1. MELLÉKLET

a Mesterséges Intelligencia Használati Szabályzathoz

MI-eszközök engedélyezési minimumkövetelményei

Kötelező ellenőrzési szempontrendszer és értékelési keretrendszer

A melléklet célja és kötelező jellege

Az intézményben kizárólag olyan MI-eszköz alkalmazható tanulókat vagy munkatársakat érintő folyamatban, amelynek vonatkozásában az alábbi hat ellenőrzési területen dokumentált megfelelőség igazolható. Az ellenőrzés elvégzése az igazgató felelőssége, amelyet az MI-felelős bevonásával, szükség esetén az adatvédelmi tisztviselő közreműködésével kell lefolytatni.

Jelen melléklet a MI Használati Szabályzat 2.3–2.4. és 10.3. pontjaihoz, valamint az MI Etikai Irányelv 3.3. és 4.3. pontjaihoz kapcsolódik.

Bevezető rendelkezések

Az Európai Unió mesterséges intelligenciáról szóló rendelete (EU AI Act, 2024/1689) és a GDPR (2016/679) rendelkezései alapján az oktatási intézmények kötelesek az általuk alkalmazott MI-eszközök kockázatát felmérni, és biztosítani, hogy e rendszerek használatával az érintett személyek – különösen kiskorú tanulók – jogai ne sérüljenek. Ennek teljesítésére szolgál az alábbi, kötelező érvényű ellenőrzési szempontrendszer.

Az intézményvezető minden egyes MI-eszköz intézményi bevezetése vagy meghosszabbítása előtt köteles elvégeztetni a jelen mellékletben rögzített hat ellenőrzési területre kiterjedő felülvizsgálatot. Az ellenőrzés eredményét az intézményi irattárban legalább 5 évig meg kell őrizni.

Figyelem – bevezetési tilalom:
Amennyiben az alábbi hat terület bármelyikén az ellenőrzés negatív eredménnyel zárul, az MI-eszköz az intézményi folyamatokban NEM alkalmazható mindaddig, amíg a hiányosság felszámolásra nem kerül, vagy az eszközt egy megfelelő alternatíva nem váltja ki.

Az ellenőrzési eljárás szabályai

Az ellenőrzést az MI-felelős végzi el, és az eredményt a jelen melléklet végén található összesítő ellenőrzési lapon dokumentálja. Amennyiben az eszköz személyes adatokat kezel, az adatvédelmi tisztviselő (DPO) bevonása kötelező. Az elvégzett ellenőrzést az igazgató hagyja jóvá.

Az ellenőrzés esetei:

- új MI-eszköz bevezetése előtt,
- meglévő MI-eszköz megújítása (szerződés, licenc meghosszabbítása) előtt,
- az eszköz adatkezelési feltételeinek változásakor,
- legalább évente egyszer, az éves szabályzati felülvizsgálattal egyidejűleg.

Az ellenőrzés forrásai:

- A szolgáltató nyilvánosan elérhető adatkezelési tájékoztatója és általános szerződési feltételei (ÁSZF),
- Oktatási intézmények számára esetlegesen elérhető külön szerződéses garancia (Data Processing Agreement – Adatfeldolgozói Megállapodás),
- A szolgáltató biztonsági tanúsítványai (pl. ISO 27001, SOC 2),
- Más intézmények tapasztalatai, fenntartói ajánlások,
- Saját tesztelési tapasztalatok.

1. ellenőrzési terület

Adatkezelési feltételek és adatvédelmi tájékoztató megfelelősége

Az adatvédelmi tájékoztató az MI-eszközök legfontosabb nyilvános dokumentuma. Meglétéből és tartalmából következtetni lehet arra, hogy a szolgáltató mennyire veszi komolyan a felhasználók – köztük kiskorúak – adatainak védelmét. Nem elegendő, ha a tájékoztató létezik: tartalmának érthetőnek, naprakésznek és jogszerűnek kell lennie.

Mit kell ellenőrizni?

1.1 Az adatkezelési tájékoztató elérhetősége

A tájékoztatónak az eszköz főoldaláról legfeljebb két kattintással hozzáférhetőnek kell lennie. Ha a tájékoztató elérése nehézkes, maga ez a tény is kockázatjelző.

- Elérhető-e a tájékoztató közvetlenül a szolgáltató weboldaláról, regisztráció nélkül?
- Magyar vagy az EU valamely hivatalos nyelvén is hozzáférhető-e?
- Tartalmaz-e dátumot, amely alapján megállapítható, mikor frissítették utoljára?

1.2 A GDPR-megfelelőség

Az EU polgárainak adatait kezelő bármely rendszerre vonatkozik a GDPR, függetlenül attól, hogy a szolgáltató székhelye hol van. Az intézménynek meg kell győződnie arról, hogy a szolgáltató ezt elismeri és betartja.

- Hivatkozik-e a tájékoztató kifejezetten a GDPR-ra, az EU AI Act-re, vagy más, az intézményre is vonatkozó jogszabályra?
- Megnevezi-e az adatkezelő szervezet pontos nevét, székhelyét, elérhetőségét?
- Tartalmaz-e információt az adatkezeléssel kapcsolatos érintetti jogokról (hozzáférés, törlés, tiltakozás)?
- Van-e az EU területén bejegyzett képviselő, ha a szolgáltató nem EU-székhelyű?

1.3 Adatfeldolgozói megállapodás

A személyes adatok MI eszközbe történő továbbítása esetén a szolgáltató és az intézmény között adatfeldolgozói jogviszony jön létre, amely kötelező írásbeli megállapodást von maga után.

- Ajánl-e a szolgáltató Adatfeldolgozói Megállapodást (Data Processing Agreement)?
- Tartalmaz-e az intézményi vagy oktatási szektornak szóló külön feltételrendszert?
- Az esetleges alvállalkozók (al-adatfeldolgozók) listája megismerhető-e?

Határeset – elfogadható kockázattal alkalmazható eszközök feltétele:

Ha az eszköz ingyenes, nyilvánosan elérhető fogyasztói szolgáltatás (pl. webes chatbot), amelybe személyes adatot az intézmény szervezett módon NEM visz be, és a tanulók kizárólag anonimizált, általános feladatokra használják, a fenti követelmények egy része elengedhető – de az anonimizálás megtartásáról és az életkori korlátokról külön meg kell győződni (lásd 3. terület).

Ellenőrzési kérdőív – 1. terület

Ellenőrzési szempont	Teljesítve	Megjegyzés
Az adatkezelési tájékoztató az eszköz főoldaláról könnyen elérhető, regisztráció nélkül.	☐	
A tájékoztató naprakész és tartalmazza a legutóbbi frissítés dátumát.	☐	
A tájékoztató hivatkozik a GDPR-ra és az EU AI Act-re.	☐	
Az adatkezelő szervezet azonosítható (név, székhely, elérhetőség).	☐	

Az érintetti jogok (hozzáférés, törlés, tiltakozás) egyértelműen szerepelnek.	☐	
Nem EU-s székhelyű szolgáltató esetén EU-s képviselő megjelölése megtörtént.	☐	
Adatfeldolgozói megállapodás (DPA) elérhető és az intézménnyel megköthető.	☐	

2. ellenőrzési terület

A személyes adatok kezelésének jogalapja és adattakarékossága

A GDPR 5. cikke szerint az adatkezelés alapelveinek részét képezi a célhoz kötöttség és az adattakarékosság. Egy MI-eszköz vonatkozásában ez azt jelenti: az eszköz kizárólag azt az adatot kérheti be és tárolhatja, amely az adott funkció ellátásához feltétlenül szükséges. Az oktatási környezetben különösen szigorúan kell érvényesíteni ezt az elvet, mivel a felhasználók egy része kiskorú.

Mit kell ellenőrizni?

2.1 Milyen adatokat gyűjt az eszköz?

Az adatkezelési tájékoztatónak, illetve az eszköz regisztrációs folyamatának egyértelmű információt kell nyújtania arról, hogy pontosan milyen adatokat kezel a rendszer. Figyelmeztető jel, ha erről az eszköz nem ad tájékoztatást

- Megnevezi-e a tájékoztató, milyen kategóriájú adatokat kezel (pl. e-mail cím, IP-cím, gépelési viselkedés, feltöltött tartalom)?
- Tartalmaz-e a rendszer a feladathoz szükségtelen adatbekérést (pl. életkor, nem, tartózkodási hely kötelező megadása)?
- Gyűjt-e az eszköz metaadatokat (pl. gépelési sebesség, munkamenetek hossza, kattintások) a felhasználó tudta nélkül?

2.2 A jogalap azonosítása

Minden egyes adatkezelési célhoz azonosítható jogalapra van szükség. Oktatási intézményi kontextusban a hozzájárulás, mint jogalap esetében kiemelt gondossággal kell eljárni, különösen kiskorú felhasználók esetén (lásd 3. terület).

- Rögzíti-e a tájékoztató, milyen GDPR szerinti jogalapra (hozzájárulás, szerződés, jogos érdek, jogi kötelezettség) támaszkodik az adatkezelés?
- Amennyiben jogos érdekre hivatkoznak, el tudja-e az intézmény dönteni, hogy az valóban arányos-e a tanulói érdekekhez képest?
- Ha hozzájárulás a jogalap: az valóban önkéntes, megfelelő tájékoztatáson alapuló, konkrét és bármikor visszavonható-e?

2.3 Adatmegőrzési idők

Az MI-rendszerek esetében különösen fontos, hogy a bevitt adatok tárolási ideje ne legyen határozatlan időtartamú. Az eszközbe feltöltött tartalmak (pl. szövegek, kérdések) törlésének feltételeit egyértelműen rögzíteni kell.

- Meghatározza-e a tájékoztató az adatok megőrzési idejét, vagy az automatikus törlés feltételeit?
- Van-e lehetőség a felhasználói adatok és korábbi munkamenetek manuális törlésére?
- Ha az adatokat a saját modelltréninghez is felhasználják, a törlési kérelem érinti-e ezeket is?

Helyes intézményi gyakorlat:

Az intézmény belső szabályzatában rögzíti, hogy az oktatók és tanulók MI-eszközbe kizárólag anonimizált, személyes azonosítókat nem tartalmazó szöveget vihetnek be. Neveket, tanulói azonosítókat, osztálynaplóból kivont adatokat tilos közvetlenül MI-chatbotba másolni.

Ellenőrzési kérdőív – 2. terület

Ellenőrzési szempont	Teljesítve	Megjegyzés
A tájékoztató megnevezi, milyen adatkategóriákat kezel a rendszer.	☐	
Az adatkezelés célja és jogalapja minden adattípusnál meghatározott.	☐	
Az eszköz nem kér be feladatához szükségtelen személyes adatot.	☐	
Az adatmegőrzési idők meghatározottak, az eszköz nem tárol adatokat határozatlan ideig.	☐	
A felhasználói adatok és munkamenetek manuálisan törölhetők.	☐	
A rendszer beállításaiban kikapcsolható az automatikus adatgyűjtés / analitika.	☐	

3. ellenőrzési terület

Kiskorú felhasználókra vonatkozó korlátozások és hozzájárulási feltételek

Az oktatási intézmény különleges felelősséggel bír a kiskorú tanulók digitális védelméért. A legtöbb fogyasztói MI-eszköz 13 vagy 16 éves korosztály alatti felhasználókat kizár a felhasználási feltételekből. Az intézménynek ezt aktívan ellenőriznie és dokumentálnia kell; nem elegendő a tanuló felelőssége típusú megközelítés.

Mit kell ellenőrizni?

3.1 A minimális életkori határ

Szinte minden nagy MI-szolgáltató felhasználási feltételei rögzítik a minimálisan szükséges életkort. Ez Európában a GDPR 8. cikke alapján tipikusan 16 év (egyes tagállamokban 13 év, Magyarországon 16 év az irányadó korhatár a hozzájárulás-alapú adatkezeléshez). Amennyiben az intézmény az MI-eszköz általános életkori korlátozásaitól iskolai fiókok használatával kíván eltérni, azt kizárólag egy erre kifejezetten felhatalmazó oktatási szerződés keretein belül teheti meg.

- Rögzíti-e a felhasználási feltétel, hogy az eszköz milyen életkortól használható önállóan?
- Összeegyeztethető-e az eszköz használatához előírt életkori korhatár az érintett tanulói korcsoporttal?
- Rendelkezik-e az eszköz olyan kifejezett oktatási vagy intézményi fiókkezelési megoldással, amely lehetővé teszi az életkori feltételek szabályszerű betartását?

3.2 Gondviselői/törvényes képviselői hozzájárulás

Amennyiben 16 év alatti tanuló személyes adatainak kezelésére kerül sor, a GDPR 8. cikke alapján a szülői felügyeleti jog gyakorlójának (gondviselő) hozzájárulása szükséges. Az intézménynek dokumentálnia kell, hogyan szerezte meg és hogyan tárolja ezeket a hozzájárulásokat.

- Van-e az intézménynek kialakított eljárásrendje a gondviselői hozzájárulás megszerzésére és nyilvántartására?
- Az eszköz hozzájárulás-kezelő mechanizmusa lehetővé teszi-e az intézményi nyilvántartást?
- Visszavonható-e a hozzájárulás, és ennek mi a menete?

3.3 Gyermekbarát adatkezelési elvek

Az EU AI Act és a Digital Services Act alapján a kiskorú felhasználókat fokozott védelemben kell részesíteni. Különösen aggályos, ha az eszköz profilozást, célzott ajánlásokat vagy manipulatív tervezési mintákat (ún. sötét tervezési elemek) alkalmaz.

- Az eszköz adatkezelési elvei kiterjednek-e kifejezetten a gyermek felhasználókra vonatkozó többletgaranciákra?
- Alkalmaz-e az eszköz személyre szabott ajánlásokat, amelyek a tanuló korábbi viselkedésén alapulnak?

- Mentes-e az eszköz olyan tervezési elemektől, amelyek a tanulókat folyamatos, intenzív használatra ösztönzik (pl. értesítési ösztönzők, pontozási rendszerek)?

Fontos figyelmeztetés:
Amennyiben az eszköz felhasználási feltételei 18 éves korhatárt írnak elő, az intézmény 18 év alatti tanulói számára a használat nem engedélyezhető – sem oktatói közreműködéssel, sem egyéb módon. Ez alól kizárólag az jelent kivételt, ha a szolgáltató olyan kifejezett intézményi vagy oktatási fiókkezelési megoldást biztosít, amely megteremti a jogszerű alkalmazás kereteit.

Ellenőrzési kérdőív – 3. terület

Ellenőrzési szempont	Teljesítve	Megjegyzés
A felhasználási feltétel tartalmaz minimális életkori követelményt.	☐	
A tanulók életkora megfelel az eszköz felhasználási feltételeiben rögzített korhatárnak, vagy az intézmény oktatási szerződéssel rendelkezik.	☐	
16 év alatti tanulók esetén gondviselői hozzájárulás megszerzésének eljárásrendje dokumentált.	☐	
Az eszköz nem alkalmaz személyre szabott ajánlást kiskorú felhasználókra vonatkozóan.	☐	
Az eszköz nem tartalmaz manipulatív, addiktív tervezési elemeket.	☐	
A hozzájárulás visszavonásának menete a gondviselők és tanulók számára ismert.	☐	

4. ellenőrzési terület

Az adatok modelltréning célú felhasználásának szabályozottsága

Az egyik legtöbb visszaélési lehetőséget rejtő terület, amelyre a legtöbb felhasználó nem figyel: a beírt szövegek, feltöltött dokumentumok, kérdések és válaszok egy részét egyes MI-szolgáltatók saját modelljeik további betanítására (tréningjére) fordítják. Oktatási intézményi kontextusban ez elfogadhatatlanul magas kockázatot jelent, különösen, ha a tartalomba tanulói adatok, vizsgafeladatok vagy belső információk kerülnek.

Mit kell ellenőrizni?

4.1 Alapbeállítás – tréning be- vagy kikapcsolt?

Számos szolgáltató alapértelmezés szerint engedélyezi az adatok modelltréning célú felhasználását, de lehetőséget ad annak letiltására. Az intézménynek ellenőriznie kell, hogy ez az opció alapértelmezetten be vagy ki van-e kapcsolva, és szükség esetén le kell tiltania.

- Az eszköz alapértelmezés szerint felhasználja-e a bevitt adatokat modelltréningre?
- Van-e lehetőség az adatok tréning célú felhasználásának letiltására fiók- vagy szervezeti szinten?
- A letiltás ingyenes, vagy csak fizetős előfizetéssel érhető el?

4.2 Milyen adatok kerülnek a tréningbe?

Fontos különbséget tenni: nemcsak a szövegek tartalma, hanem a viselkedési minták (pl. javítások, újrapromptolások, visszajelzések) is felhasználhatók. A tájékoztatónak pontosan meg kell határoznia, mi kerül be a tréningadatbázisba.

- A tájékoztató pontosan meghatározza-e, milyen adatokat és milyen formában használnak fel tréningre?
- A felhasználói visszajelzések (pl. thumb up/down gombok) felhasználása a tréningben dokumentált-e?
- Az adatokat anonimizálják-e a tréning előtt, és ha igen, milyen módszerrel?

4.3 Törlési igény és a tréningre már felhasznált adatok

Kritikus kérdés: ha a tanuló vagy az intézmény törlési kérelmet nyújt be, az érinti-e a modellbe már bekerült adatokat? Technikai szempontból a modern gépi tanulási modelleknél ez rendkívül összetett kérdés, amelyet a szolgáltatónak egyértelműen kell kezelnie.

- A törlési igény (GDPR 17. cikk) kiterjed-e a tréningadatbázisba bekerült adatokra?
- Ha az adatok már bekerültek a modellbe, a szolgáltató milyen garanciát vállal azok eltávolítására?

Az intézményi biztonságos megközelítés:
Ha az eszköz modelltréning célú adatfelhasználása nem zárható ki egyértelműen és dokumentálhatóan, az eszközt kizárólag teljesen anonimizált, személyes adatot nem tartalmazó tartalomra szabad alkalmazni. Vizsgafeladatokat, tanulói azonosítókat, minősítési anyagokat tilos bevinni az ilyen eszközbe.

Ellenőrzési kérdőív – 4. terület

Ellenőrzési szempont	Teljesítve	Megjegyzés
A tájékoztató egyértelműen rögzíti, felhasználja vagy nem használja fela bevitt adatokat modelltréningre.	☐	
Szervezeti szinten letiltható az adatok tréning célú felhasználása.	☐	
A tiltás az alapértelmezett beállítás, vagy könnyen aktiválható.	☐	
A tréningbe kerülő adattípusok pontosan meghatározottak.	☐	
A törlési kérelem a tréningadatbázisra is kiterjed.	☐	
Oktatási szerződés esetén a tréning teljes tiltása szerződésileg rögzített.	☐	

5. ellenőrzési terület

Hozzáférés-kezelési és naplózási lehetőségek

A szervezeti MI-használat csak akkor ellenőrizhető és irányítható felelősen, ha az intézménynek lehetősége van arra, hogy a hozzáféréseket kezelje és a tevékenységeket naplózza. Egy olyan eszköz, amelynek nincs szervezeti szintű adminisztrációja, nem alkalmas intézményi folyamatokba való integrálásra – különösen, ha személyes adatokkal kerülhet kapcsolatba.

Mit kell ellenőrizni?

5.1 Szervezeti fiókkezelés (admin konzol)

Intézményi használatra csak olyan eszköz engedélyezhető, amelyhez az intézmény adminisztrátori jogkörrel rendelkező szervezeti fiókot tud létrehozni. *Az egyéni fogyasztói fiókok intézményi folyamatokban nem elfogadhatók.*

- Kínál-e a szolgáltató szervezeti (intézményi/oktatási/vállalati) fiókkezelési megoldást?
- Lehetséges-e a felhasználói fiókok központi, adminisztrátori szintű kezelése (létrehozás, törlés, jogosultságok)?
- Lehetséges-e az egyes szervezeti egységek (pl. iskolák, intézmények) szintjén külön hozzáférési politikát beállítani?

5.2 Szerepkörök és jogosultságok

A mindenki mindent lát és elér megközelítés elfogadhatatlan. Az eszköz kezelésének legyen egységes, dokumentálható struktúrája, amely az igazgató, az MI-felelős, az oktató és a tanuló szerepköreit egyértelműen elkülöníti.

- Elkülönít-e az eszköz legalább tanulói és oktatói szerepkört?
- Az adminisztrátori funkciók (pl. felhasználók listázása, statisztikák) elkülönítve érhetők-e el?

- Van-e lehetőség az egyes funkciók (pl. fájlfeltöltés, internethozzáférés) szerepkörhöz kötött engedélyezésére vagy tiltására?

5.3 Naplózás (auditnapló)

Incidens esetén az intézménynek vissza kell tudnia követni, ki, mikor, milyen adatot vitt be az eszközbe. Ehhez elengedhetetlen, hogy az eszköz részletes naplókat vezessen, amelyekhez az intézményi adminisztrátor hozzáférhet.

- Vezet-e az eszköz szervezeti szintű auditnaplót (ki, mikor, mit tett)?
- Az adminisztrátor az auditnaplóhoz hozzáférhet-e, és azt le tudja-e exportálni?
- Mennyi ideig tárolja az eszköz a naplót, és az megfelel-e az intézmény biztonsági követelményeinek?
- Konfigurálható-e a naplózás részletessége (pl. a bevitt szöveg tartalmának naplózása engedélyezhető-e adatvédelmi incidens esetén)?

5.4 Egyszeri bejelentkezés (SSO) és intézményi identitáskezelés

Amennyiben az intézmény rendelkezik Microsoft 365 Education / Google Workspace for Education vagy más szervezeti identitáskezelő rendszerrel, előnyben részesítendők az azzal integrálható MI-eszközök. Ez csökkenti az admin terhelést és növeli a biztonságot.

- Integrálható-e az eszköz az intézmény identitáskezelő rendszerével (pl. Active Directory, Azure AD, Google)?
- Lehetséges-e egyszeri bejelentkezés (SSO) az intézményi fiókkal?

Ellenőrzési kérdőív – 5. terület

Ellenőrzési szempont	Teljesítve	Megjegyzés
A szolgáltató kínál szervezeti fiókkezelési megoldást.	☐	
Lehetséges a felhasználók adminisztrátori szintű, központi kezelése.	☐	
Az eszköz legalább tanulói és oktatói szerepkört különít el.	☐	
Az adminisztrátori funkciók és adathozzáférések elkülönítve érhetők el.	☐	
Az eszköz szervezeti szintű auditnaplót vezet.	☐	
Az adminisztrátor az auditnaplóhoz hozzáférhet és azt exportálhatja.	☐	
A naplók megőrzési ideje az intézmény biztonsági követelményeinek megfelel.	☐	
Az eszköz integrálható az intézményi identitáskezelő rendszerrel (opcionális, de előnyös).	☐	

6. ellenőrzési terület

Tiltott profilozási és érzelemfelismerési funkciók kizárása

Az EU AI Act kifejezetten tiltja egyes MI-alkalmazások használatát oktatási intézményekben. E tilalmak megsértése nemcsak etikai, hanem súlyos jogi következményekkel is jár. Az intézménynek aktívan meg kell győződnie arról, hogy az alkalmazott eszköz semmilyen formában nem alkalmaz automatizált profilozást vagy érzelem-/viselkedésfelismerést tanulókon.

Mit kell ellenőrizni?

6.1 Automatizált profilozás

A GDPR 22. cikke és az EU AI Act alapján tilos olyan automatizált döntéshozatalt vagy profilozást alkalmazni, amely a tanulókat egyéni jellemzőik (pl. tanulási sebesség, hibák mintázata, viselkedés) alapján kategorizálja, és ezen alapulva hoz rájuk vonatkozó döntéseket emberi kontroll nélkül.

- Az eszköz felhasználási feltételei és tájékoztatója kizárja-e a tanulói profilok automatikus, döntéshozatali célú felépítését?

Generál-e a rendszer a tanulókról profilokat vagy kockázati besorolást anélkül, hogy az eredményeket oktató vagy szakember felülbírálná? Ha az eszköz fejlesztési javaslatokat generál a tanulóra vonatkozóan, ezek csak tájékoztató jellegűek-e, és biztosított-e, hogy a végső döntést az oktató hozza meg? **6.2 Érzelemfelismerés és biometrikus elemzés**

Az EU AI Act 5. cikke tiltja az érzelmek valós idejű automatikus felismerését oktatási és munkahelyi kontextusban. Ebbe beleértendő a kamera általi arckifejezés-elemzés, a billentyűzeti viselkedés érzelmi állapotot valószínűsítő elemzése, és egyéb biometrikus feltérképezés is.

- Az eszköz végez-e kamera- vagy hangelemzést a felhasználó érzelmi állapotának meghatározásához?
- Elemzi-e az eszköz a gépelési viselkedést, egér-mozgást vagy egyéb biometrikus jelet az érintett tudta nélkül?
- Az eszköz tájékoztatója explicit módon kizárja-e az érzelemfelismerési funkciókat?

6.3 Figyelemmonitorozás (attentiveness tracking)

Számos, elsősorban e-learning platformokhoz kapcsolódó eszköz tartalmaz figyelemmonitorozási funkciókat (pl. tekintetelemzés, aktivitásmérés). Ezek Magyarországon oktatási intézményi kontextusban csak rendkívül szigorú feltételek mellett alkalmazhatók, és alapvetően érzelemfelismerésnek minősülhetnek.

- Az eszköz alkalmaz-e figyelemmonitorozást, tekintetkövető technológiát vagy hasonló megoldást?
- Ha igen, ez a funkció alapértelmezetten ki van-e kapcsolva, és az intézményi admin le tudja-e tiltani teljeskörűen?
- Ezek a funkciók szerepelnek-e a tájékoztatóban, és van-e rájuk vonatkozó külön hozzájárulási mechanizmus?

6.4 Tanulói kockázati profilok és prediktív analitika

Egyes adaptív tanulási rendszerek prediktív modelleket alkalmaznak a tanulói lemorzsolódás előrejelzésére. Önmagában a jelzés nem tiltott, de ha ez alapján automatizált, emberi kontroll nélküli döntés születik (pl. automatikus átirányítás, értesítő küldése a gondviselőnek), az problematikus.

- Az eszköz generál-e prediktív pontszámokat vagy kockázati jelzéseket az egyes tanulókra vonatkozóan?
- Ezek kizárólag az oktató tájékoztatására szolgálnak-e, és NEM alapoznak meg automatizált döntéshozatalt?
- A tanuló és gondviselő számára átlátható-e, hogy ilyen elemzés zajlik?

Abszolút tiltás – azonnali kizárás:

Amennyiben az eszköz az alábbiak bármelyikét alkalmazza, az eszköz minden körülmények között kizárandó az intézményi használatból:

- Valós idejű érzelemfelismerés kamerakép vagy hang alapján,
- Automatikus tanulói kockázati pontszám emberi kontroll nélküli döntési célú alkalmazása,
- Szociális kreditrendszerszerű viselkedési pontszámítás,
- Titkos biometrikus adatgyűjtés a tanuló vagy gondviselő tájékoztatása nélkül.

Ellenőrzési kérdőív – 6. terület

Ellenőrzési szempont	Teljesítve	Megjegyzés
A tájékoztató kizárja az automatizált, emberi kontroll nélküli tanulói profilozást.	☐	
Az eszköz nem alkalmaz érzelemfelismerési funkciót (kamera, hang, viselkedés alapján).	☐	
Az eszköz nem végez biometrikus adatgyűjtést tanulókon.	☐	

Amennyiben figyelemmonitorozás van, az alapértelmezetten kikapcsolt és letiltható.	☐	
Prediktív analitika esetén az eredmények kizárólag oktatói tájékoztatást szolgálnak.	☐	
Az EU AI Act 5. cikke szerinti tiltott MI-alkalmazások egyike sem azonosítható az eszközben.	☐	

Összesítő engedélyezési értékelési lap

Az alábbi összesítő lapot az MI-felelős tölti ki, az igazgató hagyja jóvá. Az értékelési lapot az intézményi irattárban legalább 5 évig meg kell őrizni.

MI-eszköz neve:	
Szolgáltató neve:	
Felhasználói kör:	☐ Tanulói ☐ Oktatói ☐ Adminisztratív ☐ Vegyes
Ellenőrzés dátuma:	
Ellenőrzést végezte:	
DPO bevonva:	☐ Igen ☐ Nem (indoklás: _____)

Ellenőrzési terület	Megfelel	Nem felel meg	Feltételesen
1. Adatkezelési feltételek és adatvédelmi tájékoztató megfelelősége	☐	☐	☐
2. A személyes adatok kezelésének jogalapja és adattakarékossága	☐	☐	☐
3. Kiskorú felhasználókra vonatkozó korlátozások és hozzájárulási feltételek	☐	☐	☐
4. Az adatok modelltréning célú felhasználásának szabályozottsága	☐	☐	☐
5. Hozzáférés-kezelési és naplózási lehetőségek	☐	☐	☐
6. Tiltott profilozási és érzelemfelismerési funkciók kizárása	☐	☐	☐

Feltételesen megfelelő: az eszköz alkalmazható bizonyos korlátok között (pl. kizárólag anonimizált tartalomra, kizárólag oktatói használatra, meghatározott funkciókorlátozással). A feltételeket az alábbi megjegyzés rovatban kell rögzíteni.

Feltételek, megjegyzések:
Végső döntés: ☐ Az eszköz engedélyezett ☐ Az eszköz feltételesen engedélyezett ☐ Az eszköz NEM engedélyezett

MI-felelős neve:	Igazgató neve:
Aláírás, dátum	Jóváhagyó aláírás, dátum, pecsét