



BLACK CELL
Protecting critical infrastructures

WHITEPAPER

EU AI ACT WHITEPAPER

Útmutató vállalatok számára

Created by

Kókai-Nedelkó Anna, Dr. Faragó Tamás | Compliance
2026. Július



TARTALOMJEGYZÉK

BEVEZETÉS	3
------------------	----------

VEZETŐI ÖSSZEFOGLALÓ	4
-----------------------------	----------

AZ EU MESTERSÉGES INTELLIGENCIÁRÓL SZÓLÓ RENDELETE	6
---	----------

A RENDELET JELENTŐSÉGE

AZ AI ACT CÉLJA

HATÁLY – KIRE VONATKOZIK AZ AI ACT?

KIRE ÉS MIRE NEM TERJED KI A SZABÁLYOZÁS?

LEGFONTOSABB FOGALMAK AZ AI ACT-BEN

AZ AI ACT KOCKÁZATALAPÚ MEGKÖZELÍTÉSE

A SZABÁLYOZÁS FŐBB KÖTELEZETTSÉGEI ÉS SZEREPLŐI

NAGY KOCKÁZATÚ MI-RENDSZEREK KÖVETELMÉNYEI

BEJELENTŐ HATÓSÁG, MEGFELELŐSÉGÉRTÉKELÉSI ELJÁRÁS

ÁTLÁTHATÓSÁGI KÖVETELMÉNYEK

FORGALOMBA HOZATAL UTÁNI NYOMONKÖVETÉS,

INCIDENSEK JELENTÉSE ÉS PIACFELÜGYELET

ÁLTALÁNOS CÉLÚ MI-MODELLEK ÉS KAPCSOLÓDÓ

KÖTELEZETTSÉGEK

MI SZABÁLYOZÓI TESZTKÖRNYEZET

ILLETÉKES NEMZETI HATÓSÁGOK

SZANKCIÓK AZ AI ACT SZERINT

SZANKCIÓK RENDSZERE MAGYARORSZÁGON

ALKALMAZHATÓVÁ VÁLÁS („HATÁLYBA LÉPÉS”)

AZ AI ACT ÉS A HAZAI SZABÁLYOZÁS KAPCSOLATA	41
HATÓSÁGOK	

BEVEZETÉS

Jelen útmutató összefoglalót kíván nyújtani a szervezeteknek az Európai Unió (a továbbiakban, mint EU) mesterséges intelligenciáról (a továbbiakban, mint AI vagy MI) szóló egységes normájának szervezeti szempontból való alkalmazása körében. Minden esetben a vállalkozások szemszögéből kívánjuk bemutatni az EU-s és magyar keretrendszert az értekezés kiadásakor hatályos jogszabályi környezetben.

Egyes kérdések megértése szempontjából szükségeszerű azonban bemutatni a mögöttes elvárásokat, például a szervezetek mellett a hatóságok feladatait, a működésük rendjét.

VEZETŐI ÖSSZEFOGLALÓ

Az Európai Unió 2025. augusztusában kiadta az első egységes, rendeleti szintű mesterséges intelligencia szabályozását (AI Act). A rendelet unikális, mivel az EU területén (valamint az EGT-tagországokban) valamennyi tagállamban egységesen alkalmazandó, tehát – például a NIS 2 Irányelvvel ellentétben – a tagállamoknak nem kell átültetniük azokat a nemzeti jogrendszerükbe, így minden tagállamban azonos szabályok irányadóak.

A rendelet lépcsőzetesen válik alkalmazhatóvá: egyes rendelkezések már most is alkalmazandóak, míg mások csak 2026. augusztusától, illetve 2027. augusztusától.

Az AI Act az alábbi szereplőkre vonatkozik:

- az EU-ban MI-rendszereket forgalomba hozó vagy üzembe helyező szolgáltatók,
- az MI-rendszerek EU-n belüli tartózkodási hellyel rendelkező alkalmazói,
- az MI-rendszerek importőrei és forgalmazói,
- termékgyártók, amelyek a termékükkel együtt MI-rendszert hoznak forgalomba vagy helyeznek üzembe a saját nevük vagy védjegyük alatt.

Így Az MI-rendszereket kockázatalapon több kategóriába sorolja:

- vannak olyanok, melyek használata tiltott az EU területén,
- vannak olyanok, melyek nagy kockázatúak, azonban bizonyos garanciák (kockázatkezelés, dokumentáció, tanúsítás) mellett használhatóak,
- egyesek esetén csak dokumentációs kötelezettség áll fent,
- míg megint mások használata nem jelent kockázatot a természetes személyek jogaira és szabadságára, ezért azok használata nem esik a szabályozás alá.

A kötelezettségek nemcsak a fejlesztők, de az importőrök és forgalmazók esetén is alkalmazandóak.

AZ EU MESTERSÉGES INTELLIGENCIÁRÓL SZÓLÓ RENDELETE

3.1. A RENDELET JELENTŐSÉGE

A mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet) szóló 2024/1689. Európai Parlament és Tanácsi Rendelet (a továbbiakban: AI Act) jelentősége a rendeleti jellegéből adódik, mivel az EU-s rendeletek az EU egész területén, minden tagállam esetén közvetlenül alkalmazandóak (mint például a GDPR vagy a DORA rendelet), tehát nem kell a tagállamoknak azokat átültetniük a hazai jogrendszerükbe (mint például a NIS 2 Irányelvet), így nem okozhat inkonzisztenciát a tagállami szabályozások esetén.

Azonban természetesen vannak olyan kérdések, melyek szabályozása a nem állhat EU-s hatáskörben; ilyen lehet a hatóságok (pl. piacfelügyeleti hatóság) vagy egyedüli kapcsolattartó pont tagállami kijelölése. Ezen rendelkezéseket a tagállamok saját hatáskörben törvényekben és rendeletekben, az AI Act egyfajta kiegészítéseként hozzák meg. Erről a jelen értekezés későbbi pontjaiban térünk ki.

3.2. AZ AI ACT CÉLJA

Az AI Act, az Európai Unió első átfogó, közvetlenül alkalmazandó mesterségesintelligencia-szabályozása. Célja, hogy egységes jogi keretet teremtsen a mesterséges intelligencián alapuló rendszerek EU-n belüli fejlesztésére, forgalomba hozatalára, üzembe helyezésére és használatára, miközben biztosítja az alapvető jogok, a biztonság, az egészség és az uniós értékek védelmét.

Az AI Act azért bír kiemelt jelentőséggel, mert az Európai Unión belül egységes szabályozási alapot teremt, amelyhez a tagállami végrehajtási rendszereknek is igazodniuk kell.

A rendelet logikája kockázatalapú megközelítésre épül. Ez azt jelenti, hogy nem minden MI-rendszerre vonatkoznak azonos szigorú szabályok. Minél nagyobb kockázatot jelent egy rendszer az emberekre, a társadalomra vagy az alapvető jogokra nézve, annál szigorúbb követelmények kapcsolódnak hozzá.

3.3. HATÁLY – KIRE VONATKOZIK AZ AI ACT?

- az EU-ban MI-rendszereket **forgalomba hozó** vagy **üzembe helyező**, vagy általános célú MI-modelleket forgalomba hozó **szolgáltatók** (függetlenül attól, hogy a szolgáltatók letelepedési vagy tartózkodási helye az Unióban vagy harmadik országban van-e),
- az MI-rendszerek EU-n belüli tartózkodási hellyel rendelkező **alkalmazói**,
- az MI-rendszerek azon szolgáltatói és alkalmazói, amelyek letelepedési vagy tartózkodási helye harmadik országban van, amennyiben az MI-rendszer által előállított kimenet használatára az Unióban kerül sor,
- az MI-rendszerek **importőrei** és **forgalmazói**,
- **termékgyártók**, amelyek a termékükkel együtt MI-rendszert hoznak forgalomba vagy helyeznek üzembe a saját nevük vagy védjegyük alatt.

3.4. KIRE ÉS MIRE NEM TERJED KI A SZABÁLYOZÁS?

- Katonai vagy nemzetbiztonsági célú MI használat, forgalmazás, üzembe helyezés,
- Bűnüldözési, igazságszolgáltatási célú MI használat, forgalmazás, üzembe helyezés,
- A szabad és nyílt forráskódú licencek alapján kibocsátott MI-rendszerekre, amennyiben azok nem esnek a nagy kockázatú rendszerek kategóriájába
- A kifejezetten a tudományos kutatás-fejlesztés kizárólagos céljára kifejlesztett és üzembe helyezett MI-rendszerekre vagy MI-modellekre, és azok kimenetére,
- MI-rendszereket pusztán személyes tevékenység során való használatára.

3.5. LEGFONTOSABB FOGALMAK AZ AI ACT-BEN

MI-RENDSZER

Gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet.

SZOLGÁLTATÓ

Olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely MI-rendszert vagy általános célú MI-modellt fejleszt vagy fejlesztett, és a saját neve vagy védjegye alatt – akár fizetés ellenében, akár ingyenesen – az MI-rendszert vagy az általános célú MI-modellt forgalomba hozza, vagy az MI-rendszert üzembe helyezi.

ALKALMAZÓ

Olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely a felügyelete alá tartozó MI-rendszert használja, kivéve, ha az MI-rendszert személyes, nem szakmai jellegű tevékenység során használják.

IMPORTŐR

Az Unióban tartózkodó vagy ott letelepedett természetes vagy jogi személy, aki vagy amely egy harmadik országban letelepedett természetes vagy jogi személy nevével, vagy védjeggyével ellátott MI-rendszert hoz forgalomba.

FORGALMAZÓ

Az a szolgáltatótól vagy az importőrtől eltérő természetes vagy jogi személy az ellátási láncban, aki vagy amely az uniós piacon MI-rendszert forgalmaz.

FORGALOMBA HOZATAL

Valamely MI-rendszer vagy általános célú MI-modell első alkalommal történő forgalmazása az uniós piacon.

ÜZEMBE HELYEZÉS

Valamely MI-rendszer első használatra történő rendelkezésre bocsátása közvetlenül az alkalmazó számára vagy saját használatra az Unióban, a rendeltetésének megfelelően

ÁLTALÁNOS CÉLÚ MI-MODELL

olyan MI-modell – ideértve azt is, amikor az ilyen MI-modell tanítása nagy adatmennyiséggel, nagy léptékű önfelügyelet mellett történik –, amely jelentős általánosságot mutat, és forgalomba hozatalának módjától függetlenül, különféle feladatok széles körének elvégzésére képes, valamint többféle downstream rendszerbe vagy alkalmazásba integrálható, azon MI-modellek kivételével, amelyeket a forgalomba hozatalukat megelőzően kutatási, fejlesztési vagy prototípus-alkotási tevékenységekre használnak.

DOWNSTREAM SZOLGÁLTATÓ

olyan MI-rendszer – ideértve az általános célú MI-rendszert is – szolgáltatója, amelybe MI-modellt integráltak, függetlenül attól, hogy a szolgáltató által biztosított, vertikálisan integrált MI-modellről vagy egy másik szervezet által szerződéses viszonyok alapján biztosított MI-modellről van-e szó.

3.6. AZ AI ACT KOCKÁZATALAPÚ MEGKÖZELÍTÉSE

A szabályozás megkülönböztet tiltott MI-gyakorlatokat, nagy kockázatú MI-rendszereket, bizonyos átláthatósági kötelezettség alá eső rendszereket, valamint olyan megoldásokat, amelyekre jóval enyhébb szabályok vonatkoznak.

A tiltott gyakorlatok olyan alkalmazások, amelyeket az uniós jogalkotó eleve elfogadhatatlannak tekint, míg a nagy kockázatú rendszerek esetében részletes megfelelési követelmények érvényesülnek.

AZ AI ACT SZERINTI KOCKÁZATI KATEGÓRIÁK ÉS KAPCSOLÓDÓ KÖVETELMÉNYEK

Az AI Act az alábbi kockázati kategóriákat határozza meg:

- Tiltott MI gyakorlatok
- Nagy kockázatú MI-rendszerek
- Korlátozott kockázatú (átláthatósági követelmények) MI-rendszerek
- Minimális kockázatú MI-rendszerek

A szervezeteknek először azt kell megállapítaniuk, hogy a tervezett MI-rendszer/gyakorlat a fenti kategóriák szerint melyikbe esik. Ezt a használat célja, az érintettek köre (pl. védett csoportok), a felhasználás helye (pl. nyilvános hely), illetve a felhasználó (pl. kormányzati szerv) is befolyásolja. Ezért javasoljuk, hogy az MI-rendszer/gyakorlat tervezési fázisában végezze el a szervezet a fenti besorolást, mivel már itt kiderülhet, hogy a tervezett cél/felhasználási hely okán az az EU területén tilos!

TILTOTT MI GYAKORLATOK

Tiltott az olyan MI-rendszerek forgalomba hozatala, üzembe helyezése vagy használata, amelyek:

- tudatalatti célzott manipulációs célból úgy, hogy jelentősen gyengítik a megalapozott döntéshozatalra való képességüket,
- az emberek vagy azok csoportjainak életkor, fogyatékosság, illetve egyedi szociális vagy gazdasági helyzet miatt fennálló valamilyen sebezhetőségét kihasználó rendszerek,
- közösségi magatartás megfigyelése mellett személyeket osztályoz,
- személyek kockázatértékelését végzi,
- arcképek internetről vagy térfigyelő kamerarendszerekből való, nem célzott lekérdezésével arcfelismerő adatbázisokat hoznak létre vagy ilyeneket bővítenek,
- érzelemfelismerő rendszerek (ha nem orvosi vagy biztonsági okból történik),
- biometrikus kategorizálásra alkalmas rendszerek,
- bizonyos bűnüldözési kivételektől eltekintve a valós idejű távoli biometrikus azonosító rendszerek.
- Egy elfogadott, de még ki nem hirdetett javaslat a kört kiegészíti még két esetkörrel:
 - olyan mesterséges intelligencia-rendszerek, amelyek gyermekek szexuális bántalmazását ábrázoló anyagokat képesek előállítani, vagy
 - olyan képeket, videókat és hangfelvételeket hoznak létre, amelyek azonosítható személyek intim testrészeit vagy szexuálisan explicit tevékenységeket ábrázolnak az érintettek beleegyezése nélkül (nudifier)

TILTOTT MI GYAKORLATOK

Tiltott gyakorlat	Példa	Indok
Tudatalatti célzott manipuláció	Egy mobilapp mikroadatok (pl. érintési sebesség, görgetés) alapján “gyenge pontokat” azonosít, és észrevétlenül időzített ajánlatokat jelenít meg, hogy impulzusvásárlást váltsanak ki.	A felhasználó nincs tudatában annak, hogy manipulálják a döntését
Valamilyen sebezhetőségét kihasználó rendszerek	Egy játék gyerekeknek agresszívan ajánl in-app vásárlást, kihasználva a fejlődési sajátosságait.	Védett csoportok vagy hátrányos helyzet kihasználása
Személyek osztályozása (social scoring)	Egy platform a felhasználók online viselkedése, kapcsolatai és vásárlásai alapján “megbízhatósági pontszámot” ad, ami befolyásolja például a hitelfelvételi lehetőséget vagy a közösségi közlekedés használatára való jogosultságot, egyéb szolgáltatáshoz való hozzáférést.	Általános társadalmi megítélés MI alapon
Személyek kockázatértékelése	Egy rendészeti MI-rendszer megjósolja, hogy egy adott személy várhatóan elkövet-e bűncselekményt, és ennek alapján például megfigyelés alá veteti/veszi.	Egyéni viselkedés előrejelzése (hatósági) döntések megalapozása céljából

Tiltott gyakorlat	Példa	Indok
Arcfelismerő adatbázisok létrehozása	Egy cég automatizáltan letöltött milliányi képet közösségi médiáról, majd arcfelismerő modellt tanít, adatbázist épít engedély nélkül.	Nem célzott, GDPR-ral nem összeegyeztethető adatgyűjtés
Érzelemfelismerés	Egy munkahelyi eszköz webkamera képe alapján elemzi a dolgozók hangulatát, és: “elkötelezettségi pontszámot” számít amit például teljesítményértékeléshez használ.	Érzelmi állapot MI-alapú értékelése döntésekhez / döntések előkészítéséhez
Biometrikus kategorizálás	Egy rendszer arckép alapján etnikai hovatartozást vagy vallási meggyőződést próbál meghatározni.	Biometrikus adatból történő érzékeny megállapítások
Valós idejű távoli biometrikus azonosító rendszerek	Egy bevásárlóközpont kamerarendszere előben futtat arcfelismerést, és automatikusan azonosítja a látogatókat, vásárlói listákhoz rendeli őket.	valós idejű tömeges azonosítás közterületen hozzájárulás, illetve tudomás nélkül
Gyermekek szexuális bántalmazását, kizsákmányolását ábrázoló anyagokat előállító rendszerek		Gyermekek szexuális bántalmazását, kizsákmányolására alkalmas
Szexuális képeket, videókat és hangfelvételeket létrehozó/módosító rendszerek	Olyan nudifier applikációk, melyek személyekről ruhában készült képekről „eltávolítják” a ruhát és meztelenül ábrázolják az adott személyt.	Hozzájárulás nélkül, potenciális zsarolásra, szexuális kizsákmányolásra alkalmas

NAGY KOCKÁZATÚ RENDSZEREK

- az MI-rendszert az AI Act I. mellékletben felsorolt bizonyos termékek biztonsági alkotórésze, vagy az MI-rendszer önmagában ilyen termék (pl. gépjármű, vízi jármű, játék, etc. biztonsági rendszere, élet-, baleset-, vagy vagyonvédelmét célzott szolgálni),
- természetes személyekre vonatkozó profilalkotás,
- biometria területén való alkalmazás (érzelemfelismerés, biometrikus kategorizálás, távoli biometrikus azonosító rendszerek),
- kritikus infrastruktúra irányító rendszere (pl. víz-, gáz-, fűtési vagy villamosenergia-szolgáltatás),
- oktatás és szakképzés területén való alkalmazás (bejutás, felvétel meghatározása, eredmények értékelésére való használat, szintfelmérés, tiltott tanulói magatartások észlelése),
- foglalkoztatás, a munkavállalók irányítása és az önfoglalkoztatás területén (felvétel, kiválasztás, teljesítményértékelés),
- alapvető magán- és közszolgáltatásokhoz és ellátásokhoz való hozzáférés és ezek igénybevétele területén (segélyek, kórházi vagy egyéb ellátásra való jogosultság megállapítása, hitelképesség, élet- és egészségbiztosítás),
- bűnüldözés területén (bűncselekmény áldozatává válással kapcsolatos számítások, poligráf, ismételt bűnelkövetővé válás esélyének számítása, profilalkotás),
- migráció, menekültügy, határvédelem területén (poligráf, egészségügyi kockázatértékelés, vízum vagy menekültügyi kérelmek értékelése, személyek felismerése, azonosítása),
- igazságszolgáltatás területén (ténybeli és jogi értelmezések, választások, népszavazások eredményének befolyásolása).

Nem tekinthetők nagy kockázatúnak a fentiek, amennyiben nem jelent jelentős negatív (kárt eredményező) kockázatot természetes személyek:

- egészségére,
- biztonságára vagy,
- alapvető jogaira nézve, például azáltal, hogy nem befolyásolja lényegesen a döntéshozatal kimenetelét.

Amennyiben a szolgáltató úgy ítéli meg, hogy annak ellenére, hogy a fenti tevékenységeket támogatja vagy arra irányul az MI-rendszer, úgy kockázatelemzésben kell dokumentálnia a megállapításait.

Tehát, attól, hogy egy MI-rendszer nagy kockázatúnak minősül még önmagában nem jelenti, hogy ne lenne használható; itt a szervezeteknek a rendszerek bevezetése előtt minden esetben el kell végezniük egy teljességre törekvő kockázatelemzést, melyet egyrészt dokumentálniuk kell, másrészt folyamatosan frissíteniük kell. A kockázatelemzés természetesen önmagában nem elég, minden esetben gondoskodniuk kell a kockázatkezelésről (csökkentés, áthárítás, elkerülés, elfogadás).

Nagy kockázatú gyakorlat	Példa	Indok
Biztonsági rendszer vagy alkotórész	Egy autonóm jármű MI-alapú akadályfelismerő rendszert használ, amely automatikusan fékez gyalogos észlelésekor.	MI közvetlenül érinti az élet- és vagyonbiztonságot
Profilalkotás	Egy bank MI-rendszere az ügyfél tranzakciós adatai, online viselkedése alapján hitelkockázati profilt készít, és ez alapján dönt hitelről.	Automatizált döntések egyéni profilok alapján, mely hibás lehet
Biometria (érzelemfelismerés, kategorizálás, azonosítás)	Egy call center MI hangmintából próbál stresszszintet becsülni az ügyfélnél.	Fizikai/jellemző alapú azonosítás vagy értékelés a tudomásra hozatal nélkül, vagy hibás eredmény
Kritikus infrastruktúra irányítása	Egy áramhálózati rendszerben az MI automatikusan szabályozza a terhelést és akár lekapcsolhat bizonyos hálózati részeket túlterhelés esetén.	Meghibásodás esetén társadalmi szintű hatás
Oktatás és szakképzés	Egy egyetemi felvételi rendszer MI alapján értékeli a beadott esszéket és rangsorolja a jelentkezőket.	Hozzáférés és értékelés automatizált módon a hiba lehetőségével
Foglalkoztatás és munkaerő-menedzsment	Egy vállalat MI-rendszere a munkavállaló teljesítményét értékeli produktivitási adatok alapján.	Karrierre, munkavállalásra közvetlen hatással van, hiba lehetősége fennáll

Nagy kockázatú gyakorlat	Példa	Indok
Alapvető szolgáltatásokhoz való hozzáférés	Egy olyan MI-rendszer, amely automatikusan eldönti, ki jogosult támogatásra.	Alapvető jogokhoz/ellátáshoz való hozzáférés befolyásolása, hibázhat.
Bűnüldözés	Egy MI-alapú “digitális poligráf” viselkedési jelekből próbál hazugságot detektálni.	Szabadságjogokat érintő döntés
Migráció, menekültügy, határvédelem	Egy határátkelő MI-rendszer összeveti az utas arcát az útlevéllel és automatikus döntéstámogatást ad beléptetéshez.	Alapvető jogok és státusz eldöntése
Igazságszolgáltatás	Egy MI-rendszer ítéletek adatbázisa alapján konkrét büntetésre tesz javaslatot.	Jogi és demokratikus folyamatokat, szabadságjogokat érinthet

3.7. A SZABÁLYOZÁS FŐBB KÖTELEZETTSÉGEI ÉS SZEREPLŐI

Az AI Act nemcsak a technológia fejlesztőire vonatkozik, hanem több szereplőt külön nevesít. A rendelet szabályozza többek között a szolgáltatók, az alkalmazók, az importőrök és a forgalmazók kötelezettségeit is. Ennek azért van jelentősége, mert a megfelelési kötelezettségek nem egyetlen szereplőre koncentrálódnak, hanem a rendszer életútjának különböző szakaszaiban eltérő felelősséget állapítanak meg.

MI kategória	Rendszer megfelelési követelmények	Szolgáltatóval kapcsolatos kötelezettségek
Tiltott MI gyakorlat	Nem használható	Nem használható
Nagy kockázatú MI-rendszer	• Kockázatkezelési keretrendszer, • Adatok és adatkormányzás (data governance), • Műszaki dokumentáció, • Nyilvántartás, • Átláthatóság és tájékoztatás, • Emberi felügyelet, • Pontosság, stabilitás és kiberbiztonság.	• Kapcsolati információk feltüntetése, • Minőségirányítási rendszer működtetése, • Dokumentáció vezetése, • Naplók megőrzése, • Megfelelőségértékelési eljárás, • EU-megfelelési nyilatkozat elkészítése, • CE jelölés feltüntetése, • Regisztráció.
Általános célú MI-rendszer	-	• Folyamatosan frissített műszaki dokumentáció, • Eljárások a szellemi tulajdonjogokra, szerzői és kapcsolódó jogokra vonatkozólag, amennyiben az beépíthető más rendszerekbe is, • Összefoglaló a tanítási tartalomról.

3.8. NAGY KOCKÁZATÚ MI RENDSZEREK KÖVETELMÉNYEI

A nagy kockázatú MI-rendszerek esetében a szabályozás különösen a kockázatkezelésre, az adatok minőségére, a műszaki dokumentációra, az emberi felügyeletre, az átláthatóságra, a pontosságra és a kiberbiztonságra helyez hangsúlyt. A rendelet ezzel azt kívánja biztosítani, hogy az ilyen rendszerek használata ne járjon aránytalan veszéllyel az érintettekre nézve.

KOCKÁZATKEZELÉSI KERETRENDSZER (9. CIKK)

A szervezetnek az MI-rendszer teljes életciklusában (tervezés, fejlesztés, tesztelés, bevezetés, fenntartás, változáskezelés, kivezetés) működtetnie kell a kockázatkezelési keretrendszert, melyet kialakított. Tehát praktikus azonosítania kell a rendeltetésszerű és rendellenes használatból adódó kockázatokat, azokat értékelnie kell, valamint a kockázatokat kezelnie szükséges. A keretrendszer működését folyamatosan felülvizsgált módon, dokumentáltan kell végeznie a szervezetnek.

A kockázatkezelés során az alábbiakat kell figyelembe venni:

- ismert és észszerűen előre látható kockázatok azonosítása és elemzése az MI-rendszer rendeltetésszerű használata esetén
 - az egészségre,
 - biztonságra és
 - alapvető jogokra tekintettel,
- rendeltetésszerű használata, valamint észszerűen előre látható rendellenes használata esetén felmerülő kockázatok becslése és értékelése,
- egyéb esetlegesen felmerülő kockázatok értékelése,
- kockázatok kezelésére vonatkozó intézkedések.

A kockázatok azonosítása, elemzése és értékelése körében a szolgáltató tesztek végezhet.



ADATOK ÉS ADATKORMÁNYZÁS (DATA GOVERNANCE) (10. CIKK)

Mivel a tanító- validációs- és tesztadatok az MI-rendszerek „lelke”, ezért azoknak minden esetben a rendszer használati céljának és körülményeinek megfelelőnek kell lenniük. Ennek érdekében a tanítóadatok kezelését különös körültekintéssel kell szabályoznia a szervezeteknek.

Nagy kockázatú MI-rendszerek esetén a tanításra, validációra, tesztelésre használt adatoknak relevánsnak, kellően reprezentatívnak, valamint a lehető legnagyobb mértékben hibáktól mentesnek és teljesnek kell lenniük. Figyelembe kell venniük sajátosságokat (földrajzi, kontextuális, magatartási vagy funkcionális) a nagy kockázatú MI-rendszert használati környezetéhez igazodóan.

Ennek keretében tehát a szervezeteknek szabályzatokat kell alkotniuk az adatok beszerzésével kapcsolatosan (milyen forrásból, mit minősítenek megfelelőnek, a felhasználás módja vonatkozásában kellően relevánsak-e (pl. egy Lengyelországban 65 évesnél idősebb emberekről szóló adatbázis nem lesz releváns egy Japán területén 18-25 éves korosztályra specializált rendszer esetén), a felhasználásukkal kapcsolatosan (milyen eljárások mentén kell deperszonalizálni azokat, hogyan használhatóak azok tanításra, milyen validációs értékeket fogadnak el a szervezetek a tanítóadatok esetében).

Mivel a teljes életciklus vonatkozásában kell ezeket a szabályokat megalkotni, ezért célszerű kitérni már a tervezési szakban is, valamint ezt követően a teszteléstől a továbbfejlesztésig minden időszakra.

MŰSZAKI DOKUMENTÁCIÓ (11. CIKK)

A nagy kockázatú MI-rendszerek műszaki dokumentációját a rendszer forgalomba hozatala vagy üzembe helyezése előtt kell elkészíteni, és naprakészen kell tartani.

A műszaki dokumentációval szembeni követelmények:

- világos és érthető (felhasználó és hatóság számára),
- bizonyítja az AI Act-ben foglalt kötelezettségek teljesülését,
- tartalmazza az alábbi elemeket:
 - általános leírás:
 - rendszer rendeltetése, a szolgáltató neve és a rendszer verziója, feltüntetve a korábbi verziókhoz való viszonyát,
 - MI-rendszer hogyan működik együtt hardverekkel, szoftverekkel, más MI-rendszerekkel,
 - szoftver, firmware verzió és verziófrissítési követelmények,
 - MI-rendszer forgalomba hozatali információi (letölthető app, API, etc.),
 - MI-rendszer termékek alkotóeleme, e termékek külső jellemzőit, jelölését és belső elrendezését bemutató fényképek vagy illusztrációk,
 - felhasználói felület alapeírása,
 - használati utasítás.
 - MI-rendszer elemeinek és fejlesztési folyamatának részletes leírása:
 - fejlesztési módszerek, leírások, más rendszerekkel való kapcsolat, integráció leírása,
 - rendszer tervezési leírása, algoritmusok általános logikája, tervezési döntések, etc.,
 - architektúra leírás,
 - tanítórendszer és technikák,
 - emberi felügyeleti intézkedések értékelések,
 - teljesítmény előre meghatározott változásai,
 - validálási és tesztelési megoldások,
 - bevezetett kibervédelmi intézkedések leírása.

- MI-rendszer nyomon követésére, működésére és ellenőrzésére vonatkozó részletes információk,
 - teljesítménymutatók megfelelőségének leírása,
 - kockázatkezelési rendszer részletes ismertetése,
 - életciklusa során végrehajtott releváns változtatások leírása,
 - alkalmazott harmonizált szabványok jegyzéke,
 - EU-megfelelőségi nyilatkozat másolata,
 - teljesítményének a forgalomba hozatalt követő értékelésére szolgáló rendszer részletes leírása.
- Az AI Act I. melléklete szerinti termékek esetén egységes a termék dokumentációjával.

NAPLÓZÁS (12. CIKK)

Az MI-rendszer teljes életciklusa alatt folyamatosan kötelező naplózást alkalmazni, melynek a rendszer jellegéhez igazodóan kell kialakítani, ugyanakkor legalább rögzíteni kell azokat az eseményeket, amelyek alapján utólag azonosíthatók a kockázatok, ellenőrizhető a rendszer működése, és támogatható a piacra kerülés utáni monitoring.

Gyakorlati értelemben ez azt jelenti, hogy a naplóknak lehetővé kell tenniük az egyes MI-döntések rekonstrukcióját (input, működési kontextus, output és szükség esetén emberi beavatkozás, illetve ennek bizonyíthatósága), így bizonyítható a rendszer kontrolláltsága és megfelelősége audit vagy incidens esetén.

AUTOMATIKUSAN GENERÁLT NAPLÓK (19. CIKK)

MI-rendszerek szolgáltatóinak legalább 6 hónapig meg kell őrizniük az adott nagy kockázatú MI-rendszereik által automatikusan generált naplókat, amennyiben az ilyen naplók ellenőrzésük alatt állnak.

ÁTLÁTHATÓSÁG ÉS TÁJÉKOZTATÁS (13. CIKK)

Az MI-rendszert úgy kell megtervezni és fejleszteni, hogy működésük kellően átlátható legyen ahhoz, hogy a felhasználók értelmezhessék a rendszer kimeneteit és megfelelően használhassák azokat.

Használati utasítást kell mellékelni, amely tömör, teljes körű, pontos és egyértelmű, a felhasználók számára releváns és legalább az alábbi információkat tartalmazza:

- szolgáltató és képviselőjének kilétére vonatkozó információk,
- MI-rendszer jellemzői, képességei és teljesítményének korlátait, teljesítménymutatókat,
- hardveres és szoftveres követelményeket,
- emberi felügyeleti intézkedéseket,
- naplózással kapcsolatos intézkedéseket.

EMBERI FELÜGYELET (14. CIKK)

A nagy kockázatú MI-rendszereket úgy kell megtervezni és fejleszteni, hogy azokat a használatuk időtartama alatt természetes személyek hatékonyan felügyelhessék.

Az emberi felügyeletnek alkalmasnak kell lennie:

- nyomon követni a működést és zavarokat, szükség esetén beavatkozni,
- automatizált torzításokra való figyelmeztetésre,
- figyelmen kívül hagyni a rendszer kimenetét vagy felülrni azt.

PONTOSSÁG, ELLENÁLLÓKÉPESSÉG ÉS KIBERBIZTONSÁG (15. CIKK)

A nagy kockázatú MI-rendszereket úgy kell megtervezni és fejleszteni, hogy megfelelő szintű pontosságot, működési folytonosságot (üzletmenet-folytonosságot) és (kiber)biztonságot biztosítsanak, továbbá, hogy e tekintetben a teljes életciklusuk során következetesen teljesítsenek.

A pontosság szintjeit meg kell határozni és mérőszámokat kell hozzájuk rendelni. Ez nem csak a szolgáltatók feladata, az EU - az érdekelt felekkel közösen - ösztönzi egy olyan metrika, metodológia kidolgozását, amely a pontosság szintjét, a mérés rendszerét meghatározza. A nagy kockázatú MI-rendszerek esetén a használati feltételek (használati utasítás) része kell legyen a pontosságot leíró metrika.

Az MI-rendszerek ellenállóképessége érdekében az üzletmenet-folytonosságot biztosító redundanciákat kell alkalmazni (pl. biztonsági mentés, hibatűrő [fail-safe] működés).

A kiberbiztonsági megoldásoknak alkalmazkodniuk kell a modellekhez (tanítóadat-készlet manipulálását megkísérlő támadásoknak (adatmérgezés, avagy data poisoning) vagy a tanítás során használt előtanított összetevők manipulálását megkísérlő támadásoknak („modellmérgezés”), a modell hibájának előidézésére szolgáló bemeneteknek (támadó szempontú példák vagy modellkijátszás), a bizalmasság elleni támadásoknak vagy a modellhibáknak a megelőzésére, felderítésére, az azokra való reagálásra, azok megoldására és ellenőrzésére irányulnak.

A fentieket figyelembe véve az MI-rendszerek szolgáltatóinak:

- a dokumentációk mellett szabályozókat kell megalkotniuk (pl. MI Szabályzat, incidenskezelési eljárásrend, fejlesztési eljárásrend, etc.),
- technikai és technológiai intézkedéseket kell bevezetniük, melyek hozzájárulnak a kockázatok csökkentéséhez és garantálják az MI-rendszerek biztonságos és ellenálló működését (pl. biztonsági mentések, naplózás és naplók megőrzése – retention time),
- működés folytonosságot biztosító intézkedéseket kell hozniuk, melyek lehetnek adminisztratív intézkedések (üzletmenet-folytonossági keretrendszer, BCP-k, DRP, valamint tesztelések), technikai intézkedések (pl. biztonsági mentések),

- monitoring folyamatokat kell kialakítaniuk, melyek a rendszerek képességeit, teljesítményét, pontosságát méri. Ezek is egyrészt adminisztratív intézkedések (pl. szabályzatok, jelentésminták), illetve technikai megoldások (pl. naplóelemzés, hálózati teljesítmény, valamint feldolgozási teljesítmény monitorozás),
- penetrációs tesztek, kódok felülvizsgálata, melyek biztosítják az MI-rendszerek ellenállóképességét a jogosulatlan hozzáférések, adatmanipuláció, adatmérgezés, valamint hibák és működési problémák vonatkozásában.

MINŐSÉGIRÁNYÍTÁSI RENDSZER (17. CIKK)

Mivel a nagy kockázatú MI-rendszerek működésükből adódóan kockázatosnak minősülnek, a jogalkotó elvárja, hogy olyan (minőség)irányítási rendszert építsen fel és működtessen a szervezet, mely biztosítja a rendszerek biztonságos és folyamatos működését. A nagy kockázatú MI-rendszerek szolgáltatóinak ezért – az ISO/IEC 42001:2023-mal paralell - minőségirányítási rendszert kell bevezetniük, mely legalább az alábbi szempontokra tér ki:

- jogszabályi megfelelés és kockázatkezelési keretrendszer,
- tervezéshez, fejlesztéshez, ellenőrzéshez kapcsolódó eljárások, tesztelési- és validálási technikák szabályozása,
- alkalmazandó műszaki előírások, szabványok megfelelésével kapcsolatos rendelkezések,
- adatgazdálkodási (data governance) szabályok,
- forgalomba hozatal követő nyomonkövetés rendszere,
- súlyos váratlan események bejelentésével kapcsolatos eljárások és hatósági kapcsolattartás rendszere,
- dokumentáció nyilvántartásának rendszere,
- erőforrásgazdálkodás,
- feladatok és felelősségek rendszere.

DOKUMENTÁCIÓ VEZETÉSE (18. CIKK)

A szolgáltatónak a nagy kockázatú MI-rendszer forgalomba hozatala vagy üzembe helyezése után 10 évig az illetékes nemzeti hatóságok számára elérhetővé kell tennie a következőket:

- Műszaki dokumentáció,
- Minőségirányítási rendszerre vonatkozó dokumentáció,
- Jóváhagyott változtatások dokumentációja,
- Kiadott határozatok és egyéb dokumentumok,
- EU-megfelelőségi nyilatkozat.

KORREKCIÓS INTÉZKEDÉSEK ÉS TÁJÉKOZTATÁSI KÖTELEZETTSÉG (20. CIKK)

A nagy kockázatú MI-rendszerek szolgáltatóinak, amennyiben úgy ítélik meg, hogy az általuk forgalomba hozott vagy üzembe helyezett MI-rendszer nem felel meg az AI Act rendelkezéseinek, azérintettek tájékoztatása mellett azonnal:

- korrekciós intézkedéseket kell tenniük vagy
- ki kell vonniuk a forgalomból / üzemen kívül kell helyezniük a rendszert

EGYÜTTMŰKÖDÉS AZ ILLETÉKES HATÓSÁGOKKAL (21. CIKK)

A nagy kockázatú MI-rendszerek szolgáltatóinak az illetékes hatóság indokolt kérésére, az érintett tagállam által megjelölt nyelven át kell adniuk az említett hatóság részére minden olyan információt és dokumentációt, amely szükséges annak igazolásához, hogy a nagy kockázatú MI-rendszer megfelel az AI Act rendelkezéseinek.

IMPORTŐRÖK KÖTELEZETTSÉGEI (23. CIKK)

Nagy kockázatú MI-rendszer forgalomba hozatala előtt az importőröknek biztosítaniuk kell, hogy a rendszer megfeleljen az AI Act-nek, legalább az alábbiak teljesítésével:

- importőr neve és kapcsolati adatai feltüntetésre kerültek,
- szolgáltató elvégezte a megfelelőségértékelési eljárást,
- rendelkezik a műszaki dokumentációval,
- feltüntették a CE jelölést,
- feltüntették az EU-megfelelőségi nyilatkozatot,
- rendelkezik használati utasítással,
- szolgáltató kinevezett egy EU területén letelepedett meghatalmazott képviselőt.

Az importőrnek 10 évig meg kell őriznie a bejelentett szervezet által kiállított tanúsítványt, a használati utasítást és az EU-megfelelőségi nyilatkozatot.

FORGALMAZÓK KÖTELEZETTSÉGEI (24. CIKK)

Nagy kockázatú MI-rendszer forgalmazását megelőzően a forgalmazóknak ellenőrizniük kell, hogy a nagy kockázatú MI-rendszer esetén rendelkezésre áll-e:

- CE jelölés,
- EU-megfelelőségi nyilatkozat
- használati utasítás,
- rendszer szolgáltatója, illetve importőre teljesítette-e az AI Act-ben foglalt egyéb szervezeti kötelezettségeit.

IMPORTŐRÖK ÉS FORGALMAZÓK (ÉRTÉKLÁNC) FELELŐSSÉGI KÖRE (25. CIKK)

Minden forgalmazót, importőrt, alkalmazót vagy egyéb harmadik felet nagy kockázatú MI-rendszer szolgáltatójának kell tekinteni, amennyiben:

- nevüket vagy védjegyüket egy már forgalomba hozott vagy üzembe helyezett, nagy kockázatú MI-rendszeren helyezik el,
- jelentős módosítást hajtanak végre egy már forgalomba hozott vagy már üzembe helyezett nagy kockázatú MI-rendszeren, úgy, hogy az nagy kockázatú MI-rendszer marad,

- jelentősen módosítják egy olyan MI-rendszer rendeltetését, ami addig nem volt nagy kockázatú, úgy, hogy az onnantól nagy kockázatú MI-rendszernek minősül.

A fentiek okán az MI-rendszert eredetileg forgalomba hozó vagy üzembe helyező szolgáltató többé nem tekinthető az adott konkrét MI-rendszer szolgáltatójának.

A NAGY KOCKÁZATÚ MI-RENDSZEREK ALKALMAZÓINAK KÖTELEZETTSÉGEI (26. CIKK)

A nagy kockázatú MI-rendszerek alkalmazóinak megfelelő technikai és szervezési intézkedéseket kell tenniük annak érdekében, hogy az MI-rendszer használata az AI Act-ben foglaltaknak megfeleljen, ne sértse az emberek jogait és szabadságát.

Ennek érdekében az alkalmazóknak az emberi felügyeletet olyan természetes személyekre kell bízniuk, akik rendelkeznek a szükséges szakértelemmel, képzéssel és hatáskörrel, valamint a szükséges támogatással.

Szükséges továbbá megőrizni a naplófájlokat, amennyiben a naplófájlok a rendelkezésükre állnak.

Nagy kockázatú MI-rendszer munkahelyi üzembe helyezése vagy használata előtt a munkáltatónak tájékoztatniuk kell az érintett munkavállalókat arról, hogy esetükben nagy kockázatú MI-rendszer használatára fog sor kerülni.

3.9. BEJELENTŐ HATÓSÁG, MEGFELELŐSÉGÉRTÉKELÉSI ELJÁRÁS

BEJELENTŐ HATÓSÁG

Az AI Act minden tagállam részére előírja, hogy állítson fel egy független, úgynevezett bejelentő hatóságot, mely képes a megfelelőségértékelő szervezeteket értékelni és nyilvántartásba venni. Ez a hatóság lehet nemzeti akkreditáló testület is.

Magyarországon a bejelentő hatóság akkreditáció alapján értékeli, kijelöli, bejelenti és felügyeli a nagy kockázatú MI-rendszerek követelményeit ellenőrző megfelelőségértékelő szervezeteket. Hazánkban a Nemzeti Akkreditáló Hatóság került kijelölésre, mint bejelentő hatóság, eljárásait a megfelelőségértékelő szervezetek tevékenységéről szóló 2009. évi CXXXIII. törvény szerint látja el.

MEGFELELŐSÉGÉRTÉKELÉSI ELJÁRÁS

A bejelentett szervezetek ellenőrzik, hogy a nagy kockázatú MI-rendszerek megfelelnek-e az AI Act-ben foglalt követelményeknek. A megfelelőségértékelési eljárásnak korábban már alávetett nagy kockázatú MI-rendszereket új megfelelőségértékelési eljárásnak kell alávetni akkor, amikor lényeges módosításon mennek keresztül. Nem minősül lényeges változásnak, ha a rendszer természetes velejárója a folyamatos tanulás.

TANÚSÍTVÁNYOK

A megfelelőségértékelési eljárás keretében tanúsítvány adható ki, mely maximum 5 évre érvényes.

MEGFELELŐSÉGÉRTÉKELÉSI ELJÁRÁSTÓL VALÓ ELTÉRÉS

Indokolt kérésre bármely piacfelügyeleti hatóság engedélyezheti adott nagy kockázatú MI-rendszerek forgalomba hozatalát vagy üzembe helyezését a közbiztonság vagy a személyek életének és egészségének védelmét, a környezetvédelmet, valamint a kulcsfontosságú ipari és infrastrukturális eszközök védelmét szolgáló rendkívüli okokból.

PIACFELÜGYELETI HATÓSÁG

Az MI-piacfelügyeleti hatósága Magyarországon a vállalkozásfejlesztésért felelős miniszter hatáskörébe tartozik, általános hatáskörű hatóságként hivatalból jár el az AI Act szerinti piacfelügyeleti ügyekben. Az MI-piacfelügyelet kizárólagos hatáskörben jár el, ha az ügyfél nem fogyasztó, és az ügy tárgya kizárólag az AI Act 3. cikk 1. pont szerinti MI-rendszer vizsgálata.

Nem tartoznak ide a pénzügyi szektor bizonyos ügyei: ha a nagy kockázatú MI-rendszer közvetlenül pénzügyi szolgáltatáshoz kapcsolódik, a felügyeletet az MNB látja el.

EU MEGFELELŐSÉGI NYILATKOZAT

A szolgáltatónak a nagy kockázatú MI-rendszerre vonatkozóan EU-megfelelőségi nyilatkozatot kell készítenie és 10 évig az illetékes nemzeti hatóság számára elérhetővé kell tennie. A megfelelőségi nyilatkozatban fel kell tüntetni, hogy az érintett nagy kockázatú MI-rendszer megfelel az AI Act követelményeinek és tartalmaznia kell a meghatározott információkat. A nyilatkozatot le kell fordítani azon tagállamok nyelvére, amelyekben a nagy kockázatú MI-rendszert forgalomba hozták vagy forgalmazzák.

CE JELÖLÉS

A CE-jelölést a nagy kockázatú MI-rendszerek esetében jól láthatóan, olvashatóan és eltávolíthatatlan módon kell elhelyezni. Amennyiben a nagy kockázatú MI-rendszer jellege miatt ez nem lehetséges vagy nem indokolt, a jelölést a csomagoláson vagy adott esetben a kísérő dokumentáción kell feltüntetni. Elhelyezhető digitálisan is, ha a termék jellege ezt indokolja.

REGISZTRÁCIÓ

Az AI Act III. mellékletben felsorolt nagy kockázatú MI-rendszer forgalomba hozatala vagy üzembe helyezése előtt a szolgáltatónak saját magát és a rendszerét regisztrálnia kell az EU-s adatbázisban.

3.10. ÁTLÁTHATÓSÁGI KÖVETELMÉNYEK

Vannak olyan, a nagy kockázatú MI-rendszereknél jóval alacsonyabb kockázati szintként értékelt rendszerek, melyeknek nem kell megfelelniük a fenti követelményeknek, azonban a jogalkotó mégis úgy döntött, hogy bizonyos átláthatósági követelményeket támaszt velük szemben. Az átláthatósági követelmények a következők:

- A természetes személyekkel közvetlen interakcióra szánt MI-rendszernek legkésőbb az első interakció vagy kitettség alkalmával tájékoztatniuk kell a használót, hogy MI-rendszerrel állnak interakcióban.
- A hang-, kép-, video- vagy szöveges tartalmat létrehozó MI-rendszerek szolgáltatóinak biztosítaniuk kell, hogy az MI-rendszer kimenetei mesterségesen létrehozottként vagy manipuláltként észlelhetők legyenek.
- Az érzelemfelismerő rendszer vagy a biometrikus kategorizálási rendszer – amennyiben nem minősül tiltott tevékenységnek – alkalmazóinak tájékoztatniuk kell a rendszer működéséről a személyeket, akik a rendszer működésének ki vannak téve, valamint az adatkezelésnek meg kell felelnie a GDPR-nak.

- A deepfake kép-, hang- vagy videotartalom létrehozására alkalmas MI-rendszereknek közölniük kell, hogy a tartalmat mesterségesen hozták létre vagy manipulálták.

3.11. FORGALOMBA HOZATAL UTÁNI NYOMONKÖVETÉS, INCIDENTSEK JELENTÉSE ÉS PIACFELÜGYELET

NYOMONKÖVETÉSI RENDSZER

A szolgáltatóknak a forgalomba hozatal után gyűjteniük kell az MI-rendszerek teljesítményére vonatkozó releváns adatokat.

SÚLYOS VÁRALTAN ESEMÉNYEK BEJELENTÉSE

Az EU-ban forgalomba hozott nagy kockázatú MI-rendszerek szolgáltatóinak minden súlyos váratlan eseményt azonnal, de legkésőbb a tudomásra jutást követő 10/15 napon (függően az eseménytől) belül be kell jelenteniük a piacfelügyeleti hatóságainak, ahol az esemény történt.

3.12. ÁLTALÁNOS CÉLÚ MI-MODELLEK ÉS KAPCSOLÓDÓ KÖTELEZETTSÉGEK

Általános célú MI-modell: olyan MI-modell - ideértve azt is, amikor az ilyen MI-modell tanítása nagy adatmennyiséggel, nagy léptékű önfelügyelet mellett történik -, amely jelentős általánosságot mutat, és forgalomba hozatalának módjától függetlenül, különféle feladatok széles körének elvégzésére képes, valamint többféle downstream rendszerbe vagy alkalmazásba integrálható, azon MI-modellek kivételével, amelyeket a forgalomba hozatalukat megelőzően kutatási, fejlesztési vagy prototípus-alkotási tevékenységekre használnak.

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.

AZ ÁLTALÁNOS CÉLÚ MI-MODELLEK SZOLGÁLTATÓIRA VONATKOZÓ KÖTELEZETTSÉGEK

A szolgáltatók kötelezettségei:

- folyamatosan frissített műszaki dokumentáció,
- eljárások a szellemi tulajdonjogokra, szerzői és kapcsolódó jogokra vonatkozólag, amennyiben az beépíthető más rendszerekbe is,
- összefoglaló a tanítási tartalomról.

RENDSZERSZINTŰ KOCKÁZATOT JELENTŐ ÁLTALÁNOS CÉLÚ MI-MODELLEK SZOLGÁLTATÓIRA VONATKOZÓ KÖTELEZETTSÉGEK

Rendszerszintű kockázat: az általános célú MI-modellek nagy hatású képességeire jellemző kockázat, amely - a modellek jelentős elterjedtsége miatt, vagy a népegészségre, a biztonságra, a közbiztonságra, az alapvető jogokra vagy a társadalom egészére gyakorolt tényleges vagy észszerűen előrelátható negatív hatások révén - olyan jelentős hatást gyakorol az uniós piacra, amely nagy léptékben továbbterjedhet az értékláncban.

A szolgáltatók kötelezettségei:

- folyamatosan frissített műszaki dokumentáció,
- eljárások a szellemi tulajdonjogokra, szerzői és kapcsolódó jogokra vonatkozólag, amennyiben az beépíthető más rendszerekbe is,
- összefoglaló a tanítási tartalomról,
- modellértékelés a rendszerszintű kockázatok azonosítása és enyhítése céljából,
- a fejlesztéséből, forgalomba hozatalából vagy használatából eredő lehetséges, kockázatok csökkentése,
- nemzeti hatóságok részére a súlyos váratlan események jelentése,
- megfelelő szintű kiberbiztonsági védelem az MI-modell és a modell fizikai infrastruktúrája számára.

3.13. MI SZABÁLYOZÓI TESZTKÖRNYEZET

Minden tagállamnak 2026. augusztus 2-áig MI tesztkörnyezetet kell létrehoznia, ahol a leendő szolgáltatók a modelljeik fejlesztését, tanítását, tesztelését, valamint a minőségértékelési- és piacfelügyeleti szervezetek az eljárást elvégezhetik.

Unióban székhellyel vagy fiókteleppel rendelkező kkv-k, köztük az induló innovatív vállalkozások számára elsőbbségi hozzáférést biztosítanak az MI szabályozói tesztkörnyezetekhez.

3.14. ILLETÉKES NEMZETI HATÓSÁGOK

Minden tagállam legalább egy bejelentő hatóságot és legalább egy piacfelügyeleti hatóságot kell létrehoznia. Hazánkban a két hatóság:

- Bejelentő hatóság: Nemzeti Akkreditáló Hatóság
- Piacfelügyeleti hatóság (általánosságban): Vállalkozásfejlesztésért felelős miniszter (Gazdasági és Energetikai Miniszter)
- Piacfelügyeleti hatóság (pénzügyi ágazatban): Magyar Nemzeti Bank

3.15. SZANKCIÓK AZ AI ACT SZERINT

A tagállamok felelőssége is a szankciókra és egyéb végrehajtási intézkedésekre vonatkozó szabályok megalkotása, de vannak az AI Act-ben is, a GDPR-hoz hasonlóan meghatározott tételek:

- MI-gyakorlatok tilalmának be nem tartása legfeljebb 35 millió euró összegű, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 7%-át kitevő összegű közigazgatási bírsággal sújtandó, a kettő közül a magasabb összegűt figyelembe véve,

- az MI-rendszer nem felel meg a következő rendelkezések bármelyikének, az legfeljebb 15 millió euró összegű, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 3%-át kitevő összegű közigazgatási bírsággal sújtandó, a kettő közül a magasabb összegűt figyelembe véve,
- helytelen, hiányos vagy félrevezető információ szolgáltatása történik, az legfeljebb 7,5 millió euró összegű, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 1%-át kitevő összegű közigazgatási bírsággal sújtandó, a kettő közül a magasabb összegűt figyelembe véve.

AZ ÁLTALÁNOS CÉLÚ MI-MODELLEK SZOLGÁLTATÓIRA KISZABOTT PÉNZBÍRSÁGOK

Az előző pénzügyi évben az éves teljes globális árbevételük legfeljebb 3%-át kitevő összegű vagy legfeljebb 15 millió euró összegű pénzbírságot szabhat ki, a kettő közül a magasabb összegűt figyelembe véve, amennyiben a Bizottság megállapítja, hogy a szolgáltató szándékosan vagy gondatlanságból megsértette az AI Act rendelkezéseit, nem tett eleget a tájékoztatási vagy dokumentálási kötelezettségének vagy nem biztosít hozzáférést az MI-modellhez.

3.16. SZANKCIÓK RENDSZERE MAGYARORSZÁGON

A piacfelügyelet az a hatósági tevékenység, amelynek célja annak ellenőrzése, hogy a Magyarországon forgalomba hozott, üzembe helyezett vagy alkalmazott mesterségesintelligencia-rendszerek megfelelnek-e az AI Act és a kapcsolódó hazai szabályozás előírásainak. A piacfelügyeleti eljárás nem a technológia fejlesztésére, hanem annak jogszerű és biztonságos használatára, forgalmazására és működtetésére irányul. Ennek keretében a hatóság azt vizsgálja, hogy az adott MI-rendszer teljesíti-e a rá vonatkozó követelményeket, nem sérti-e az alapvető jogokat, és nem jelent-e indokolatlan kockázatot a felhasználókra, a fogyasztókra vagy a társadalom egészére nézve.

A piacfelügyeleti hatóság feladata alapvetően az AI Act-ben részletezett előírások betartásának ellenőrzése, vagyis azt felügyeli, hogy az érintett szereplők (szolgáltatók, alkalmazók, importőrök, azok meghatalmazott képviselői vagy bizonyos termékgyártók) betartják-e a rendelet rájuk vonatkozó kötelezettségeit. Az eljárás kiterjed az AI Act 99. cikke szerinti szankciók alkalmazására az említett szereplők jogsértése esetén.

A piacfelügyeleti hatóság a magyar törvény alapján az eljárás végén három fő dolgot tehet:

- közigazgatási bírságot szabhat ki,
- megállapíthatja az MI-rendszer jogellenes alkalmazását, illetve
- felhívhatja az érintettet a jogellenes magatartás megszüntetésére vagy a jogszerű állapot helyreállítására.

Vagyis nemcsak pénzbírságot alkalmazhat, hanem kötelezheti is az érintettet a szabálytalanság kijavítására.

A szankciók tekintetében a Korm. rendelet kimondja, hogy az AI Act-ben euróban meghatározott bírságmaximumokat forintban kell alkalmazni. Ennek megfelelően a legmagasabb figyelembe veendő összegek a következők:

AI Act	Szabálytalanság	Bírságtétel
99. Cikk (3) bek.	Amennyiben valaki az AI Act által tiltott MI-gyakorlatokat sérti meg, tehát tiltott MI gyakorlatot alkalmaz: például manipulatív vagy megtévesztő MI használat, sérülékeny csoportok kihasználása, társadalmi pontozás (social scoring), profilozás alapú bűnisméltés-előrejelzés, vagy biometrikus adatbázisok tömeges (scraping alapú) építése valósul meg.	13 300 000 000 forint, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 7 %-át kitevő összegű közigazgatási bírsággal sújtandó, a kettő közül a magasabb összegűt figyelembe véve.
99. Cikk (4) bek.	Amennyiben valaki nagy kockázatú MI-rendszerre vonatkozó kötelezettségét sértette meg az importőr, forgalmazó, üzemeltető vagy intergátor: például nem végezte el a kockázatelemzést, nem működtet kockázatkezelési keretrendszer vagy nem tesz eleget a felhasználók tájékoztatásának.	5 700 000 000 forint, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 3 %-át kitevő összegű közigazgatási bírsággal sújtandó, a kettő közül a magasabb összegűt. Itt több rényezőt mérlegel a hatóság.
99. Cikk (5) bek.	Amennyiben valaki a bejelentett szervezetek vagy az illetékes nemzeti hatóságok kérésére válaszul helytelen, hiányos vagy félrevezető információ szolgáltatást ad: például az MI-rendszer képeeségeire, működésére vagy kockázati besorolására vonatkozóan hamisan nyilatkozik felhívásra.	2 850 000 000 forint, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 1 %-át kitevő összegű közigazgatási bírsággal sújtandó, a kettő közül a magasabb összegűt figyelembe véve.

3.17. ALKALMAZHATÓVÁ VÁLÁS („HATÁLYBA LÉPÉS”)

Az AI Act lépcsőzetesen, négy lépésben válik alkalmazandóvá, minden lépcsőfokhoz különböző megfelelőségi követelményeket társítva. Figyelembe véve a Digital Omnibus / Omnibus VII elfogadott javaslatot, jelölésre kerül az eredeti, illetve a módosított alkalmazhatósági dátum.

Terület	Eredeti dátum	Módosított dátum
MI generált tartalom jelölési követelményei	2026. augusztus 2.	2026. december 2.
Önálló magas kockázatú MI-rendszerek	2026. augusztus 2.	2027. december 2.
Termékekbe beágyazott magas kockázatú MI-rendszerek	2027. augusztus 2.	2028. augusztus 2
Nemzeti sandboxok nemzeti szintű létrehozása	2026. augusztus 2.	2027. augusztus 2.

AZ AI ACT ÉS A HAZAI SZABÁLYOZÁS KAPCSOLATA

Mivel az AI Act rendeleti szintű, így minden EU-s tagállamban közvetlenül alkalmazandó, nem szükséges átültetni a nemzeti jogrendszerbe – ellenben például a NIS 2 irányelvvel –, a nemzeti jogalkotóknak azonban van feladata, többek között a hatóságok kijelölése és a hatósági eljárások rendszerének szabályozása. A magyar jogalkotó feladata ezért elsősorban nem egy teljesen önálló szabályrendszer kialakítása volt, hanem annak biztosítása, hogy az AI Act rendelkezései Magyarországon is intézményi, eljárási és piacfelügyeleti szempontból végrehajthatók legyenek.

Ezt a célt szolgálják a hazai végrehajtási szabályok, különösen a 2025. évi LXXV. törvény és az ahhoz kapcsolódó végrehajtási rendeletek.

A 2025. évi LXXV. törvény jelöli ki az EU AI Act hazai végrehajtásának kereteit, meghatározza:

- a kijelölt hatóságokat,
- az eljárási rendet és
- a szankciók rendszerét.

A felügyelet hatálya kiterjed a Magyarországon forgalomba hozott vagy üzembe helyezett MI-rendszerekre, valamint az ilyen rendszerek kimenetének belföldi felhasználására is.

A pénzügyi szektor külön szabályozási ágat képez, ahol a piacfelügyeleti feladatokat az MNB gyakorolja. A törvény létrehozta a Magyar Mesterséges Intelligencia Tanácsot, és megteremti az MI szabályozói tesztkörnyezet (sandbox) hazai kereteit.

4.1. HATÓSÁGOK

A MI bejelentő hatóság és az MI piacfelügyeleti hatóság kijelölését a 344/2025. (X.31.) Korm. rendelet 1. § (1) bekezdése tartalmazza. Az MI-piacfelügyelet országos illetékességgel látja el az AI Act 70. cikke szerinti egyedüli kapcsolattartó pontot, és a szabályozói tesztkörnyezetet (sandboxot) is.

BEJELENTŐ HATÓSÁG

A bejelentő hatóság akkreditáció alapján értékeli, kijelöli, bejelenti és felügyeli a nagy kockázatú MI-rendszerek követelményeit ellenőrző megfelelőségértékelő szervezeteket. A kijelölésre és e szervezetek tevékenységére a 2009. évi CXXXIII. törvény (Msztv.) szabályai irányadók. A kérelemhez a kérelmező alkalmasságának Msztv. szerinti igazolása szükséges.

PIACFELÜGYELETI HATÓSÁG

Az MI-piacfelügyeleti hatósága a vállalkozásfejlesztésért felelős miniszter (Gazdasági és Energetikai Miniszter) hatáskörébe tartozik, általános hatáskörű hatóságként hivatalból jár el az AI Act szerinti piacfelügyeleti ügyekben. Az MI-piacfelügyelet kizárólagos hatáskörben jár el, ha az ügyfél nem fogyasztó, és az ügy tárgya kizárólag az AI Act szerinti MI-rendszer vizsgálata.

Nem tartoznak ide a pénzügyi szektor bizonyos ügyei: ha a nagy kockázatú MI közvetlenül pénzügyi szolgáltatáshoz kapcsolódik, a felügyeletet az MNB látja el.

EGYEDÜLI KAPCSOLATTARTÓ PONT

Az egyedüli kapcsolattartó pont a tagállam által kijelölt központi kapcsolattartó szerv, amely az AI Act végrehajtásával összefüggő ügyekben összefogja a nemzeti hatósági kapcsolattartást, és kapcsolatot tart az Európai Bizottsággal, a többi tagállam illetékes hatóságaival, valamint az érintett hazai szereplőkkel.

ÁGAZATI PIACFELÜGYELETI SZAKHATÓSÁGI FELADATOK

Az MI-piacfelügyeleti hatóság bizonyos esetekben nem önállóan, hanem szakhatóságként vesz részt az eljárásban. Erre akkor kerül sor, ha az MI-rendszer olyan ágazatban kerül forgalomba hozatalra vagy üzembe helyezésre, amelynek piacfelügyeletét egyébként külön hatóság látja el.

AZ MI SZABÁLYOZÓI TESZTKÖRNYEZET (SANDBOX)

Az MI-piacfelügyeleti hatóság hozza létre és működteti az MI szabályozói tesztkörnyezetet, azaz a sandboxot. Ez olyan szabályozott és felügyelt tesztelési környezetet jelent, amelyben az új mesterségesintelligencia-rendszerek fejlesztése és kipróbálása a hatóság szakmai támogatása mellett, a vonatkozó jogi és biztonsági követelmények figyelembevételével történhet. A működés részleteit a miniszter rendeletben állapítja meg, és a működtetéshez állami nagy teljesítményű számítástechnikai kapacitásból elkülönített erőforrás is biztosítható.

KAPCSOLAT

Az AI Act követelményeinek való megfelelés nem csupán jogszabályi kérdés, hanem a felelős AI-alkalmazás és a hatékony vállalatirányítás alapja is.

Amennyiben szervezetének támogatásra van szüksége az AI Act értelmezésében, a megfelelési felkészülésben vagy az AI irányítási folyamatok kialakításában, szakértőink készséggel állnak rendelkezésére.

Vegye fel velünk a kapcsolatot, és segítünk felkészíteni szervezetét az AI Act követelményeire.

Black Cell Hungary Zrt.

www.blackcell.io

compliance@blackcell.io