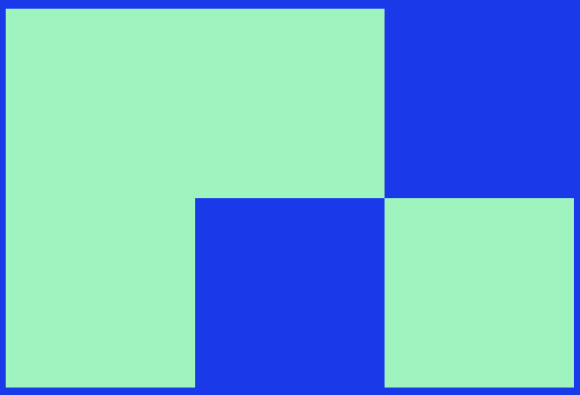
DIGITÁLIS VÁLLALKOZÁSOK SZÖVETSÉGE

Gyakorlati útmutató KKV-knak

Biztonságos és felelős AI-használat cégeknek

Gyakorlati útmutató az AI Act, a GDPR, az adatbiztonság és a mindennapi AI-használat követelményeihez.

A cég felel azért, hogyan használja fel az AI által generált anyagokat.



Ugrás a tartalomra

Tartalomjegyzék

1 perces útmutató 03

Alapelvek 04

A lényeg 05

Leltár 06

Kockázat 07

Adatok 08

Ellenőrzés 11

Akcióterv 13

Ellenőrzőlista 14

A biztonságos AI-használat nem csak egyetlen jogszabály kipipálása.

Tartsd nyilván az eszközöket, rögzítsd, milyen adat hova kerülhet, és jelöld ki, ki ellenőrzi a fontos AI által generált anyagokat. Ez a vállalati minimum.

Együtt kell vizsgálni az AI Act, a GDPR, a kiberbiztonság, a titoktartás és üzleti titok, a pontosság és az emberi felülvizsgálat, a szerzői és kereskedelmi felhasználási jogok, a csalás és megszemélyesítés, valamint az ágazati szabályok követelményeit.

1 perc · Minden munkatársnak

Amikor AI-t használsz

Ha csak egy perced van, ezt a két listát nézd át. A céges szabályzat ennél szigorúbb is lehet.

Tedd

- Jóváhagyott, vállalati kezelésű fiókot használj.
- Csak a feladathoz feltétlenül szükséges, engedélyezett adatot oszd meg, töltsd fel.
- Ellenőrizd a tényeket, számításokat és forrásokat; a hivatkozásokat nyisd meg.
- A fontos eredményeket nézesd át hozzáértő személlyel.
- Olvasd át a teljes anyagot, mielőtt elküldöd, közzéteszed vagy felhasználod.
- Azonnal jelentsd a téves feltöltést, váratlan hozzáférést és veszélyesnek tűnő kimenetet.

Ne tedd

- Ne adj meg jelszót, API-kulcsot, hitelesítő kódot, tokent vagy privát kulcsot.
- Ne tölts fel ügyfél-, munkavállalói, egészségügyi vagy pénzügyi adatot személyes fiókba.
- Ne feltételezd, hogy egy idézet, jogszabály, hivatkozás vagy számítás valódi.
- Ne telepíts AI-bővítményt és ne kapcsolj össze rendszert jóváhagyás nélkül.
- Ne futtass AI által írt kódot, makrót vagy parancsot ellenőrzés nélkül.
- Ne engedd, hogy AI-agent emberi jóváhagyás nélkül üzenetet küldjön, fizessen, rekordot módosítson vagy adatot töröljön.

Ha bizonytalan vagy az adatban, az eszközben vagy a lehetséges következményben: állj meg, és kérdezd meg a kijelölt felelőst.

A felelős AI-használat alapelvei

01

Emberi felelősség

Az AI támogatja a munkát, de a döntésekért és az eredmények felhasználásáért mindig az ember felel.

02

Ellenőrzés és emberi felügyelet

Az AI által generált tartalmat, elemzést vagy javaslatot felhasználás előtt mindig ellenőrizni kell. Az AI eredménye nem fogadható el automatikusan, szükség esetén azt a felhasználónak módosítani, elutasítani vagy felülbírálni kell.

03

Adatvédelem

Csak olyan adatot szabad AI-eszközre feltölteni, amelynek kezelése megfelel a szervezet adatvédelmi és információbiztonsági szabályainak.

04

Átláthatóság

Az AI használatának ténye és szerepe legyen visszakövethető. Nem szabad eltitkolni vagy félrevezetően bemutatni az AI közreműködését olyan esetekben, amikor annak ismerete lényeges az eredmény értelmezéséhez, elfogadásához vagy felhasználásához.

05

Jogszerűség

Az AI-használat során be kell tartani a vonatkozó jogszabályokat, belső szabályzatokat és szerződéses kötelezettségeket.

06

Méltányosság és elfogulatlanság

Az AI eredményeit úgy kell felhasználni, hogy azok ne eredményezzenek indokolatlan megkülönböztetést, elfogult döntéseket vagy tisztességtelen bánásmódot egyetlen személlyel vagy csoporttal szemben sem.

07

Kockázatarányosság

Minél nagyobb hatással van az AI által generált eredmény emberekre, üzleti folyamatokra vagy jogokra, annál alaposabb ellenőrzés és jóváhagyás szükséges.

08

Biztonság

Az AI-használat nem veszélyeztetheti a szervezet információbiztonságát, működését vagy jó hírnevét.

09

Célhoz kötöttség

Az AI által előállított eredmények nem használhatók fel az eredeti céltól eltérő módon, megfelelő felülvizsgálat és jóváhagyás nélkül.

10

Folyamatos tanulás

Az AI-t használó munkatársaknak ismerni kell az eszközök korlátait, kockázatait és a szervezet vonatkozó szabályait.

01 · A lényeg

Négy kérdés minden használat előtt

Az AI használatának kockázata minden esetben a felhasználás céljától függ. Ötletelésnél alacsony a kockázat, emberekről szóló döntéseknél viszont külön szakértői vizsgálatra lehet szükség.

1

Mi a cél?

Vázlatot készít, ügyfelet szolgál ki, vagy személyekről szóló döntést támogat?

2

Milyen adat?

Nyilvános, belső, bizalmas, személyes vagy különleges adatot adsz meg?

3

Mi a hatás?

Befolyásolja valaki állását, pénzét, üzleti lehetőségét, jogát vagy hozzáférését?

4

Ki felel?

Van ideje, tudása és joga egy embernek ellenőrizni és felülbírálni?

Egyszerű döntési szabály

Minél nagyobb a hatás emberekre, jogaikra vagy lehetőségeikre, annál alaposabb kockázatértékelésre és szakértői felülvizsgálatra van szükség. Az AI támogatja a döntéseket, de nem helyettesíti a felelős emberi döntéshozatalt.

A használó cég is alkalmazónak számít

Az AI Act alkalmazónak tekinti azt a céget is, amelynek munkatársai AI-eszközt használnak a munkájukhoz. Ehhez saját fejlesztés sem kell. A munkatársak AI-jártasságának fejlesztését 2025. február 2. óta a feladataikhoz kell igazítani; ezt a nemzeti hatóságok 2026. augusztus 2-től ellenőrzik.

Készíts leltárt a tényleges használatról

A leltár megmutatja, milyen eszközökhöz, adatokhoz és folyamatokhoz szükséges vállalati szabályozás.

Egy egyszerű táblázat is elég

AI-eszköz vagy funkció	Használó csapat
Üzleti cél	Adattípus
Fiók és előfizetés	Szerződéses keret
Döntési hatás	Név szerinti felelős

Vedd fel külön az AI-szolgáltatásokat, a meetingjegyzetelőket, a böngészőbővítményeket, a HR- és CRM-rendszerek AI-funkcióit, valamint a Microsoft 365 vagy a Google Workspace beépített lehetőségeit.

Tulajdonos

Jelölj ki koordinátort

Bízd a feladatot egy emberre vagy kis csoportra, amely karbantartja a leltárt, megválaszolja a kérdéseket, és egyeztet a jogi, adatvédelmi, biztonsági és üzleti területekkel.

Shadow AI

Adj használható alternatívát

A puszta tiltás rejtett használathoz vezethet. Legyen gyors és egyértelmű a jóváhagyás, adj céges fiókot, és legyen kitől kérdezni. Így kisebb az esélye, hogy üzleti adat személyes fiókba kerül.

Gyors besorolás: mehet, feltételes vagy stop

Ezzel a szűrővel gyorsan elbírálhatod a hétköznapi használatot. A kényes eseteket időben irányítsd szakértőhöz, a jogi minősítést pedig külön végezd el.

Stop	Munkahelyi vagy oktatási érzelemfelismerés; káros manipuláció vagy sebezhetőség kihasználása; tiltott társadalmi pontozás; beleegyezés nélküli intim tartalom létrehozása, tömeges arcképgyűjtés arcfelismerési adatbázisokhoz, biometrikus kategorizálás. Ezeknél állítsd le a projektet, és vonj be jogi szakértőt, mert ezek az AI-használatok tiltottak az Európai Unióban.
Külön szakértői átnézés szükséges	Toborzás és munkavállalói döntések, hitelképesség, biztosítás, oktatás és képzés, biometrikus azonosítás, alapvető szolgáltatáshoz való hozzáférés vagy más jelentős, embereket érintő döntés. Ilyenkor dokumentált besorolás és hatásvizsgálat kell, mert ezek emberi sorsokat érintő, magas kockázatú felhasználásnak minősülnek.
Feltételekkel	Ügyfélkommunikáció, szerződés- vagy pénzügyi anyag elemzése, meetingjegyzetelés, webes chatbot. Használj jóváhagyott céges eszközt, tájékoztasd az érintetteket, és ellenőriztesd az eredményt hozzáértő emberrel.
Jellemzően mehet	Ötletelés, nyilvános forrás összefoglalása, általános szövegvázlat vagy munka fiktív adatokkal. A tényeket és a forrásokat itt is ellenőrizd, a végső kimenetet pedig olvasd át.

Az emberi ellenőrzés nem módosítja a besorolást

A magas kockázatú besorolás attól sem változik, hogy a végén egy ember jóváhagyja az eredményt. Az emberi felügyelet a jogszerű és megbízható működést segíti.

Két szempont dönt: az adat és a felhasználás kockázata

Az adat besorolása meghatározza a minimális beavatkozási szintet, de a felhasználás célja, hatása, integrációi és műveleti jogosultságai további védelmet tehetnek szükségessé.

Gyakorlati szabály

Ha bizonytalan vagy egy adat besorolásában, akkor kezeld mindig a magasabb kockázati szint szerint. AI-eszközbe csak annyi adatot adj meg, amennyi a feladathoz feltétlenül szükséges. Ahol lehet, használj anonimizált, kitakart (maszkolt) vagy fiktív adatokat.

Az adatok érzékenységével arányosan növeld a védelem, az eszközválasztás és az emberi ellenőrzés szintjét.

Adatérzékenység × felhasználási hatás és jogosultság

Egy elszigetelt, csak szöveget készítő chat és egy e-mailhez, CRM-hez vagy könyveléshez hozzáférő AI ugyanazzal az adattal is más kockázati szintet jelenthet. A fizetős személyes előfizetés pedig nem vállalati fiók: üzleti használathoz megfelelő szerződés, központi adminisztráció és adatkezelési garanciák kellenek.

0 · Nyilvános	A nyilvános nem jelent automatikusan szabadon feltölthető vagy újrafelhasználható adatot. Csak jóváhagyott AI-eszközzel, jogszerűen használható anyaggal dolgozz; ellenőrizd a szerzői jogot, az adatbázis- és platformfeltételeket is. Nyilvános weboldalon közzétett személyes adat sem használható automatikusan: csak akkor, ha a felhasználása jóváhagyott és jogszerű — lásd 3. pont.
1 · Belső, nem érzékeny	Belső munkaanyag személyes adat és üzleti titok nélkül: sablon, általános folyamatleírás, prezentációvázlat vagy munka fiktív adatokkal. Jóváhagyott céges AI-eszközben kezeld.
2 · Bizalmas üzleti és üzleti titok	Szerződés, árazás, ajánlat, pénzügyi adat, forráskód vagy tárgyalási anyag. Csak jóváhagyott céges AI-fiókba töltsd fel! Ellenőrizd a szolgáltató titoktartási és adatfelhasználási vállalásait, ügyfélanyagnál pedig azt is, hogy az NDA (Non-Disclosure Agreement - titoktartási megállapodás) engedi-e külső szolgáltató bevonását.

3 · Személyes	Név, e-mail-cím, önéletrajz, ügyféllevelezés, CRM-rekord vagy munkavállalói adat. Olyan céges AI-eszközt használj, amelyre kiterjed a DPA (Data Processing Agreement - adatfeldolgozási megállapodás). Megfelelő jogalap, tájékoztatás, adatminimalizálás és jogszerű adattovábbítás is kell.
4 · Hozzáférési és biztonsági titok	Jelszó, token, API-kulcs, hitelesítő vagy helyreállítási kód, privát kulcs és kapcsolati karakterlánc. Ezeket általában vállalati AI-környezetbe sem szabad megadni, feltölteni vagy egyedi asszisztens utasításaiba írni. Használj titokkezelőt és maszkolt (kitakart) tesztadatot.
5 · Különleges személyes adat	Faji vagy etnikai származás, politikai vélemény, vallási vagy világnézeti meggyőződés, szakszervezeti tagság, genetikai adat, egyedi azonosításra használt biometria, egészségi adat, szexuális életre vagy irányultságra vonatkozó adat. Külön GDPR-feltétel és szakértői jóváhagyás kell; hatásvizsgálat is szükséges lehet.
6 · Gyermekek adatai	A gyermek adata önmagában nem a GDPR 9. cikke szerinti különleges adat, de fokozott védelem illeti meg. Vizsgáld a jogalapot, az életkornak megfelelő tájékoztatást, a hozzájárulás szabályait és a gyermek legjobb érdekét; használat előtt kérj adatvédelmi jóváhagyást.
7 · Szakmai titok	Ügyvédi, orvosi vagy más szakmai titoktartás alá eső adat. Csak akkor használható, ha a szakmai és szerződéses szabályok megengedik, a szolgáltatói hozzáférés rendezett, és az illetékes szakmai felelős jóváhagyta.
8 · Ágazatilag szabályozott adat	Pénzügyi, biztosítási, egészségügyi, távközlési, közmű- vagy más ágazati szabály alá eső információ. A GDPR-on túl az adott ágazat biztonsági, kiszervezési, megőrzési és auditkövetelményeit is ellenőrizni kell.
9 · Szigorúan védett	Minősített adat, védelmi információ vagy kritikus infrastruktúra érzékeny adata. Nyilvános AI-szolgáltatásba nem tölthető! Csak külön jóváhagyott, zárt megoldásban kezelhető.

Az anonimizálás nem csupán a név törlését jelenti!

Ha az adatok munkakör, projekt, dátum vagy más részletek alapján egy emberhez visszakapcsolhatók, továbbra is személyes adatként kezeld őket.

Mitől alkalmas egy fiók üzleti adatok kezelésére?

5 feltételnek kell teljesülnie.

Van megfelelő szerződés. Személyes adatnál elfogadott vagy aláírt DPA (Data Processing Agreement - adatfeldolgozási megállapodás) kell; bizalmas üzleti adatnál megfelelő titoktartási és adatfelhasználási feltétel megléte szükséges. Egy weben elérhető dokumentum önmagában nem elég.

Az adat nem kerül modelltréningbe. A szolgáltató alapértelmezés szerint nem használja a vállalati adatot a saját modelljeinek tanítására.

A cég kezeli a fiókokat. Központilag szabályozza a hozzáférést, a megőrzési időt és az engedélyezett funkciókat.

Ismert az adat helye. Az adat az EU-ban marad, vagy dokumentált garancia védi az EU-n kívüli továbbítást.

A cég követni tudja az al-adatfeldolgozókat. A szolgáltató értesít a változásokról.

Ügyféladatnál azt is ellenőrizd, hogy a szerződés vagy az NDA engedi-e a külső AI-szolgáltató bevonását.

A szintek áttekintése

A döntés alapjai a tényleges szerződés és a megfelelő, bekapcsolt beállítások legyenek.

Szint	Példa	Mire alkalmas?	Mire nem?
Ingyenes vagy személyes fizetős	ChatGPT Free és Plus, Claude Free, Pro és Max, Gemini személyes Google-fiókkal	Magáncélra. Munkában legfeljebb jóváhagyott és jogszerűen használható nyilvános anyagra, ha a céges szabályzat engedi.	Nem nyilvános üzleti, ügyfél- vagy személyes adatra; nyilvánosan közzétett személyes adat sem használható automatikusan.
Team vagy Business	ChatGPT Business, Claude Team, Google Workspace Geminivel, Microsoft 365 Copilot	Belső üzleti munkára. DPA-val, megfelelő jogalappal és beállításokkal ügyfél- és személyes adat is kezelhető benne.	Magas kockázatú felhasználásra önmagában; hozzáférési titokra, különleges adatra, gyermekek adatára vagy szakmai titokra külön döntés nélkül.
Enterprise	ChatGPT Enterprise, Claude Enterprise, Google Workspace Enterprise Geminivel, Microsoft 365 Enterprise és Copilot	Nagyobb mennyiségű ügyféladatra, szigorúbb adminisztrációhoz és auditkövetelményekhez.	Nem váltja ki a használati szabályokat, a jogalapot, az ágazati követelményeket vagy az emberi ellenőrzést; hozzáférési adatokat ebbe se tölts fel!

Ellenőrizd a többi adatkezelési feltételt is

Külön ellenőrizd a megőrzést, a naplózást, az emberi betekintést, az adattovábbítást és az al-adatfeldolgozókat. A szolgáltatói feltételek változásait is követni kell.

05 · Ellenőrzés

Az ellenőrzés mélysége igazodjon a felhasználás következményeihez

A cég felel azért, hogyan használja fel az AI eredményét. Fontos kimenetnél nevezd meg a felülvizsgálót, és őrizd meg a döntést alátámasztó adatokat.

Az AI által generált tartalmat minden esetben ellenőrizni kell. A pontosságért, a jogszabályoknak való megfelelésért és a felhasználás következményeiért az AI-t használó munkatárs és a jóváhagyó szervezeti egység felel.

Idő

Meg tudja nézni

A felülvizsgálónak legyen elég ideje az eredmény alapos ellenőrzésére.

Tudás

Meg tudja ítélni

A felülvizsgáló értse a témát, a korlátokat és egy tévedés lehetséges következményeit.

Jogkör

Felülbírálhatja

Eltérhet az AI javaslatától, és a szervezet elfogadja a döntését.

Publikálás vagy felhasználás előtt ezt a hat területet fusd át

01 Hallucináció vagy konfabuláció

A meggyőző megfogalmazás nem bizonyíték. Ellenőrizd független forrásból a neveket, számokat, idézeteket, jogszabályokat és hivatkozásokat.

02 Prompt injection

E-mailben, weboldalon, PDF-ben vagy dokumentumban rosszindulatú utasítás lehet az AI számára. A külső tartalmat kezeld nem megbízható adatként, és ne engedd, hogy felülírja a céges szabályokat.

03 Agentek és összekapcsolt rendszerek

Az e-mail-, CRM-, felhőtárhely- vagy könyvelési hozzáférés nagyobb kockázatú, mint egy különálló chat. Adj minimális, lehetőleg csak olvasási jogot, szűk hatókört és naplózást; fontos művelethez kérj emberi megerősítést.

04 Nem biztonságos kimenetkezelés

AI-kimenet ne kerüljön ellenőrzés nélkül weboldalba, adatbázisba, parancssorba, táblázatmakróba vagy alkalmazásba. Felhasználás előtt hitelesítsd, szükség esetén tisztítsd, alakítsd át és teszteld.

05 Hozzáférési adatok és titkok

Ellenőrizd, hogy a promptban, csatolmányban, kimenetben és egyedi asszisztens utasításaiban sincs jelszó, token, API-kulcs, helyreállítási kód vagy privát kulcs.

06 Fiók- és hozzáférés-kezelés

Használj vállalati identitást és többtényezős hitelesítést, tiltsd a fiókmegosztást, gondoskodj a gyors visszavonásról, és rendszeresen vizsgáld felül az összekapcsolt alkalmazásokat.

05 · Ellenőrzés

Kockázatalapú ellenőrzés

Minél nagyobb lehet egy tévedés vagy jogosulatlan művelet hatása, annál erősebb és dokumentáltabb ellenőrzés kell.

Kategória	Minimális ellenőrzés
Alacsony hatás	Olvasd el a teljes kimenetet; javítsd a nyilvánvaló hibákat, a félrevezető vagy nem megfelelő tartalmat.
Közepes hatás	Ellenőrizd az állításokat eredeti forrásból, számold újra a számokat, és erősítsd meg a neveket, dátumokat és szerződéses részleteket.
Magas hatás	Hozzáértő felülvizsgáló, független bizonyíték, dokumentált jóváhagyás és az érintettek számára elérhető emberi felülvizsgálat szükséges.
Generált kód vagy automatizálás	Kódellenőrzés, tesztelés, biztonsági vizsgálat és ellenőrzött környezetben történő futtatás kell.
Jogi, egészségügyi, pénzügyi vagy biztonsági anyag	A megfelelő képesítéssel és jogkörrel rendelkező személy vizsgálja felül felhasználás előtt.

Az AI által generált forráslista önmagában nem bizonyíték.

Minden hivatkozást meg kell nyitni, az eredeti forrást el kell olvasni, és ellenőrizni kell, hogy valóban alátámasztja-e az állítást.

Tájékoztasd az érintetteket az AI használatáról

• Tedd egyértelművé, ha az érintett AI-rendszerrel lép kapcsolatba, például chatbottal beszél.

• Deepfake vagy más megtévesztésre alkalmas, AI-jal létrehozott vagy módosított tartalom esetén használj jól látható jelölést.

• AI-jegyzetelő vagy más, személyes adatot feldolgozó eszköz előtt adj tájékoztatást, és ahol indokolt, hagyd meg a választás lehetőségét.

• Egy személyt érdemben érintő döntés esetében az érintett kérhessen emberi felülvizsgálatot és magyarázatot.

Aktuális állapot

Az AI Act 50. cikkének átláthatósági szabályai 2026. augusztus 2-től alkalmazandók. A részletes megoldást mindig az adott felhasználás és a legfrissebb bizottsági iránymutatás alapján válaszd meg.

06 · Akcióterv

30 napos bevezetési terv

A megfelelő irányításhoz egészítsd ki a meglévő adatvédelmi, információbiztonsági, HR- és beszerzési folyamatokat.

1–5. nap	**Felelős kijelölése és leltár** Jelöld ki a koordinátort, és kérdezd meg a csapatokat igényeikről. Rögzítsd az eszközöket, a használat célját, az adattípust, a fiókokat és a felelősöket.
6–10. nap	**Gyors kockázati szűrés** Válaszd külön az azonnal leállítandó, a szakértői vizsgálatot igénylő és a normál kontrollokkal kezelhető felhasználásokat.
11–20. nap	**Eszközlista, szerződések, tájékoztatás** Nevezd meg a jóváhagyott céges fiókokat, ellenőrizd a szerződéses garanciákat, és frissítsd a chatbot-, meeting-, ügyfél- és munkavállalói tájékoztatókat.
21–30. nap	**Képzés és próbaellenőrzés** Tarts szerepkörhöz illő gyakorlati képzést, dokumentáld a részvételt, majd egy valódi folyamaton próbáld ki, hogy a szabály működik-e.

Fenntartás – rendszeres ellenőrzés

Negyedévente frissítsd a leltárt, és nézd át a szolgáltatói változásokat. Évente ellenőrizd a szabályzatot, a képzést és a szerződéseket. Új eszköznél vagy felhasználási célnál ne várj a következő ciklusig.

Egylapos vezetői ellenőrzés

Ha bármelyik válasz „nem” vagy „nem tudjuk”, jelölj ki felelőst és határidőt. A lista gyorsan végigvehető működési ellenőrzés; a jogi minősítést külön végezd el.

Megvan a vállalati minimum?

Jelöld be a tizenkét pontot.

- [ ] Van naprakész AI-eszközleltárunk
- [ ] Minden tételnek van üzleti célja és felelőse
- [ ] Ismerjük az egyes használatok adattípusát
- [ ] Van jóváhagyott eszköz- és fióklistánk
- [ ] Személyes adatnál rendezett az adatfeldolgozói keret
- [ ] Bizalmas adatnál ellenőriztük az NDA-t és a szerződést
- [ ] A fontos kimeneteket hozzáértő ember felülvizsgálja
- [ ] Az ember valóban eltérhet az AI javaslatától
- [ ] A tiltott és magas kockázatú eseteket külön szűrjük
- [ ] Az érintettek időben megkapják a szükséges tájékoztatást
- [ ] A munkatársak a munkakörükhöz illő AI-képzést kaptak
- [ ] Van incidensjelentési és rendszeres felülvizsgálati rend

Jogi, adatvédelmi és biztonsági források

Az útmutató az AI-szabályozás mellett adatvédelmi, szellemi tulajdoni, kiberbiztonsági és szolgáltatói forrásokra épül. A követelményeket mindig az adott felhasználás, szerződés és ágazat alapján kell alkalmazni.

Az AI Act aktuális állapota: az (EU) 2026/1744 rendeletet 2026. július 24-én kihirdették; az önálló, III. melléklet szerinti magas kockázatú rendszerekre vonatkozó alkalmazási dátum 2027. december 2., az uniós termékbiztonsági szabályokba ágyazott rendszereké 2028. augusztus 2.

- Az EU AI Act hivatalos szövege – (EU) 2024/1689
- Digital Omnibus on AI – (EU) 2026/1744
- Európai Bizottság: iránymutatás az 50. cikk átláthatósági szabályaihoz
- Európai Bizottság: az átláthatósági szabályok röviden
- Európai Bizottság: AI-jártasság az AI Actben
- European IP Helpdesk: Navigating Intellectual Property in the Age of Artificial Intelligence
- Európai Bizottság: különleges személyes adatok kezelése
- Európai Bizottság: a gyermekek adatainak külön biztosítékai
- Australian Cyber Security Centre: Artificial intelligence for small business
- OWASP Top 10 for LLM and GenAI
- OpenAI: üzleti adatok védelme és vállalati kontrollok
- Anthropic: a kereskedelmi ügyfelek adatainak felhasználása
- Google Workspace: Gemini üzleti és vállalati adatkezelés
- Microsoft: vállalati adatvédelem a Microsoft 365 Copilotban
- AI principles | OECD
- AI Risk Management Framework | NIST

Jogi tájékoztató: ez a kézikönyv általános útmutatást ad. Egyedi ügyben kérj jogi tanácsot. Magas kockázatú, személyes vagy különleges adatot kezelő, illetve embereket jelentősen érintő használat előtt kérj jogi, adatvédelmi és információbiztonsági ellenőrzést. A szolgáltatói feltételeket és a jogi határidőket bevezetés előtt újra ellenőrizni kell.

Biztonságos és felelős AI-használat cégeknek

IVSZ – Digitális Vállalkozások Szövetsége · 2026