

A Shadow AI jelentette kockázatok és intézkedések a csökkentésükre NIS2 és AI Act előírások a kockázatok kezelésére

VFP3 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/53

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.23	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A shadow AI a munkatársak által a szervezet tudta, jóváhagyása és felügyelete nélkül használt mesterséges intelligencia. Mögötte ritkán áll rossz szándék, a munkatárs egyszerűen gyorsabban akar dolgozni, ezért bemásol egy szerződéstervezetet egy ingyenes chatbotba. Egy 2025 végi hazai felmérés szerint a munkájukban MI-t használók 65 százaléka saját kezdeményezésre teszi ezt, és csak 11 százalékuk használ munkáltató által biztosított eszközt.

A legnagyobb kockázat, hogy az adat olyan szolgáltatóhoz kerül, amellyel a Szervezetnek nincs szerződése, és amely a bevitt tartalmat modellje fejlesztésére is felhasználhatja. A kimenet ellenőrzés nélkül jut el döntésekbe és programkódba, a böngészőbővítmények és a saját telepítésű MI-ügynökök pedig a munkatárs jogosultságaival érik el a vállalati rendszereket.

A NIS2 hazai szabályozása nem használja a shadow AI kifejezést, követelményei mégis erre a helyzetre is választ adnak. A Kiberbiztonsági törvény szerint a vezetőnek gondoskodnia kell a szervezet által használt rendszerek felméréséről és nyilvántartásba vételéről, a 7/2024. (VI. 24.) MK rendelet pedig minden biztonsági osztályban előírja, hogy a viselkedési szabályok korlátozzák a külső alkalmazások használatát és a céges azonosítóval történő regisztrációt. Az AI Act alapján a Szervezet alkalmazóként felelhet a munkavégzés során használt MI-eszközökért, a munkahelyi érzelemfelismerés tiltott, a pályázók chatbottal történő rangsorolása pedig szolgáltatói kötelezettségekkel járhat.

A javasolt megközelítés a kiváltás, nem a pusztán tiltás, amely a használatot a még kevésbé látható magán-eszközökre szorítja ki. A Szervezet adjon szerződéssel lefedett MI-eszközt és világos szabályt a bevihető adatokról, tegye láthatóvá a tényleges használatot, és ehhez igazítsa a technikai korlátozásokat.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) munkatársai olyan MI-alapú eszközöket is használnak, amelyeket a Szervezet nem hagyott jóvá, és amelyekről gyakran nem is tud. A vizsgálandó kérdés az, hogy mit jelent a shadow IT és a shadow AI, mennyire elterjedt a jelenség, milyen kockázatokat hordoz, és milyen adminisztratív és technikai eszközökkel védekezhet ellene a Szervezet. Vizsgáljuk továbbá, hogy a hazai NIS2 szabályozás, különösen a 7/2024. (VI. 24.) MK rendelet, valamint az AI Act milyen előírásokat tartalmaz a kockázatok kezelésére.

Az állásfoglalás a jóváhagyott MI-használattal foglalkozó 2026/45. számú (általános célú MI-rendszerek) és 2026/48. számú (MI-célszoftverek) állásfoglalást egészíti ki, ezért nem tárgya a jóváhagyott eszközök bevezetésének elemzése. Az adatvédelmi és munkajogi kérdéseket csak annyiban érintjük, amennyiben a védekezés szempontjából meghatározók.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2 irányelv)

3. GYAKORLATI JAVASLATOK

3.1 Adminisztratív eszközök

A védekezés nem technikai kérdéssel kezdődik. A munkatárs azért használ nem jóváhagyott eszközt, mert segítség kell a munkájához, a Szervezet pedig nem kínál jobbat, vagy a jóváhagyás túl lassú. A brit Nemzeti Kiberbiztonsági Központ (NCSC) is azt javasolja, hogy a szervezet előbb ezeket az igényeket értse meg.² Javasoljuk, hogy a Szervezet legalább a következőket rögzítse.

- MI-használati szabályzat a viselkedési szabályok részeként, amely az eszközöket engedélyezett, feltételekkel engedélyezett és tiltott kategóriába sorolja, adatosztályonként meghatározza a bevihető adatokat, és szabályozza a céges e-mail-címmel történő regisztrációt. Megismeréséről a munkatárs nyilatkozatot tesz.
- MI-nyilvántartás a rendszernyilvántartás részeként, eszközönként a szolgáltató, a felhasználási cél, a bevihető adatok, az adatkezelés helye és a felelős megjelölésével.
- Gyors jóváhagyási eljárás a szolgáltatói feltételek és az adatkezelési hely ellenőrzésével, szükség esetén adatvédelmi hatásvizsgálattal, mert a hetekig tartó engedélyezés a titkos használatot erősíti.
- Jóváhagyott alternatíva, vagyis olyan vállalati MI-szolgáltatás, amelynek feltételei kizárják a bevitt adatok tanításra való felhasználását, céges fiókkal érhető el, és naplót ad a Szervezetnek. Ilyen eszköz nélkül a tiltás nem működik.
- Eszközspezifikus MI-jártassági képzés a vezetőknek is, konkrét példákkal arról, mi történik a bevitt adattal, miben téved a modell, és kinek kell szólni téves adatbevitel esetén.
- Átmeneti amnesztia, amelynek keretében a munkatársak szankció nélkül jelezhetik az eddig használt eszközöket.

3.2 Technikai eszközök

A technikai eszközök első célja a láthatóság, mert amiről a Szervezet nem tud, azt sem jóváhagyni, sem kiváltani nem tudja.

- Felderítés a proxy-, DNS- és tűzfalnaplók, a felhőhozzáférés-biztonsági (CASB, SSE) megoldások, a végponti szoftverleltár és az egyszeri bejelentkezés naplóinak elemzésével, amely kimutatja a használt MI-szolgáltatásokat, bővítményeket és OAuth-hozzáféréseket.
- Hozzáférés-irányítás a webes átjárón, a jóváhagyott szolgáltatások engedélyezésével, a többi letiltásával vagy a jóváhagyott eszközre terelő figyelmeztetéssel, valamint a vállalati munkaterületre korlátozással (tenant restriction), hogy magánfiókkal ne lehessen belépni.
- Adatszivárgás-megelőzés (DLP) a böngészőben és a végponton, amely a beillesztett szöveget és a feltöltött fájlt vizsgálva a minősített adatot nem engedi a nem jóváhagyott szolgáltatás felé. Hatékonysága az adatosztályozás minőségén múlik.
- Végponti és böngészőkontroll, az alkalmazások engedélyezőlistája, a helyi rendszergazdai jog megvonása, a bővítmények központi engedélyezése és a saját telepítésű MI-ügynökök tiltása.

² NCSC (UK), Shadow IT, 2023. július 27., felülvizsgálva 2026. augusztus 14. (ncsc.gov.uk)

- MI-átjáró a fejlesztőknek és az integrációknak, amely központilag kezeli az API-kulcsokat, naplózza a lekérdezéseket és kiszűri a személyes adatot.
- Naplózás és riasztás a biztonsági eseménykezelő (SIEM) rendszerben a tömeges feltöltésre és az új MI-szolgáltatás megjelenésére.

Ezek az eszközök a munkavállalók ellenőrzésére is alkalmasak, ezért alkalmazásukról a munkavállalót előzetesen írásban tájékoztatni kell,³ a promptok tartalmának vizsgálata előtt pedig érdekmérlegelést, indokolt esetben adatvédelmi hatásvizsgálatot kell végezni.⁴ A 7/2024. (VI. 24.) MK rendelet maga is előírja, hogy a Szervezet jogi állásfoglalást kérjen a rendszerfelügyeleti tevékenységekről.⁵

3.3 Jó gyakorlatok és megoldások KKV-k számára

Egy kis- vagy középvállalkozásnak nincs szüksége drága platformra. A leghatékonyabb lépés egy vállalati előfizetés egy ismert MI-szolgáltatásra, amelynek feltételei kizárják a tanítási célú felhasználást, és amelyet mindenki céges fiókkal ér el. Mellé elég egy egyoldalas szabály arról, hogy ügyféladat, személyes adat és szerződés csak ebbe az eszközbe vihető be.

A második lépés a meglévő eszközök beállítása. A külső alkalmazásoknak adható hozzáférést rendszergazdai jóváhagyáshoz kell kötni, a böngészőben csak engedélyezett bővítmények futhatnak, és a munkatárs ne telepíthessen szoftvert. A harmadik egy félévente ismételt, szankció nélküli kérdőív a használt MI-eszközökről, ez a legolcsóbb felderítés.

3.4 A javasolt eljárás

- a) Felmérés, a naplók, az OAuth-hozzáférések és egy munkatársi kérdőív alapján a ténylegesen használt MI-eszközök feltérképezése és felvétele a rendszernyilvántartásba.
- b) Kockázatelemzés és döntés, eszközönként a kezelt adatok, a szolgáltatói feltételek és a felhasználási cél értékelése, majd a vezető döntése az engedélyezésről, a kiváltásról vagy a tiltásról.
- c) Szabályozás és kiváltás, az MI-használati szabályzat kiadása, a jóváhagyott eszköz bevezetése, a munkatársak nyilatkozata és az átmeneti amnesztia.
- d) Technikai kontrollok, a folyamatos felderítés, a nem jóváhagyott szolgáltatások korlátozása és az adatszivárgás-megelőzés bevezetése a munkavállalók előzetes tájékoztatása mellett.
- e) Felülvizsgálat, a nyilvántartás, a szabályzat és a kockázatelemzés legalább évenkénti, új eszköztípus megjelenésekor soron kívüli frissítése.

³ 2012. évi I. törvény (Mt.) 11/A. § (1) bekezdés

⁴ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) 6. cikk (1) bekezdés f) pont és 35. cikk (1) bekezdés

⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.13.6. pont (A, J, M)

4. VÁLASZ ÉS INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

A Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik. A shadow AI megítéléséhez három kiindulópontot rögzítünk.

Az első, hogy a nem jóváhagyott MI-szolgáltatás nem a Szervezet elektronikus információs rendszere, mert nincs a rendelkezésében.⁶ A Szervezet rendelkezésében vannak viszont azok a végpontok, fiókok, hálózati kapcsolatok és adatok, amelyekkel a szolgáltatást használják, így a követelmények ezeken keresztül érik el a shadow AI-t.

A második, hogy a vezető gondoskodik a szervezet által használt elektronikus információs rendszerek felméréséről és nyilvántartásba vételéről, és ő dönt a használatbavételükről.⁷ Álláspontunk szerint a felmérésnek a munkavégzéshez ténylegesen használt külső MI-szolgáltatásokat is ki kell mutatnia.

A harmadik, hogy a kockázatelemzésben a 3. melléklet fenyegetéskatalógusát kell alkalmazni,⁸ amelynek 31. tétele, az eszközök vagy az elektronikus információs rendszer engedély nélküli kezelése vagy használata, maga a shadow IT és a shadow AI.

4.2 A fogalmak pontosítása

4.2.1 A shadow IT

A shadow IT (árnyékinformatika) a szervezetben üzleti célra használt, de a szervezet számára ismeretlen eszközök és szolgáltatások összessége.⁹ Tipikus példája a magán felhőtárhely, a munkahelyi egyeztetésre használt magán üzenetküldő vagy a céges kártyával előfizetett szoftverszolgáltatás. Az okok között a brit NCSC a jóváhagyott eszközök hiányzó funkcióit, a lassú kérelmezést és a kockázat ismeretének hiányát említi. Amiről a szervezet nem tud, azt nem tudja védeni, naplózni és kivizsgálni.

4.2.2 A shadow AI

A shadow AI a shadow IT leggyorsabban terjedő formája, az IBM meghatározása szerint bármely MI-eszköz vagy -alkalmazás használata a munkatársak részéről az informatikai terület hivatalos jóváhagyása vagy felügyelete nélkül.¹⁰ Ide tartozik a magánfiókkal használt nyilvános chatbot, a jóváhagyott szoftverbe épített, de nem értékelt MI-funkció (például egy videokonferencia jegyzetelője), a levelezéshez kapcsolódó böngészőbővítmény és OAuth-integráció, valamint a munkatárs által telepített, a nevében önállóan cselekvő MI-ügynök.

A shadow AI három ponton különbözik a hagyományos shadow IT-től. A felhőtárhely csak tárolja az adatot, az MI-szolgáltatás feldolgozza, és akár a modell fejlesztésére is felhasználhatja. Telepítést sem igényel, ezért a szoftverleltár nem mutatja ki. Végül a kimenet visszaáramlik szerződésbe, ügyféllevélbe vagy programkódba, így a bizalmasság mellett a sértetlenséget is veszélyezteti.

⁶ 2024. évi LXIX. tv. 6. § (1) bekezdés

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

⁸ 7/2024. (VI. 24.) MK rendelet 2. § (4) bekezdés és 3. melléklet

⁹ NCSC (UK), Shadow IT (ncsc.gov.uk)

¹⁰ IBM, What is shadow AI?, 2024. október 25. (ibm.com)

4.3 A shadow AI elterjedtsége

A nemzetközi felmérések szerint a munkahelyi MI-használat jelentős része a szervezetek látókörén kívül zajlik. A KPMG és a Melbourne-i Egyetem 47 országra kiterjedő 2025-ös kutatásában a munkavállalók 57 százaléka mondta, hogy eltitkolja az MI használatát, és az MI által készített munkát a sajátjaként mutatja be. Csaknem felük a munkahelyi szabályokkal ellentétesen is használta az MI-t, például érzékeny céges információt töltött fel nyilvános MI-eszközbe.¹¹

A Gartner 2025-ös felmérésében a szervezetek 69 százaléka gyanította vagy tudta, hogy munkatársai tiltott nyilvános generatív MI-eszközt használnak, és az elemzőcég szerint 2030-ra a vállalatok több mint 40 százaléknál következik be shadow AI-hoz köthető biztonsági vagy megfelelési incidens.¹² A Netskope 2026. januári jelentése szerint a generatív MI-t használók 47 százaléka még mindig magánfiókot használ, egy átlagos szervezetnél pedig havonta 223 kapcsolódó adatbiztonsági szabályszegést rögzítenek, kétszer annyit, mint egy évvel korábban.¹³ Az IBM 2026. júliusi jelentése szerint a shadow AI-t érintő biztonsági események aránya egy év alatt 20-ról 43 százalékra nőtt, az incidenst elszenvedett szervezetek több mint kétharmadának pedig nem volt MI-irányítási szabályzata.¹⁴

A hazai helyzet sem kedvezőbb. A Medián 2025 novemberi, 600 fős reprezentatív felmérése szerint a munkavállalók több mint fele használ MI-t a munkájában. Az MI-t használók 65 százaléka saját kezdeményezésre teszi ezt, és csak 11 százalékuk használ munkáltató által biztosított megoldást. A válaszadók közel 80 százaléka szerint a munkahelyén hivatalosan szóba sem került az MI használata.¹⁵ A hazai munkahelyi MI-használat tehát nagyrészt shadow AI.

4.4 A shadow AI jelentette kockázatok

A kockázatok a 3. melléklet fenyegetéskatalógusával írhatók le. A kiinduló fenyegetés mindig az engedély nélküli használat (31. tétel), a következmények azonban eltérőek.

4.4.1 Bizalmasság és adatkiáramlás

A leggyakoribb eset, hogy a munkatárs szerződést, ügyféllistát vagy forráskódot másol be egy nyilvános szolgáltatásba. A Samsung munkatársai 2023-ban így juttattak belső forráskódot a ChatGPT-be, a vállalat ezt követően átmenetileg korlátozta a generatív MI-eszközök használatát.¹⁶ Ez a védett információ nyilvánosságra kerülése (20. tétel) és a személyes adatokkal történő visszaélés (39. tétel) esete. A magánfiókos szolgáltatások feltételei gyakran megengedik a bevitt tartalom tanításra való felhasználását, a Szervezet pedig sem törlést, sem naplót nem kérhet. 2025 nyarán a ChatGPT-ben megosztott beszélgetések ezrei voltak megtalálhatók keresőkben,¹⁷ 2025 decemberében pedig kiderült, hogy milliók által használt

¹¹ KPMG és University of Melbourne, Trust, attitudes and use of artificial intelligence, 2025. április (kpmg.com)

¹² Gartner, sajtóközlemény, 2025. november 19. (gartner.com)

¹³ Netskope, Cloud and Threat Report 2026, 2026. január 7. (netskope.com)

¹⁴ IBM és Ponemon Institute, Cost of a Data Breach Report 2026, 2026. július 29. (ibm.com), ismerteti Cybersecurity Dive, 2026. július 29.

¹⁵ Medián a Sicontact Kft. (ESET) megbízásából, MI a baj? kutatás, 2025. november (median.hu)

¹⁶ CNBC, 2023. május 2. (cnbc.com)

¹⁷ The Register, 2025. augusztus 1. (theregister.com)

böngészőbővítmények a ChatGPT-, Claude-, Gemini- és Copilot-beszélgetéseket a kiadó szervereire továbbították.¹⁸

4.4.2 Sértetlenség és a kimenet megbízhatósága

A kimenet ellenőrzés nélkül kerül vissza a Szervezetbe. A nyelvi modell magabiztosan téved, nem létező jogszabályhelyet vagy forrást is előállíthat, ez a nem megbízható forrásból származó információ (21. tétel) esete. A KPMG felmérésében a munkavállalók 66 százaléka ellenőrzés nélkül fogadja el az MI kimenetét, 56 százaléku hibázott is már emiatt.¹⁹ Egy 2025-ös kutatás szerint a kódgeneráló modellek által javasolt szoftvercsomagok közül a kereskedelmi modelleknél legalább 5,2, a nyílt modelleknél 21,7 százalék nem létezett,²⁰ ilyen néven pedig a támadó kártékony csomagot tehet közzé (slopsquatting).

4.4.3 Jogosultságok, MI-ügynökök és ellátási lánc

A bővítmények, az OAuth-integrációk és a saját telepítésű MI-ügynökök a munkatárs jogosultságaival érik el a levelezést, a dokumentumtárat, egyes esetekben a parancssort is. Ez az engedélyekkel való visszaélés (33. tétel) és a rosszindulatú szoftverek (40. tétel) kockázata. A 2026 elején gyorsan elterjedt OpenClaw személyi MI-ügynök hozzáfér a levelezéshez, a naptárhoz és a böngészőhöz, és parancsokat futtathat. Néhány hét alatt súlyos sérülékenységeket (köztük a CVE-2026-25253 azonosítójút) és több száz kártékony kiegészítőt azonosítottak hozzá.²¹ A shadow AI mögött ismeretlen ellátási lánc is áll, a szolgáltatás zavara (12. tétel) pedig olyan folyamatot állíthat le, amelyről a vezetés nem is tudta, hogy MI-re épül.

4.4.4 Jogi és megfelelési kockázatok

A shadow AI a jogszabályok vagy szerződések megszegésének kockázatát (30. tétel) is hordozza. Ha a munkatárs személyes adatot visz be olyan szolgáltatásba, amellyel nincs adatfeldolgozói szerződés, sérül az a követelmény, hogy az adatkezelő csak megfelelő garanciákat nyújtó adatfeldolgozót vegyen igénybe. Az adatokhoz hozzáférő személy ráadásul csak az adatkezelő utasítása szerint kezelhetné azokat.²² A holland adatvédelmi hatóság ezt adatvédelmi incidensnek tekinti, ha a munkatárs a munkáltatói megállapodással ellentétesen jár el.²³ Az üzleti titok védelmének feltétele, hogy a jogosult a titokban tartás érdekében az adott helyzetben általában elvárható magatartást tanúsítsa.²⁴ Ha a Szervezet tudja, hogy a munkatársai bizalmas információt másolnak nyilvános MI-szolgáltatásba, és nem lép, egy jogvitában nehezen igazolja az elvárható magatartást, és a munkavállaló titoktartási kötelezettségére²⁵ alapított fellépése is gyengülhet. Az ügyfélszerződések és titoktartási megállapodások megszegése szintén valós kockázat.

¹⁸ The Hacker News, 2025. december 15. (thehackernews.com)

¹⁹ KPMG és University of Melbourne, 2025 (kpmg.com)

²⁰ Spracklen és társai, We Have a Package for You!, USENIX Security 2025 (arxiv.org)

²¹ Kaspersky, 2026. február 16. (kaspersky.com)

²² (EU) 2016/679 rendelet 28. cikk (1) bekezdés és 29. cikk

²³ Autoriteit Persoonsgegevens (holland adatvédelmi hatóság), 2024. augusztus (autoriteitpersoonsgegevens.nl); (EU) 2016/679 rendelet 4. cikk 12. pont és 33. cikk (1) bekezdés

²⁴ 2018. évi LIV. törvény 1. § (1) bekezdés

²⁵ 2012. évi I. törvény 8. § (4) bekezdés

4.5 NIS2 előírások a kockázatok kezelésére

4.5.1 A törvényi keret

A NIS2 irányelv a kockázatkezelési intézkedések minimumaként írja elő többek között az informatikai biztonsági szabályzatokat, az ellátási lánc biztonságát, a kiberhigiéné és a képzést, valamint a hozzáférés-ellenőrzést és az eszközgazdálkodást.²⁶ A Kiberbiztonsági törvényben ezek a vezető feladataiként jelennek meg. A vezető gondoskodik a szervezet által használt rendszerek felméréséről és nyilvántartásba vételéről, kiadja a felhasználókra vonatkozó információbiztonsági szabályzatot, dönt a használatbavételről,²⁷ és gondoskodik a képzésről, valamint az események nyomonkövethetőségéről.²⁸ A jóváhagyott MI-szolgáltatóval szemben a kiberbiztonsági követelményeknek szerződéses kötelemként kell teljesülniük.²⁹ A shadow AI mindezeket megkerüli, kezelése ezért nem többletfeladat, hanem a törvényi kötelezettségek teljesítésének feltétele.

4.5.2 A rendelet védelmi intézkedései

A 7/2024. (VI. 24.) MK rendelet 2. mellékletének több követelménye közvetlenül a shadow AI kezelésére szolgál. A legfontosabbak a viselkedési szabályok, amelyeket a Szervezet minden osztályban dokumentál, kihirdet, és a hozzáférés előtt nyilatkozattal fogadtat el,³⁰ és amelyeknek a külső alkalmazások használatát is korlátozniuk kell.

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

[...]

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)

Az MI-használati szabályzat tehát egy minden osztályban kötelező követelmény teljesítése, és a céges e-mail-címmel történő regisztrációt is szabályoznia kell.

A Szervezet minden osztályban meghatározza, milyen feltételekkel dolgozhatnak fel az általa ellenőrzött információk külső rendszerben, vagy megtiltja a meghatározott típusú külső rendszerek használatát. Jelentős és magas osztályban külső rendszer csak akkor használható, ha a Szervezet ellenőrizte a rajta alkalmazott védelmi intézkedéseket, vagy jóváhagyott megállapodás van az üzemeltetőjével.³¹ A magánfiókos, szerződés nélküli MI-szolgáltatás egyik feltételnek sem felel meg, használata esetén a Szervezet ezekben az osztályokban nem teljesíti a követelményt. A nem szervezeti tulajdonban lévő rendszerek korlátozása opcionális.³² A jóváhagyott szolgáltatóval szemben a Szervezet szerződésben követeli meg a biztonsági

²⁶ (EU) 2022/2555 irányelv 21. cikk (2) bekezdés a), d), g) és i) pont

²⁷ 2024. évi LXIX. tv. 6. § (3) bekezdés 1., 7. és 12. pont

²⁸ 2024. évi LXIX. tv. 6. § (5) bekezdés a) és c) pont

²⁹ 2024. évi LXIX. tv. 6. § (5) bekezdés d) pont

³⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3. pont (A, J, M)

³¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.115. pont (A, J, M) és 2.116. pont (J, M)

³² 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.118. pont (O)

követelményeket, és ellenőrzi a szolgáltatót, jelentős és magas osztályban a beszállítói kockázatok rendszeres értékelése is kötelező.³³

A végpontokon a Szervezet minden osztályban meghatározza a tiltott vagy korlátozott szoftvereket és szolgáltatásokat, szabályozza a felhasználói szoftvertelepítést, és csak a szerződési feltételeknek és a jogszabályoknak megfelelő szoftvert használ.³⁴ Jelentős és magas osztályban a futtatható szoftverekre az alapértelmezett tiltás és a kivétel alapú engedélyezés elve érvényes,³⁵ ez a bővítmények és a helyben telepített MI-ügynökök elleni leghatékonyabb eszköz. A rendszerelem-leltár minden osztályban kötelező, magas osztályban a jogosulatlan elemek automatizált észlelése is, jelentős és magas osztályban pedig dokumentálni kell a meghatározott információk feldolgozásának és tárolásának helyét.³⁶

A hálózaton a Szervezet minden osztályban csak menedzselt interfészen kapcsolódik külső rendszerekhez. Jelentős és magas osztályban a forgalomra az alapértelmezett elutasítás elve érvényes, a meghatározott forgalmat pedig hitelesített proxykiszolgálón kell átvezetni,³⁷ ez teszi lehetővé az MI-forgalom felderítését és szűrését. A monitorozás minden osztályban kiterjed a jogosulatlan használat azonosítására, jelentős és magas osztályban a kimenő forgalom ellenőrzésére, magas osztályban a nem engedélyezett hálózati szolgáltatások észlelésére.³⁸ Az információszivárgás megakadályozása és a nyílt forrásokban megjelenő szervezeti információk figyelése opcionális,³⁹ a jelentős és magas osztályú rendszereknél bevezetésüket javasoljuk.

A biztonságtudatossági képzés minden osztályban kötelező, a tananyagot a változásokhoz és a biztonsági események tanulságaihoz kell igazítani.⁴⁰ A kihirdetett szabályok megszegése esetén a rendelet fegyelmi eljárás kezdeményezését írja elő,⁴¹ ezért érdemes elválasztani a szabályzat kiadása előtti használatra adott amnesztiát a későbbi szankcionálástól. A téves adatbevitel biztonsági esemény, kezeléséhez az opcionális információszivárgási követelmény ad mintát.⁴² Végül a kockázatelemzést jelentős változáskor frissíteni kell,⁴³ és a munkahelyi MI-használat elterjedése ilyen változás.

4.6 AI Act előírások a kockázatok kezelésére

Az AI Act a Szervezetet elsősorban alkalmazóként érinti. Alkalmazó az, aki a felügyelete alá tartozó MI-rendszert használja, kivéve, ha a használatra személyes, nem szakmai jellegű tevékenység során kerül sor.⁴⁴ Munkavégzésnél ez a kivétel nem áll fenn, arra azonban a rendelet nem ad egyértelmű választ, hogy a Szervezet tudta nélkül használt eszköz a felügyelete alá tartozik-e. Az egyik értelmezés szerint a jóváhagyás hiánya kizárja a felügyeletet, a másik szerint

³³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont (A, J, M) és 19.16. pont (J, M)

³⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.26., 6.47. és 6.49. pont (A, J, M)

³⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.31. pont (J, M)

³⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.36. pont (A, J, M), 6.39. pont (M) és 6.52. pont (J, M)

³⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 17.17. pont (A, J, M), 17.20. és 17.22. pont (J, M)

³⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.13. pont (A, J, M), 18.17. pont (J, M) és 18.33. pont (M)

³⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 17.24. és 4.44. pont (O)

⁴⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 3.2. pont (A, J, M)

⁴¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.12. pont (A, J, M)

⁴² 7/2024. (VI. 24.) MK rendelet 2. melléklet 9.9. pont (A, J, M) és 9.35. pont (O)

⁴³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.4. pont (A, J, M)

⁴⁴ Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (AI Act) 3. cikk 4. pont

a munkavégzés keretében, a Szervezet érdekében történő használat a Szervezet felelősségi körébe esik. Az Európai Bizottság szerint az a vállalat, amelynek munkatársai például fordításra használják a ChatGPT-t, köteles eleget tenni az MI-jártassági kötelezettségnek.⁴⁵ Álláspontunk szerint a Szervezet nem hivatkozhat biztonsággal arra, hogy a használatról nem tudott. Ezt a kötelezettséget az (EU) 2026/1744 rendelet enyhítette, de nem szüntette meg.

(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 [...]. 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 (EU) 2026/1744 rendelettel megállapított szöveg]

A shadow AI további felelősséget is teremthet. Az első a tiltott gyakorlat. Az AI Act 2025. február 2. óta tiltja a természetes személyek érzelmeiből következtetést levonó MI-rendszer használatát a munkahelyeken, kivéve, ha az orvosi vagy biztonsági okokból történik.⁴⁶ Ha egy vezető online szolgáltatással elemezteti a munkatársak érzelmi állapotát egy videóértekeztet hang- és képanyagából, a Szervezet tiltott gyakorlatot valósít meg. Erre legfeljebb 35 millió eurós vagy a teljes éves globális árbevétel 7 százalékáig terjedő bírság szabható ki, a kettő közül a magasabb.⁴⁷ A második a szerepváltás. Aki egy általános célú MI-rendszer rendeltetését jelentősen módosítva nagy kockázatúvá teszi, a nagy kockázatú rendszer szolgáltatójának minősül.⁴⁸ Ha a HR-munkatárs nyilvános chatbottal szűri és rangsorolja a pályázókat, a felhasználás a III. melléklet szerinti kiválasztási célra irányul,⁴⁹ így a Szervezet a 2027. december 2-től alkalmazandó szolgáltatói kötelezettségek alanyává válhat.⁵⁰ Végül a deepfake audiovizuális tartalmat létrehozó MI-rendszer alkalmazójának 2026. augusztus 2. óta közölnie kell, hogy a tartalom mesterségesen jött létre.⁵¹

A kockázatkezelés eszközei az AI Act szerint is ugyanazok. A felhasználási célt is rögzítő MI-nyilvántartás, a tiltott és a nagy kockázatú felhasználások kizárása a szabályzatban és az eszközspecifikus MI-jártassági képzés egyszerre teljesíti a két szabályozás elvárásait.

⁴⁵ Európai Bizottság, AI Literacy, Questions & Answers, 2026. július 27-i frissítés (digital-strategy.ec.europa.eu)

⁴⁶ (EU) 2024/1689 rendelet 5. cikk (1) bekezdés f) pont és 113. cikk harmadik bekezdés a) pont, az (EU) 2026/1744 rendelettel megállapított szöveg

⁴⁷ (EU) 2024/1689 rendelet 99. cikk (3) bekezdés

⁴⁸ (EU) 2024/1689 rendelet 25. cikk (1) bekezdés c) pont

⁴⁹ (EU) 2024/1689 rendelet III. melléklet 4. pont a) alpont

⁵⁰ (EU) 2024/1689 rendelet 113. cikk harmadik bekezdés c) pont i. alpont, az (EU) 2026/1744 rendelettel megállapított szöveg

⁵¹ (EU) 2024/1689 rendelet 50. cikk (4) bekezdés és 113. cikk második bekezdés

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; az (EU) 2016/679 rendelet (GDPR)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.); 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről és a védelmi intézkedésekről; 2012. évi I. törvény a munka törvénykönyvéről; 2018. évi LIV. törvény az üzleti titok védelméről
- NCSC (UK), Shadow IT (2023, felülvizsgálva 2026); IBM, What is shadow AI? (2024); Európai Bizottság, AI Literacy, Questions & Answers (2026. július 27.); Autoriteit Persoonsgegevens (2024. augusztus)
- IBM és Ponemon Institute, Cost of a Data Breach Report 2026; Gartner (2025. november 19.); KPMG és University of Melbourne (2025); Netskope, Cloud and Threat Report 2026; Medián, MI a baj? (2025. november)
- Spracklen és társai, USENIX Security 2025; Kaspersky (2026. február 16.); The Hacker News (2025. december 15.); The Register (2025. augusztus 1.); CNBC (2023. május 2.)

6. KAPCSOLÓDÓ ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- MKIK VFP3 KiberVéd jogi állásfoglalás 2026/45 (általános célú MI-rendszerek, MI-ügynökök, MI-jártasság, átláthatóság) - Elérhető: <https://nis2.mkik.hu/jogi-allasfoglalasok/45> ;
- MKIK VFP3 KiberVéd jogi állásfoglalás 2026/48 (meghatározó MI-komponenst tartalmazó célszoftverek) - Elérhető: <https://nis2.mkik.hu/jogi-allasfoglalasok/48> ;
- NCSC (UK), Shadow IT;
- OWASP Top 10 for LLM Applications 2025;
- ISO/IEC 42001 és ISO/IEC 27001, az MI-irányítási és az információbiztonsági irányítási rendszer nemzetközi keretei.