

Milyen információbiztonsági kockázatok merülnek fel általános célú MI-rendszerek (LLM) vállalati használatánál? NIS2 és AI Act előírások a kockázatok kezelésére

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/43

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.17	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Az általános célú MI-rendszerek, vagyis a nagy nyelvi modellekre épülő asszisztensek és az ezekből építkező MI-ügynökök nem új szoftverkategóriát, hanem új adatáramlási útvonalat és új cselekvő szereplőt hoznak a szervezetbe. A munkatárs a promptba másolt ügyféladattal vagy forráskóddal egy még a legjobb esetben sem átlátható módon működő külső rendszerbe visz ki információt, a modell választ pedig építi be a munkájába (jó esetben emberi ellenőrzéssel). Az MI-ügynök ennél tovább megy, mert a felhasználó nevében eljáró folyamatként fér hozzá levelezéshez, fájlokhoz és üzleti rendszerekhez.

A NIS2 hazai szabályozása nem alkotott külön MI-fejezetet, de nem is szükséges hozzá. A Kiberbiztonsági tv. szerint a szervezet rendelkezésében lévő minden elektronikus információs rendszer a védelem tárgya, a vezető pedig köteles a használt rendszereket felmérni, a kockázatokat elemezni és a védelmi intézkedéseket bevezetni. A 7/2024. (VI. 24.) MK rendelet több, minden biztonsági osztályban kötelező követelménye kifejezetten a külső rendszerek használatára, a külső alkalmazások korlátozására, a felhasználó által telepített szoftverekre, a beszállítói szerződésekre és a biztonságtudatossági képzésre vonatkozik. Ezek együtt teljes keretet adnak az MI-használat szabályozásához.

Az AI Act a szervezetet alkalmazóként érinti. A már hatályos legfontosabb kötelezettség a munkatársak MI-jártasságának fejlesztése, 2026. augusztus 2-től pedig az átláthatósági szabályok is alkalmazandók, a nagy kockázatú rendszerekre vonatkozó kötelezettségeket az (EU) 2026/1744 rendelet 2027. december 2-ra, illetve 2028. augusztus 2-ra halasztotta.

Kis- és középvállalkozások számára a javasolt megoldás nem új rendszer, hanem a meglévő szabályzat és eszközkészlet kiegészítése. Vállalati előfizetés központi bejelentkezéssel a személyes fiókok helyett, adatosztályozásra épülő beviteli szabályok, a kimenet emberi ellenőrzése, az ügynökök saját fiókkal és a legkisebb jogosultsággal, naplózás, rövid gyakorlati képzés és dokumentált felhasználói nyilatkozat. Ezekkel a NIS2 audit és az AI Act megfelelés egyszerre igazolható.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) munkatársai általános célú MI-rendszereket használnak szövegírára, fordításra, elemzésre és programozásra, a Szervezet pedig MI-ügynökök bevezetését tervezi ügyfélszolgálati és belső adminisztratív feladatokra. A vizsgálandó kérdés az, hogy mit értünk általános célú MI-rendszerek alatt milyen információbiztonsági kockázatokat hordoz ezek vállalati használata, továbbá hogy a hazai NIS2 szabályozás és az AI Act milyen kockázatcsökkentő intézkedéseket ír elő.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

Nem tárgya az állásfoglalásnak az MI-komponenst tartalmazó hagyományos szoftver (például a gépi tanulást használó levélszemétszűrő), a saját MI-modell fejlesztésének és tanításának kockázata, az MI-ügynökök használata, az AI Act nagy kockázatú rendszerekre vonatkozó teljes megfelelési rendszere, valamint az adatvédelmi és szerzői jogi kérdések részletes elemzése. Az állásfoglalás kizárólag a Szervezet által alkalmazóként, külső szolgáltatásként igénybe vett általános célú MI rendszerekkel foglalkozik.

3. GYAKORLATI JAVASLATOK

3.1 Alapvető szabályok az általános célú MI rendszerek használatára

A jogszabályok nem írnak elő önálló MI-szabályzatot, a követelmények az információbiztonsági szabályzatba és a viselkedési szabályokba beépíthetők. Javasoljuk, hogy a Szervezet legalább a következőket rögzítse.

- Munkavégzés céljára főszabály szerint csak olyan MI-rendszer használható, amelyhez a szervezet előfizetéssel rendelkezik, vagy maga üzemelteti azt! Bizalmas információ vagy személyes adat kizárólag ilyen rendszerbe tölthető fel prompt, állomány (docx, xlsx stb.) feltöltés, API-hozzáférés vagy ügynökhözáférés esetén.
- Előfizetés esetén olyan csomagot kell választani, amely garantálja a bizalmasságot, azt, hogy a szolgáltató nem használja fel további modellek tanítására a bevitt információkat, továbbá meg kell felelni a GDPR adatfeldolgozókra és nemzetközi adattovábbításra vonatkozó előírásainak is.
- Az engedélyezett szolgáltatások, a vállalati előfizetésben és központi bejelentkezéssel használt MI-rendszerek listája, minden más szolgáltatás és a személyes fiókok munkacélú használatának tilalma.
- A bevihető adatok köre, az adatosztályozás alapján meghatározva, mely adatkategóriák adhatók meg a promptban vagy tölthetők fel, és melyek soha még üzleti előfizetéssel sem (különösen védett üzleti titok, hitelesítő adatok, jelszavak, API kulcsok, kritikus rendszerek forráskódja, stb).
- A kimenet kezelése, a válasz emberi ellenőrzése a felhasználás előtt, a generált kód biztonsági átvizsgálása, a mesterségesen előállított tartalom jelölése, ahol azt jogszabály vagy az ügyfél elvárja.
- Az MI-ügynökök szabályai, minden ügynök saját, nyilvántartott fiókkal, csak a feladatához szükséges jogosultsággal működik, a visszafordíthatatlan műveletekhez (küldés, törlés, fizetés) emberi jóváhagyás szükséges, az elérhető eszközök és adatforrások engedélyezési listán szerepelnek.
- A naplózás és az incidensek, a promptok, a válaszok és az ügynöki műveletek naplózása és megőrzése, valamint a jelentendő események (bizalmas adat bevitele, az ügynök szokatlan viselkedése, eltérített utasítás gyanúja) és a jelentés csatornája.
- A képzés és a nyilatkozat, a felhasználók MI-jártassági képzése, a szabályok megismeréséről szóló dokumentált nyilatkozat.

- A beszállítói követelmények, a bevitt adatok tanításra való felhasználásának kizárása, az adatkezelés helye, a megőrzési idő és a törlés, az incidensértesítés, valamint a független tanúsítás megléte.

3.2 Jó gyakorlatok és megoldások KKV-k számára

Egy kis- vagy középvállalkozásnak nem kell külön MI-biztonsági platformot beszereznie. A legnagyobb kockázatcsökkentést az hozza, ha a személyes fiókokat vállalati előfizetés váltja fel, amelybe a munkatársak a központi identitáskezelővel jelentkeznek be. A vállalati konstrukciók lehetővé teszik a tanításra való felhasználás kizárását, az adatmegőrzés korlátozását, az EU-n belüli adatkezelést és a naplók exportját, a személyes fiókok ezt nem garantálják. A fiók így a kilépéskor a többi jogosultsággal együtt megszűnik.

A második lépés az engedély nélküli használat láthatóvá tétele. A meglévő webszűrő vagy végpontvédelmi eszköz a legtöbb esetben képes az MI-szolgáltatások naplózására és a nem engedélyezett oldalak blokkolására, a böngésző központi kezelése pedig a nem jóváhagyott MI-bővítményeket zárja ki.

A felhasználókat rendszeres MI jártassági képzésben kell részesíteni. A képzés rendszeres, rövid és gyakorlati legyen. Elég egy – két óra, amely bemutatja, milyen adat nem vihető be, hogyan néz ki egy rejtett utasítást tartalmazó e-mail, és miért kell a modell választ ellenőrizni. Viszont érdemes 1-2 havonta, legkésőbb negyedévente, frissített tematikával megismételni. Dokumentálva ez a NIS2 és az AI Act képzési követelményeinek teljesítéséhez egyaránt hozzájárul.

3.3 A javasolt eljárás

- a) Felmérés, a ténylegesen használt MI-szolgáltatások, fiókok, bővítmények és ügynöki integrációk feltárása a naplók és a munkatársak megkérdezése alapján.
- b) Döntés és nyilvántartás, az engedélyezett MI szolgáltatások kijelölése és felvétele az elektronikus információs rendszerek nyilvántartásába, a többi szolgáltatás tiltása.
- c) Kockázatelemzés, a fenyegetéskatalógus alapján az MI-használat kockázatainak dokumentálása, a biztonsági hatásvizsgálat elvégzése a bevezetés előtt, az adatosztályozás felülvizsgálata.
- d) Szabályozás és szerződés, a szabályzat és a viselkedési szabályok kiegészítése, a felhasználói nyilatkozat megújítása, a szolgáltatói feltételek dokumentált ellenőrzése.
- e) Technikai intézkedések, központi bejelentkezés, szolgáltatói beállítások, webszűrés, ügynöki fiókok és jogosultságok, naplózás.
- f) Képzés és felügyelet, a képzés dokumentált megtartása, a naplók rendszeres áttekintése, a kockázatelemzés és a szabályok legalább évenkénti, jelentős változás esetén soron kívüli felülvizsgálata.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik, és kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el.² Az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek eltéréseit külön pont foglalja össze. A törvény a védelmet nem a szervezet tulajdonában, hanem a rendelkezésében lévő rendszerekre írja elő.

6. § (1) A szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert. [2024. évi LXIX. törvény 6. § (1) bekezdés]

Az elektronikus információs rendszer a törvény szerint minden olyan eszköz vagy egymással kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi.³ A Szervezet által előfizetett MI-szolgáltatás és az általa konfigurált ügynök ezért a Szervezet elektronikus információs rendszere akkor is, ha a modellt a szolgáltató üzemelteti. Ha a rendelkezési jog a rendszernek csak egyes elemeire terjed ki, a védelmi intézkedéseket ezekre az elemekre kell teljesíteni,⁴ az MI-szolgáltatásnál ez a Szervezet fiókjait, beállításait és adatáramlását jelenti.

4.2 A fogalmak pontosítása

4.2.1 Általános célú MI-modell és általános célú MI-rendszer

A magyar kiberbiztonsági jogszabályok az MI fogalmait nem határozzák meg, ezért az AI Act, vagyis az (EU) 2024/1689 rendelet fogalmait vesszük alapul.⁵ A rendelet megkülönbözteti a modellt és a rendszert. Az általános célú MI-modell a tanított modell maga, amely jelentős általánosságot mutat és feladatok széles körének elvégzésére képes,⁶ önmagában azonban nem MI-rendszer, ahhoz felhasználói felület és további alkotóelemek szükségesek.⁷

66. „általános célú MI-rendszer”: általános célú MI-modellen alapuló MI-rendszer, amely – mind közvetlen felhasználás, mind más MI-rendszerekbe való integráció céljából – többféle célt képes szolgálni; [(EU) 2024/1689 rendelet 3. cikk 66. pont]

A vállalati gyakorlatban ilyen a csevegőasszisztens, az irodai alkalmazásokba épített MI-segéd, a programozást támogató asszisztens és minden alkalmazás, amely nyelvi modellel szabadon

² 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

³ 2024. évi LXIX. tv. 4. § 24. pont b) alpont

⁴ 7/2024. (VI. 24.) MK rendelet 2. § (3) bekezdés

⁵ Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, 3. cikk 1. pont (MI-rendszer)

⁶ (EU) 2024/1689 rendelet 3. cikk 63. pont

⁷ (EU) 2024/1689 rendelet (97) preambulumbekkezdés

megadott feladatokat old meg. A Szervezet ezekben a viszonyokban alkalmazó, mert a felügyelete alá tartozó MI-rendszert szakmai tevékenysége során használja.⁸

4.2.2 MI-ügynök

Az MI-ügynök fogalmát sem az AI Act, sem a magyar jog nem határozza meg. Az Európai Bizottság tájékoztatása szerint az MI-ügynök nem külön kategória, hanem jellemzően általános célú MI-modellre épülő MI-rendszer, amely a környezetéből bemenetet fogad, azt feldolgozza, és ennek alapján a környezetére ható műveleteket hajt végre. Az ügynököt négy jellemző különbözteti meg a csevegőasszisztentstől, az eszközhasználat (levelezés, fájlrendszer, böngésző, üzleti alkalmazás), a többlépéses önálló tervezés, a memória és a más ügynökökkel folytatott kommunikáció. Információbiztonsági szempontból az ügynök a felhasználó nevében eljáró folyamat, amelyre a hozzáférés-ellenőrzés szabályai ugyanúgy vonatkoznak, mint a felhasználóra. Az MI ügynökök biztonságával külön állásfoglalásban foglalkozunk.

4.2.3 Elhatárolás, mi az, ami nem tárgya a vizsgálatnak

Az MI-komponenst tartalmazó hagyományos szoftver, amelynél a modell rögzített feladatot lát el, és a felhasználó nem ad neki szabad utasítást, a szoftverbeszerzés szokásos szabályai alá tartozik. Az elhatárolás másik iránya a Szervezet szerepe. Ha a Szervezet egy általános célú MI-rendszer rendeltetését úgy módosítja, hogy az nagy kockázatú MI-rendszerré válik, szolgáltatónak minősül, és a szolgáltatói kötelezettségek terhelik.⁹

4.3 Az információbiztonsági kockázatok

A rendelet előírja, hogy a Szervezet a kockázatelemzés során a 3. melléklet fenyegetéskatalógusának elemeit vizsgálja.¹⁰ Az alábbi kockázatok mindegyike a katalógus valamely tételére vezethető vissza, az MI-használat tehát nem új módszertant, hanem új rendszert és új adatáramlást jelent.

4.3.1 Bizalmasság, az adatok kikerülése a promptokon keresztül

A leggyakoribb kockázat a védett információ nyilvánosságra kerülése (a katalógus 20. tétele) azáltal, hogy a munkatárs a promptba vagy a feltöltött fájlba bizalmas adatot ír. Személyes fiókban az adat a szolgáltató feltételei szerint tanításra is felhasználható, megőrzési ideje ismeretlen, a Szervezet pedig sem törlést, sem naplót nem tud kérni. A Netskope 2026. évi jelentése szerint a munkahelyi generatív MI-használók 47 százaléka személyes fiókot használ.¹¹ Az IBM 2025. évi jelentése szerint az MI-t érintő incidenst jelentő szervezetek 97 százalékánál hiányzott az MI-hozzáférés ellenőrzése, a szervezetek ötöde pedig engedély nélküli, úgynevezett árnyék-MI használatra visszavezethető incidensről számolt be.¹²

4.3.2 Sértetlenség, a kimenet és az utasítás megbízhatatlansága

⁸ (EU) 2024/1689 rendelet 3. cikk 4. pont

⁹ Európai Bizottság, AI Act Service Desk, „How are AI agents addressed within the AI Act?” (ai-act-service-desk.ec.europa.eu)

¹⁰ Hasonló leírást ad a CISA és partnerügynökségei közös útmutatója, Careful Adoption of Agentic AI Services, 2026. április 30. (cisa.gov)

¹¹ (EU) 2024/1689 rendelet 25. cikk (1) bekezdés c) pont

¹² 7/2024. (VI. 24.) MK rendelet 2. § (4) bekezdés és 3. melléklet

A nyelvi modell hihető, de téves állítást, nem létező hivatkozást vagy sérülékeny kódot is előállíthat. Ez a nem megbízható forrásból származó információ (21. tétel) és az információmanipuláció (23. tétel) kockázata, a generált kód ellenőrzés nélküli használata pedig a szoftverek sérülékenységei (29. tétel) körébe tartozik. Az MI-specifikus sértetlenségi kockázat a prompt injection, amikor a modellnek átadott tartalom (e-mail, weboldal, dokumentum) rejtett utasítást tartalmaz, amelyet a modell a felhasználó utasításával azonos súllyal hajt végre. A brit NCSC 2025. decemberi elemzése szerint a nyelvi modellben nincs az adatot és az utasítást elválasztó mechanizmus, ezért a prompt injection valószínűleg soha nem küszöbölhető ki teljesen, a védelmet a modellen kívüli, determinisztikus korlátoknak és a legkisebb jogosultságnak kell adnia.¹³ Az ENISA 2026. évi fenyegetettségi jelentése a közvetett prompt injectiont a modellek korlátainak megkerülésére használt módszerek között említi,¹⁴ az OWASP 2025. évi listája pedig az első helyen szerepelteti.¹⁵

4.3.3 Rendelkezésre állás és ellátási lánc

Az MI-szolgáltatás a külső szolgáltató zavara (12. tétel) esetén kiesik, a modell verzióját a szolgáltató a Szervezet beleegyezése nélkül cseréli, a bővítmények és az ügynöki eszközkapcsolatok pedig új elemei a beszállítói láncnak (11. tétel). Ha egy üzleti folyamat az MI-szolgáltatásra épül, a kiesésével az üzletmenet-folytonossági tervben számolni kell.

4.3.4 Az MI-ügynökök sajátos kockázatai

Az ügynöknél a fenti kockázatok cselekvéssé válnak. Az eltérített ügynök nemcsak téves választ ad, hanem levelet küld, fájlt töröl vagy tranzakciót indít, ez az engedélyekkel való visszaélés (33. tétel) és a rendszer engedély nélküli használata (31. tétel). Az OWASP 2026. évi ügynöki listája a cél eltérítését, az eszközökkel való visszaélést, a jogosultság kihasználását, a memória mérgezését és a hibák láncolódását sorolja a fő fenyegetések közé.¹⁶ Az ENISA szerint az MI-alkalmazások és környezetük egyre gyakrabban válnak célponttá, különösen ott, ahol fájlokhoz, hitelesítő adatokhoz, böngésző-munkamenetekhez vagy fejlesztői környezetekhez férnek hozzá.¹⁷

4.3.5 Az emberi tényező

Az automatizálási torzítás, vagyis a modell válaszában kritikátlan elfogadása nem informatikai hiba, mégis a legtöbb kárt okozó tényező. A támadók emellett az MI-t a pszichológiai manipuláció (43. tétel) eszközeként is használják, ezért a képzés a védelem része.

4.4 NIS2 előírások a kockázatok kezelésére

4.4.1 A törvényi keret

A Kiberbiztonsági tv. a szervezet vezetőjének feladatává teszi a használt rendszerek felmérését és nyilvántartását, a kockázatmenedzsmentet, a védelmi intézkedések meghatározását, az

¹³ Netskope, Cloud and Threat Report 2026, 2026. január (netskope.com)

¹⁴ IBM, Cost of a Data Breach Report 2025, 2025. július 30. (newsroom.ibm.com)

¹⁵ NCSC (UK), „Prompt injection is not SQL injection (it may be worse)“, 2025. december 8. (ncsc.gov.uk)

¹⁶ ENISA Threat Landscape 2026, 2026. szeptember 22., 15. o.

¹⁷ OWASP Top 10 for LLM Applications 2025, LLM01 Prompt Injection (genai.owasp.org)

információbiztonsági szabályzat kiadását és a használatbavételről szóló döntést.¹⁸ A vezető gondoskodik a munkatársak kiberbiztonsági képzéséről, közreműködő igénybevétele esetén a követelmények szerződéses érvényesítéséről, valamint a kiberbiztonsági incidensek kezeléséről és bejelentéséről.¹⁹ Az MI-szolgáltatás bevezetése tehát felmérési, kockázatelemzési, szabályozási, szerződéses és képzési kötelezettséget vált ki, a bizalmas adat kikerülése pedig kiberbiztonsági incidens.²⁰ Az adatosztályozás a d) pont szerinti szervezetnél is kötelező, és ez adja meg, milyen adat vihető be külső MI-rendszerbe.²¹

4.4.2 A rendelet védelmi intézkedései

A 7/2024. (VI. 24.) MK rendelet 2. melléklete nem tartalmaz MI-re vonatkozó követelményt, az általános követelmények azonban közvetlenül alkalmazhatók. A külső rendszerek használatára vonatkozó, minden osztályban kötelező követelmény pontosan azt írja le, amit egy külső MI-szolgáltatás jelent.

2.115. A szervezet:

2.115.1. Meghatározza a felhasználási feltételeket, és megállapítja, hogy az elvárt követelmények megvalósultak-e a külső rendszerekben, összhangban a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel létrehozott bizalmi kapcsolatokkal, amelyek lehetővé teszik az arra jogosult személyek számára, hogy:
[...]

2.115.1.2. feldolgozzák, tárolják vagy továbbítják a szervezet által ellenőrzött információkat külső rendszerek használatával; vagy

2.115.2. megtiltja a meghatározott típusú külső rendszerek használatát.
[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.115. pont] (A, J, M)

A Szervezetnek tehát vagy meg kell határoznia, mely MI-szolgáltatások használhatók és milyen feltételekkel, vagy meg kell tiltania a használatukat, a hallgatás nem felel meg a követelménynek. Minden biztonsági osztályban a külső rendszer csak akkor engedélyezhető, ha a Szervezet ellenőrizte a rajta alkalmazott védelmi intézkedéseket, vagy jóváhagyott feldolgozási megállapodást tart be a szolgáltatóval. A viselkedési szabályokba a rendelet külön korlátozásokat ír elő.

13.4. A szervezet a viselkedési szabályaiba a következő korlátozásokat építi be:

13.4.1. a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozása;

13.4.2. a szervezeti információk közzétételének korlátozása nyilvános weboldalakon; és

¹⁸ OWASP Top 10 for Agentic Applications 2026, ASI01 Agent Goal Hijack, ASI02 Tool Misuse, ASI03 Identity and Privilege Abuse, ASI06 Memory and Context Poisoning, ASI08 Cascading Failures (genai.owasp.org)

¹⁹ ENISA Threat Landscape 2026, 17. o.

²⁰ 2024. évi LXIX. tv. 6. § (3) bekezdés 1., 4., 6., 7. és 12. pont

²¹ 2024. évi LXIX. tv. 6. § (5) bekezdés a), d) és e) pont

13.4.3. a szervezet által biztosított azonosító és hitelesítő adatok használatának korlátozása külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor. [7/2024. (VI. 24.) MK rendelet 2. melléklet 13.4. pont] (A, J, M)

A viselkedési szabályokat a felhasználók dokumentált nyilatkozattal fogadják el, frissítéskor újra.²² Ez az a dokumentum, amelyben az MI-használati szabályok a legtermészetesebben elhelyezhetők.

A szolgáltatóval szemben a rendelet szerződéses követelményeket vár el, a teljesítést pedig a Szervezetnek ellenőriznie kell.

16.49. A szervezet:

16.49.1. Szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.

[...]

16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont] (A, J, M)

A nagy MI-szolgáltatókkal egyedi szerződés ritkán köthető, a követelmény ilyenkor az elfogadott feltételek, az adatfeldolgozási megállapodás és a szolgáltató tanúsítványainak dokumentált ellenőrzésével teljesíthető. Ide kapcsolódik az ellátási lánc kockázatelemzése, az ellátási lánc folyamatai, az alvállalkozók továbbkötelezése és az értesítési megállapodások,²³ jelentős és magas osztályban a beszállítók rendszeres értékelése is.²⁴

Az engedély nélküli MI-használat, vagyis az árnyék-MI ellen a konfigurációkezelés követelményei adnak alapot. A felhasználó által telepített szoftverre vonatkozó, minden osztályban kötelező szabály szerint a Szervezet meghatározza a felhasználói telepítés lehetőségeit, érvényesíti a szabályokat és ellenőrzi a betartásukat.²⁵ Ez a böngészőbővítményekre és az ügynöki eszközkapcsolatokra is kiterjed. A legszűkebb funkcionalitás elve alapján a Szervezet meghatározza a tiltott vagy korlátozott szoftvereket és szolgáltatásokat, jelentős és magas osztályban alapértelmezett tiltással és kivétel alapú engedélyezéssel.²⁶ Az új MI-szolgáltatás bevezetése változás, amelynek biztonsági hatását előre meg kell vizsgálni, és amely a nyilvántartás frissítését igényli.²⁷

Az MI-ügynökökre a hozzáférés-ellenőrzés követelményei vonatkoznak. A fiókkezelés minden osztályban megköveteli az engedélyezett fióktípusok meghatározását, a fiókok jóváhagyását,

²² 2024. évi LXIX. tv. 4. § 46. pont

²³ 2024. évi LXIX. tv. 9. § (1) bekezdés

²⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.116. pont (J, M)

²⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3. pont (A, J, M)

²⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.5. pont (A, J, M), 19.4. pont (A, J, M), 19.7. pont (A, J, M) és 19.19. pont (A, J, M)

²⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.16. pont (J, M)

nyomon követését és a jogviszony megszűnésével összehangolt megszüntetését.²⁸ Jelentős és magas osztályban a legkisebb jogosultság elve az ügynökre szó szerint illik.

2.60. A szervezet a legkisebb jogosultság elvét alkalmazza, és a felhasználók vagy a felhasználók nevében eljáró folyamatok számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi. [7/2024. (VI. 24.) MK rendelet 2. melléklet 2.60. pont] (J, M)

Ugyanezen osztályokban a privilegizált fiókok korlátozása, a jogosultságok rendszeres felülvizsgálata, a privilegizált funkciók naplózása és a felelőségek szétválasztása is kötelező.²⁹ Az ügynök API-kulcsa hitelesítő eszköz, amelyre a hitelesítő eszközök kezelésének szabályai vonatkoznak.³⁰

A prompt injection elleni védelem szempontjából a bemeneti információ ellenőrzése jelentős és magas osztályban kötelező,³¹ az adatok injektálásának megakadályozása pedig opcionális követelmény, amely nyelvi modelleknél a modellen kívüli, determinisztikus szűrőket jelenti.³² A kamerára és a mikrofonra vonatkozó, minden osztályban kötelező szabály az MI-alapú értekezlet-jegyzetelők távoli aktiválására is kiterjed.³³

A naplózás körében a Szervezet meghatározza a naplózandó eseményeket, a naplókat felülvizsgálja és megőrzi, a rendszert pedig a jogosulatlan használat felismerése érdekében monitorozza.³⁴ Az MI-szolgáltatásnál ez a szolgáltatói naplók exportját és az ügynöki műveletek naplózását jelenti, jelentős és magas osztályban a kimenő forgalom ellenőrzését is.³⁵

A biztonságtudatossági képzés minden osztályban kötelező, a tananyagot a rendszerben bekövetkezett változás esetén frissíteni kell, a képzés a vezetőkre és a szerződéses partnerekre is kiterjed, és dokumentálni kell.³⁶ Jelentős és magas osztályban a pszichológiai manipuláció felismerésére külön képzés szükséges, amelybe az MI-vel előállított megtévesztő tartalmak is beletartoznak.³⁷

4.5 AI Act előírások a kockázatok kezelésére

4.5.1 Hatály és időbeli alkalmazás

²⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.49. pont (A, J, M)

²⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.26. pont (A, J, M) és 6.31. pont (J, M)

³⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.15. pont (A, J, M) és 1.5. pont (A, J, M)

³¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.2. pont (A, J, M)

³² 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.65. pont (J, M), 2.67. pont (J, M), 2.69. pont (J, M) és 2.59. pont (J, M)

³³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 8.21. pont (A, J, M)

³⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.59. pont (J, M)

³⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.65. pont (O)

³⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 17.54. pont (A, J, M)

³⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 4.2. pont (A, J, M), 4.13. pont (A, J, M), 4.38. pont (A, J, M) és 18.13. pont (A, J, M)

Az AI Act az Unióban letelepedett alkalmazókra alkalmazandó.³⁸ Az (EU) 2026/1744 rendelettel 2026. július 27-től módosított 113. cikk szerint a rendelet 2026. augusztus 2-től alkalmazandó, az általános célú MI-modellekre vonatkozó V. fejezet 2025. augusztus 2-től, a nagy kockázatú rendszerekre vonatkozó követelmények pedig a III. melléklet szerinti rendszerekre 2027. december 2-től, az I. melléklet szerinti rendszerekre 2028. augusztus 2-től.³⁹ Magyarországon a végrehajtásról a 2025. évi LXXV. törvény rendelkezik, a piacfelügyeleti hatóság a 344/2025. (X. 31.) Korm. rendelet szerint a vállalkozásfejlesztésért felelős miniszter, a feladatot 2026 szeptemberétől a Tudományos és Technológiai Minisztériumban működő MI Piacfelügyeleti Hatóság látja el.⁴⁰

4.5.2 MI-jártasság

Az alkalmazó legfontosabb, minden MI-rendszerre kiterjedő kötelezettsége a módosított 4. cikkben szerepel.

(1) Az MI-rendszerek szolgáltatói és alkalmazói intézkedéseket hoznak annak érdekében, hogy támogassák személyzetük, valamint a nevükben az MI-rendszerek működtetésével és használatával foglalkozó bármely más személyek MI-jártasságának fejlesztését, figyelembe véve szakmai ismereteiket, tapasztalatukat, végzettségüket és képzettségüket, valamint azon körülményeket, amelyek között az MI-rendszereket használni fogják, és figyelembe véve azon személyeket, vagy azon személyek csoportjait, akik tekintetében az MI-rendszereket használni fogják. Ez a kötelezettség nem írja elő a szolgáltatók vagy az alkalmazók számára, hogy bármely személy számára garantálják az MI-jártasság bármely konkrét szintjét.
[(EU) 2024/1689 rendelet 4. cikk (1) bekezdés]

Az MI-jártasság a rendelet fogalma szerint a kockázatok és a lehetséges károk ismeretét is magában foglalja,⁴¹ ezért a biztonsági kockázatokat bemutató képzés a kötelezettség része. A NIS2 biztonságtudatossági képzése és az MI-jártassági képzés egy tananyagban összevonható, a dokumentálás mindkét igazolási igényt kielégíti.

4.5.3 A szolgáltató kötelezettségei, amelyekre az alkalmazó támaszkodhat

Az általános célú MI-modell szolgáltatója dokumentációt készít és bocsát rendelkezésre a modell képességeiről és korlátairól,⁴² a rendszerszintű kockázatot jelentő modell szolgáltatója pedig támadó szempontú tesztelést végez, és megfelelő szintű kiberbiztonsági védelmet biztosít a modell és fizikai infrastruktúrája számára.⁴³ Az alkalmazó ezeket a beszállítói átvilágítás során

³⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.17. pont (J, M)

³⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 3.2. pont (A, J, M) és 3.13. pont (A, J, M)

⁴⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 3.5. pont (J, M)

⁴¹ (EU) 2024/1689 rendelet 2. cikk (1) bekezdés b) pont

⁴² (EU) 2024/1689 rendelet 113. cikk, az (EU) 2026/1744 rendelettel megállapított szöveg

⁴³ 2025. évi LXXV. törvény 3. § (1) bekezdés; 344/2025. (X. 31.) Korm. rendelet 1. § (1) bekezdés b) pont; MI Piacfelügyeleti Hatóság (mihivatal.gov.hu)

hasznosíthatja, a közzétett modelldokumentáció és az általános célú MI gyakorlati kódex biztonsági fejezetének aláírása a 16.49. pont szerinti ellenőrzés bizonyítéka lehet.⁴⁴

4.5.4 Átláthatóság

2026. augusztus 2-től a természetes személyekkel közvetlenül érintkező MI-rendszereknél a szolgáltatónak biztosítania kell, hogy az érintett tudja, MI-rendszerrel áll kapcsolatban, a szintetikus tartalmat előállító rendszerek kimenetét pedig géppel olvasható módon jelölni kell.⁴⁵ Az alkalmazó a valósnak tűnő kép-, hang- vagy videotartalom mesterséges eredetét közli, a közérdekű ügyekről tájékoztató, MI-vel előállított szöveget pedig emberi felülvizsgálat és szerkesztői felelősség hiányában jelöli.⁴⁶ Az Európai Bizottság tájékoztatása szerint az átláthatósági szabályok az MI-ügynökökre is vonatkoznak, ügyfélszolgálati ügynök bevezetésekor ezért az ügyfél tájékoztatásáról gondoskodni kell.⁴⁷

4.5.5 Ha az MI-rendszer nagy kockázatú

Ha a Szervezet az általános célú MI-rendszert a III. melléklet szerinti területen, például a munkavállalók értékelésére használja, az alkalmazói kötelezettségek 2027. december 2-től terhelik. Az alkalmazó a rendszert a használati utasítás szerint használja, az emberi felügyeletet megfelelő szakértelemmel és hatáskörrel rendelkező személyre bízva, a működést nyomon követi, a súlyos incidenst jelenti, a naplót pedig legalább hat hónapig megőrzi.⁴⁸ A rendelet a nagy kockázatú rendszerek kiberbiztonsági követelményei között nevesíti az adatmérgezést, a modellszennyezést és a modell kizárását,⁴⁹ ami az alkalmazói kockázatelemzéshez is kiindulópont.

4.6 A közszférába tartozó szervezetek

A Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetekre a fentiek három eltéréssel irányadók. Ezek a szervezetek nem privát felhőszolgáltatást, így nyilvános MI-szolgáltatást kizárólag az adatosztályozás alapján vehetnek igénybe. A döntés előtt az a) pont szerinti közigazgatási szervezet költség-haszon elemzést és kilépési tervet, a többi szervezet legalább kilépési tervet készít.⁵⁰

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv); az (EU) 2024/1689 rendelet (AI Act), az (EU) 2026/1744 rendelettel módosított, 2026. július 27-től hatályos szöveg
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

⁴⁴ (EU) 2024/1689 rendelet 3. cikk 56. pont

⁴⁵ (EU) 2024/1689 rendelet 53. cikk (1) bekezdés b) pont

⁴⁶ (EU) 2024/1689 rendelet 55. cikk (1) bekezdés a) és d) pont

⁴⁷ Európai Bizottság, General-Purpose AI Code of Practice, Safety and Security Chapter, 2025. július 10.

⁴⁸ (EU) 2024/1689 rendelet 50. cikk (1) és (2) bekezdés

⁴⁹ (EU) 2024/1689 rendelet 50. cikk (4) bekezdés

⁵⁰ Európai Bizottság, AI Act Service Desk, „How are AI agents addressed within the AI Act?” (ai-act-service-desk.ec.europa.eu)

- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról; 2025. évi LXXV. törvény az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról; 344/2025. (X. 31.) Korm. rendelet
- Európai Bizottság, AI Act Service Desk, How are AI agents addressed within the AI Act; General-Purpose AI Code of Practice (2025)
- ENISA Threat Landscape 2026 (2026. szeptember 22.); CISA, NSA, ASD ACSC, CCCS, NCSC-NZ, NCSC-UK, Careful Adoption of Agentic AI Services (2026. április 30.); NCSC (UK), Prompt injection is not SQL injection (it may be worse) (2025. december 8.)
- OWASP Top 10 for LLM Applications 2025; OWASP Top 10 for Agentic Applications 2026; IBM Cost of a Data Breach Report 2025; Netskope Cloud and Threat Report 2026

6. KAPCSOLÓDÓ ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- ENISA (Európai Unió Kiberbiztonsági Ügynökség): Multilayer Framework for Good Cybersecurity Practices for AI – Iránymutatás a mesterséges intelligencia rendszerek kiberbiztonságának biztosítására, a kiberfenyegetések (pl. adatmérgezés, prompt injection) elleni védekezésre.
- EDPB (Európai Adatvédelmi Testület): ChatGPT Task Force jelentések és iránymutatások a generatív mesterséges intelligencia (LLM) és a GDPR megfelelés kapcsolatáról, különös tekintettel az adatbiztonságra és a célhoz kötöttségre.
- NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság): Állásfoglalások és ajánlások a mesterséges intelligencia és a nyelvi modellek munkahelyi alkalmazásának adatvédelmi és adatbiztonsági követelményeiről.
- CISA – NCSC: Guidelines for secure AI system development – Iránymutatás az MI-rendszerek biztonságos telepítéséhez és üzemeltetéséhez az ellátási lánc kockázatainak csökkentése érdekében.
- EU MI Hivatal (AI Office): Gyakorlati kódexek (Code of Practice) és értelmező iránymutatások az AI Act alkalmazásához, különösen az általános célú MI-modellek szolgáltatói és alkalmazói kötelezettségeihez.