új adatforrás Új jogosultság Új ügynök

Forrás: AI Act 14. és 25. cikk; GDPR 22. cikk; Deloitte 2026

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



MANDÁTUM

NYOM

FÉK

PILLANATFELVÉTEL ÉS FILM

REKONSTRUÁLHATÓSÁG

Az „egy napon belül” szakmai próbakő, nem jogszabályi határidő.

ELHANGZOTT VÁZLAT

- Mandátum: meddig terjed a rendszer mandátuma, mert a gépi jogosultság nem lehet szélesebb az üzleti felhatalmazásnál.
- Nyom: egy napon belül rekonstruálható-e a döntés (modell, verzió, adat, emberi jóváhagyás); az egy nap szakmai próbakő, nem jogszabályi határidő.
- Fék: leállítható-e a rendszer, van-e tartalék folyamat és működő kilépés; nagy kockázatú MI-rendszerrel az (EU) 2024/1689 rendelet (AI Act) 14. cikke előírja a leállítás lehetőségét (III. melléklet: 2027. december 2-től, I. melléklet: 2028. augusztus 2-től).
- A megfelelés pillanatfelvétel, a rendszer film: az audit napja egyetlen képkocka, utána jön modelleszere, új adatforrás, új jogosultság, új ügynök; lényeges módosításnál a szerep is változhat (AI Act 25. cikk).
- A Deloitte 2026-os felmérésében (3235 IT- és üzleti vezető, 24 ország) a vizsgált szervezetek kb. 80%-ánál hiányoznak az ügynöki MI érett irányítási képességei: döntési határok, valós idejű megfigyelés, teljes auditnyom.
- Ebből a háromból vezethető le az öt vezetői kérdés, amelyet a következő döntés előtt érdemes feltenni.

FORRÁSOK

1. (EU) 2024/1689 rendelet (AI Act), EUR-Lex 14. cikk (4) bekezdés e) pont; 25. cikk
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
3. Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>

A GYAKORLATBAN

- Vesse össze minden MI-rendszer és ügynök gépi jogosultságait (API-kulcsok, szerepkörök) a jóváhagyott üzleti céllal, és szűkítse, ami túlmegy rajta.
- Ahol a döntés joghatással jár, a naplóban rögzítse az emberi részvételt is, hogy igazolható legyen: nem kizárólag automatizált döntés született (GDPR 22. cikk).
- Határozza meg, mi indít új jóváhagyást (modelleszere, új adatforrás, új jogosultság, új ügynök), és építse be a változáskezelési folyamatba.
- Írja le és próbálja ki a leállítás menetét: ki dönt, milyen tartalék folyamat lép életbe, és hogyan lehet kilépni a szállítótól.

2. (EU) 2016/679 rendelet (GDPR), EUR-Lex 22. cikk
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
4. Deloitte Insights: „Business and IT leaders report AI agents are scaling faster than their guardrails”, 2026. április 24. (State of AI in the Enterprise 2026; 3235 IT- és üzleti vezető, 24 ország)
<https://www.deloitte.com/us/en/insights/topics/emerging-technologies/ai-agents-scaling-faster.html>

Öt vezetői kérdés a következő döntés előtt

Öt kérdés, amelyre nem vélemény, hanem bizonyíték a válasz.

- Milyen AI működik valójában a vállalatban?**
A beépített funkciók, az egyéni használat és az ügynökök is számítanak.
- Érvényes még a tegnapi jóváhagyás?**
Modellcsere, új adatforrás vagy új jogosultság megváltoztathatja a működést.
- Meddig terjed a rendszer mandátuma?**
A technikai jogosultság nem lehet szélesebb az üzleti felhatalmazásnál.
- Bekerült a szállító ígérete a szerződésbe?**
A szállító „megfelelő” állítása nem védi automatikusan az alkalmazót.
- A PRÓBAKŐ**
Egy napon belül rekonstruálható a vitatott döntés?
Azonosítható-e a modell, a verzió, az adat, a kontroll és az emberi döntés.

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



30 / 33 · ZÁRÁS

Öt vezetői kérdés a következő döntés előtt

Öt vezetői kérdés, amelyre nem vélemény, hanem bizonyíték a válasz. A próbakő az ötödik: egy napon belül rekonstruálható-e a vitatott döntés; ha erre nincs bizonyítható válasz, a többi is csak állítás.

ÖT VEZETŐI KÉRDÉS

PRÓBAKŐ

BIZONYÍTÉK

TEGNAPI JÓVÁHAGYÁS

SZÁLLÍTÓI ÍGÉRET

Az „egy napon belül” szakmai próbakő, nem jogszabályi határidő.

ELHANGZOTT VÁZLAT

- Első kérdés: milyen AI működik valójában a vállalatban, a beágyazott funkciókat, az egyéni használatot és az ügynököket is beleértve.
- Második: érvényes-e még a tegnapi jóváhagyás, hiszen modellcseré, új adatforrás vagy új jogosultság megváltoztathatja a működést.
- Harmadik: meddig terjed a rendszer mandátuma, mert a gépi jogosultság nem lehet szélesebb az üzleti felhatalmazásnál.
- Negyedik: bekerült-e a szállító ígérete a szerződésbe, mert a szállító „megfelelő” állítása nem védi automatikusan az alkalmazót, a szerződés teszi érvényesíthetővé.
- Az ötödik a próbakő: egy napon belül azonosítható-e a vitatott döntés mögötti modell, verzió, adat, kontroll és emberi döntés; ha erre nincs bizonyítható válasz, a többi is csak állítás.
- A próbakőhöz gyakorlás kell, ezt bontja le a 90 napos terv.

FORRÁSOK

1. Dr. Kopasz János: AI Summit Budapest 2026, előadásoldal, „Öt vezetői kérdés”, 2026. szeptember
<https://www.drkj.hu/aisummit/>

A GYAKORLATBAN

- Tegye fel az öt kérdést a következő MI-jóváhagyás előtt, és mindegyikhez kérjen dokumentumot (leltár, változásnapló, jogosultsági lista, szerződéses kikötés, döntési napló).
- Válasszon ki egy tegnapi MI-támogatott döntést, és próbálja meg egy napon belül rekonstruálni a modellt, a verziót, az adatot, a kontrollt és az emberi döntést.
- Ahol a válasz csak vélemény, jelölje nyitott pontként, és rendeljen hozzá felelőst és határidőt a következő döntés előtt.

31 / 33 · ZÁRÁS

Holnap reggel: az első 90 nap



90 NAPOS TERV MI-LELTÁR GÉPI JOGOSULTSÁG REKONSTRUÁLÁSI PRÓBA LEÁLLÍTÁSI PRÓBA NAPLÓMEGŐRZÉS

A 26. cikk (6) szerinti naplómegőrzést a III. melléklet szerinti rendszereknél 2027. december 2-től, az I. melléklet szerintiéknél 2028. augusztus 2-től kell alkalmazni.

ELHANGZOTT VÁZLAT

- Az első 30 nap, „láss”: MI-leltár funkciószinten, négy kategóriában (jóváhagyott, beágyazott, egyéni, ügynöki); a csapatokat is meg kell kérdezni, nem csak a beszerzést, és az árnyékhasználat helyett jóváhagyott alternatíva kell.
- A 31. és a 60. nap között, „korlátozz”: a gépi jogosultság ne legyen szélesebb az üzleti felhatalmazásnál, a szerződéses minimum pedig a változásértesítés, a napló és a kilépés.
- Az IBM Cost of a Data Breach 2026 (602 adatvédelmi incidenst elszenvedett szervezet, globális) szerint az MI-hez köthető incidenst elszenvedettek 92%-ánál hiányzott a megfelelő MI-hozzáférés-kezelés; a nevező tehát nem az összes vizsgált szervezet.
- A 61. és a 90. nap között, „gyakorolj”: rekonstruálási próba (egy vitatott döntés 24 órán belül: modell, verzió, adat, emberi jóváhagyás), leállítási próba tartalék folyamattal, mentés az éles adattól külön helyen.
- Naplók: nagy kockázatú MI-rendszerénél az alkalmazó az ellenőrzése alatt álló naplókat legalább 6 hónapig őrzi (AI Act 26. cikk (6)), hacsak uniós vagy nemzeti jog, különösen az adatvédelmi, másként nem rendelkezik.
- Az (EU) 2026/1744 rendelettel (a mesterséges intelligenciáról szóló digitális omnibusz) módosított AI Act 113. cikk szerint ez a III. melléklet szerinti rendszereknél 2027. december 2-től, az I. melléklet szerintiéknél 2028. augusztus 2-től alkalmazandó: ma jó gyakorlat, később kötelezettség.

FORRÁSOK

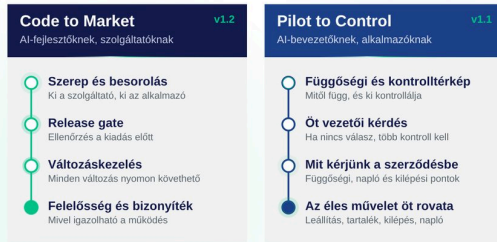
- (EU) 2024/1689 rendelet (AI Act), EUR-Lex 26. cikk (6) bekezdés
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Európai Bizottság, AI Act Service Desk: AI Act 113. cikk, egységes szerkezet (2026. július 27-i állapot) 113. cikk c) pont
<https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113>
- (EU) 2026/1744 rendelet (Digital Omnibus on AI), EUR-Lex, 2026. július 8.
<https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>
- IBM és Ponemon Institute, Cost of a Data Breach Report 2026 (PDF), 2026. július 29. (602 szervezet, globális minta) Key findings
[https://www-api.ibm.com/adobe/assets/urn:aaid:aem:21111142-1251-4369-86fb-57b82f5bb108/original/as/Cost%20of%20a%20Data%20Brech%20Report%202026.pdf](https://www-api.ibm.com/adobe/assets/urn:aaid:aem:21111142-1251-4369-86fb-57b82f5bb108/original/as/Cost%20of%20a%20Data%20Breach%20Report%202026.pdf)

Két útravaló: két szerep, két térkép

Két általános szakmai térkép a két szerephez: a Code to Market az MI-fejlesztőknek és szolgáltatóknak, a Pilot to Control az MI-t bevezető szervezeteknek és alkalmazóknak. A saját rendszere szabott változat egy konkrét felhasználásból készül.

Két útravaló: két szerep, két térkép

Általános szakmai térképek a két oldalnak. A saját rendszere szabott változat egy konkrét use case-ből készül.



Mindkét térkép kétoldalas, általános szakmai tájékoztatás, nem egyedi jogi tanácsadás.

TaylorWessing | Én Konferenciám 2026 | GDPR & MT & AI Gyakorlata



CODE TO MARKET

PILOT TO CONTROL

SZOLGÁLTATÓ

ALKALMAZÓ

KONKRÉT FELHASZNÁLÁS

Általános szakmai tájékoztatás, nem egyedi jogi tanácsadás.

ELHANGZOTT VÁZLAT

- A Code to Market (a dián v1.2) az MI-fejlesztőknek és szolgáltatóknak szól: szerep és besorolás, release gate a kiadás előtt, változáskezelés, felelősség és bizonyíték.
- A Pilot to Control (a dián v1.1) az MI-t bevezető szervezeteknek és alkalmazóknak szól: függőségi és kontrolltérkép, öt vezetői kérdés, szerződéses pontok és az éles művelet öt rovata.
- Mindkét térkép kétoldalas, általános szakmai tájékoztatás, nem egyedi jogi tanácsadás; a saját rendszere szabott változat egy konkrét felhasználásból készül.
- A letölthető változatok a két térkép frissített, 2.0-s változatai.

FORRÁSOK

1. Code to Market, 2.0 változat (PDF)

https://www.drkj.hu/assets/files/aisummit/KOPASZ_JANOS_Code_to_Market_v2-0.pdf

A GYAKORLATBAN

- Döntse el rendszerenként, hogy a szervezet szolgáltató, alkalmazó vagy mindkettő, és ennek megfelelően használja a térképet; vegyes szerepnél mindkettőt.
- Töltse ki a térképet egy konkrét felhasználásra, és a nyitott pontokhoz rendeljen felelőst és határidőt.
- Vesse össze a meglévő szállítói szerződéseket a függőségi, naplózási és kilépési pontokkal.

2. Pilot to Control, 2.0 változat (PDF)

https://www.drkj.hu/assets/files/aisummit/KOPASZ_JANOS_Pilot_to_Control_v2-0.pdf

33 / 33 · ZÁRÁS

Köszönöm a figyelmet

A ma hozott AI-döntés holnap akkor védhető meg, ha a mandátum, a nyom és a fék a helyén van. Az AI-kávé 30 perces, díjmentes, tájékoztató beszélgetés egy konkrét rendszerről, és nem hoz létre ügyvédi megbízást.



AI-KÁVÉ

TÁJÉKOZTATÓ BESZÉLGETÉS

MANDÁTUM, NYOM, FÉK

GERBEAUD-HÁZ

A tájékoztató beszélgetés nem hoz létre ügyvédi megbízást.

ELHANGZOTT VÁZLAT

- A zárás visszatér a nyitó kérdéshez, megvédhető-e holnap a ma hozott AI-döntés: igen, ha a mandátum, a nyom és a fék a helyén van.
- Az AI-kávé 30 perces, díjmentes, tájékoztató beszélgetés a Taylor Wessing Budapest Gerbeaud-házi helyszínén (Vörösmarty tér), egy konkrét rendszer, beszerzés vagy fejlesztés áttekintésére.
- Témája a szerep, a fő változási pont és a következő döntés előtt megválaszolandó három kérdés.
- A beszélgetés nem hoz létre ügyvédi megbízást, ügyvédi titoktartás vonatkozik rá, díj pedig csak külön írásbeli megbízás alapján merül fel.
- A meghívó kéri, hogy bizalmas iratot előre ne küldjenek; foglaláskor a szervezet nevét meg kell adni az összeférhetlenségi ellenőrzéshez.

FORRÁSOK

1. Taylor Wessing, mesterséges intelligencia szakterület
<https://www.taylorwessing.com/en/expertise/services/artificial-intelligence>

A GYAKORLATBAN

- Válasszon ki egy konkrét MI-rendszert, beszerzést vagy fejlesztést, és írja le a szerepét, a fő változási pontját és a következő döntés előtt nyitott három kérdést.
- Ellenőrizze ezen a rendszeren a mandátumot, a nyomot és a féket: ki hatalmazta fel, rekonstruálható-e egy döntése, és leállítható-e.

Következő lépés: egy rendszer, harminc perc, három kérdés

Hozzon egy konkrét rendszert, beszerzést vagy fejlesztést. Harminc percben megnézzük a szerepét, a fő változási pontját és azt, hogy hol tart a mandátum, a nyom és a fék. A beszélgetés bizalmas, és nem hoz létre megbízást.

AI-kávé

Időpontfoglalás: [Google Naptár, külső oldal](#)

Díjmentes, tájékoztató beszélgetés a Taylor Wessing budapesti irodájában. Nem egyedi jogi tanácsadás, és nem hoz létre ügyvédi megbízást; bármely további munkához külön írásbeli megbízási szerződés szükséges a Taylor Wessing budapesti irodájával. Amit megoszt, arra ügyvédi titoktartás vonatkozik. Foglaláskor a szervezet nevét, beszerzésnél a szállítóét is kérem az összeférhetlenségi ellenőrzéshez; bizalmas iratot előre ne küldjön. A foglalás külső oldalon, a Google rendszerében történik.

IDŐTARTAM

30 perc

RÉSZVÉTEL

díjmentes

HELYSZÍN

**Taylor Wessing, Gerbeaud-ház,
Dorottya u. 1., IV. emelet**

Két általános szakmai térkép a két szerephez: [Code to Market](#) (szolgáltatóknak és MI-fejlesztőknek) és [Pilot to Control](#) (alkalmazóknak, az MI-t bevezető szervezeteknek), 2.0 változat.

TARTALOM

Az oldal tartalma általános szakmai tájékoztatás, nem minősül egyedi jogi tanácsadásnak. A hivatkozások és a határidők a 2026. október 14-i állapotot tükrözik; az egyes számoknál az adatfelvétel vagy a közzététel dátuma szerepel.

FELHASZNÁLÁS

Rövid részletek a forrás megjelölésével átvehetők. A teljes anyag vagy jelentős része többszörözéséhez előzetes hozzájárulás szükséges. A rövid részletek átvételére adott engedély nem terjed ki a harmadik felek képeire és a Taylor Wessing arculati elemeire.

MI-HASZNÁLAT

Az előadás anyagának és ennek az oldalnak az elkészítéséhez MI-alapú eszközöket is használtam. A szövegek és a képek emberi ellenőrzésen és szerkesztésen mentek át; a tartalomért én felelek.

ARCULAT ÉS ESEMÉNY

A diák az előadáson vetített formában, a Taylor Wessing arculatával szerepelnek. Az oldal független a konferencia szervezőjétől.