# Milyen szoftverdokumentációra van szükség NIS2 kötelezett szervezetnél SaaS szolgáltatás igénybevétele esetén?

## VFP3 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/17

VERZIÓKÖVETÉS

| Verziószám | Dátum | Módosította | Módosítások leírása |
|---|---|---|---|
| **1.0** | 2026.11.17 | Kálmán és Társa Ügyvédi Iroda | Első kiadott verzió |

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

Megjelent a Magyar Kereskedelmi és Iparkamara (MKIK) **NIS2-Tudástárában**. A témához kapcsolódó alkalmakat a **workshopok oldala** sorolja fel. A dokumentum oldala a **Tudástárban**.

## 1. VEZETŐI ÖSSZEFOGLALÓ

A Magyar Kereskedelmi és Iparkamara iránymutatása szerint a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) hatálya alá tartozó, NIS2-kötelezett szervezet a szoftverként igénybe vett szolgáltatásnál (a továbbiakban: SaaS) nem a termék, hanem a szolgáltatás dokumentációját követeli meg, és a szolgáltató megfelelését bizonyítékokkal igazolja. A szolgáltató mérete és székhelye a Szervezet felelősségét nem csökkenti, csak az eszközöket változtatja meg.

- SaaS-nál a dokumentáció tárgya a szolgáltatás és a felelősségmegosztás. A szolgáltatásleírás, a szolgáltató megosztott felelősségi modellje, a biztonsági intézkedéseinek leírása, a független tanúsítványok és auditjelentések, az adattárolás helye és az al-adatfeldolgozók jegyzéke, az interfészleírás, a kilépési feltételek és az

incidensértesítési rend lépnek a telepítési dokumentáció helyébe. A követelmények teljesülését a rendszerbiztonsági tervben követelményenként ki kell fejteni, ehhez a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) sablonja ajánlott.

- A Szervezet saját dokumentációja nem spórolható meg. A tenant[1] biztonsági alapkonfigurációja, a jogosultságkezelés, a saját rendszerekhez való kapcsolódás, a rendszerbiztonsági terv és a kilépési terv a Szervezet feladata marad, mert a követelmények ügyféloldali részét senki más nem teljesíti helyette.
- A nagy szolgáltató általános szerződési feltételei is szerződéses kötelmet jelentenek, de csak azt, ami bennük áll. A Szervezet feladata a standard feltételcsomag megőrzése, a követelményekkel való összevetése, a kiegészítő opciók kihasználása, a maradék hiányra helyettesítő intézkedés és vezető által jóváhagyott, dokumentált eltérés. Ha a hiány így sem ellensúlyozható, a szolgáltatást el kell vetni.
- Külföldi szolgáltatónál a magyar hatóság a szolgáltató felett rendszerint nem rendelkezik felügyeleti jogkörrel, ezért a megfelelés kizárólag a Szervezet felelőssége. A Szervezet azonosítja a szerződő felet, biztosítja az adattovábbítás feltételeit, lehetőség szerint európai adatrégiót választ, a külföldi jog szerinti hozzáférés kockázatát saját kulcsú titkosítással vagy az adatkör szűkítésével kezeli, és kilépési tervet készít.
- Generatív MI-asszisztensnél csak a vállalati előfizetés fogadható el, amelyhez adatfeldolgozási szerződés, adminisztrátori ellenőrzés és a tanításra felhasználás kizárása tartozik. Az európai adattárolás és a saját kulcs itt gyakran nem elérhető, ezért a használati szabályzat és az adatkör szűkítése a fő kontroll.
- Az audit a szolgáltatónál nem végezhető el, ezért a bizonyítékot a Szervezetnek kell gyűjtenie és megőriznie. A tanúsítványok hatókörét, a jelentések érvényességét és az ügyféloldali követelmények teljesítését az auditor a Szervezetnél, a rendszerbiztonsági terv alapján kéri számon.

## 2. A VIZSGÁLANDÓ KÉRDÉS

A vizsgálandó kérdés az, hogy a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban „Kiberbiztonsági tv.”) hatálya alá tartozó szervezet (a továbbiakban „Szervezet”) milyen dokumentációt köteles és milyen dokumentációt célszerű megkövetelnie, ha szoftvert szolgáltatásként (SaaS) vagy más felhőalapú szolgáltatásként vesz igénybe.

Az iránymutatás külön vizsgálja azt a gyakori helyzetet, amikor a szolgáltató nagy, nemzetközi vállalat, amelynél egyedi szerződés nem köthető, és azt, amikor a szolgáltató külföldi, például egyesült államokbeli cég.

A saját infrastruktúrán futó szoftver dokumentációját az MKIK 2026/16. számú, on-premise szoftverről szóló iránymutatása, a közreműködői szerződés tartalmát a 2026/10., az anyavállalati szolgáltatást a 2026/12. számú iránymutatás tárgyalja, ezekre a jelen anyag épít.

[1] Tenant (bérlő) a felhőszolgáltató több ügyfél által közösen használt infrastruktúráján belül a Szervezethez tartozó, logikailag elkülönített példány, amely a Szervezet felhasználóit, adatait, beállításait és adminisztrátori jogosultságait foglalja magában. Az iránymutatás a magyar szakmai gyakorlatban elterjedt tenant kifejezést használja.

## 3. GYAKORLATI JAVASLATOK

Az alábbi javaslatok a mindennapi munkához készültek, ezért a jogszabályi hivatkozásokat nem tartalmazzák. Az egyes lépések jogalapját a 4. fejezet, a követelmények pontos megjelölését az 1. melléklet tartalmazza.

### 3.1 A szolgáltatás besorolása és a felelősség tisztázása

A dokumentációs elvárás összeállítása előtt az alábbi kérdéseket kell tisztázni.

- Az új SaaS-szolgáltatás a Szervezet melyik elektronikus információs rendszerének (a továbbiakban: EIR) része, és az a rendszer melyik biztonsági osztályba tartozik, mert a biztonságiosztály határozza meg, mennyi bizonyítékot kell a szolgáltatótól kérni.
- A szolgáltató közreműködőnek minősül, hiszen a rendszer üzemeltetését és az adatok feldolgozását ő végzi, ezért a biztonsági követelményeknek vele szemben szerződéses kötelezettségként kell fennállniuk. Meg kell határozni, hogy ezek a követelmények milyen formában teljesülnek (pl. a szolgáltató ÁSZF-je).
- Az adott biztonsági osztályhoz tartozó követelmények teljesülését a rendszerbiztonsági tervben követelményenként ki kell fejteni, megjelölve, hogy az adott követelményt a szolgáltató, a Szervezet vagy a kettő együtt teljesíti, és ezt milyen bizonyíték támasztja alá. Ehhez a Nemzeti Kibervédelmi Intézet által kiadott, biztonsági osztályonkénti rendszerbiztonsági terv sablon használatát javasoljuk, amely a terv fejezeteit és azok elvárt tartalmát megadja. Külön felelősségi mátrix készítése nem szükséges, a szolgáltató közzétett megosztott felelősségi modellje és önértékelése a terv kitöltésének forrása.

Viszonteladón keresztüli vásárlásnál, ami az irodai platformoknál a leggyakoribb, a szolgáltató mellett a viszonteladó is közreműködő lehet. A szolgáltató feltételeit a Szervezet elfogadja, a szerződés azonban a viszonteladóval jön létre. A viszonteladó akkor közreműködő, ha a licencen túl támogatást nyújt, vagy a tenanthoz hozzáfér. Ha a tenantban delegált adminisztrátori jogot kap, üzemeltetési közreműködő, akire a 2026/10. számú iránymutatás követelményei teljes körűen vonatkoznak.

### 3.2 A SaaS dokumentációs követelményjegyzék

A szolgáltatótól az alábbi dokumentumokat javasoljuk megkövetelni minden biztonsági osztályban, magasabb osztályban részletesebb tartalommal. Nagy szolgáltatónál ezek a megfelelőségi portálról és a jogi dokumentumok oldaláról gyűjthetők össze, a 3. melléklet néhány elterjedt szolgáltatásnál mutatja a fellelhetőségüket.

a) **Szolgáltatásleírás és szolgáltatási szint.** A funkciók, a rendelkezésre állás vállalt szintje, a karbantartási ablakok, a támogatási csatornák és válaszidők, valamint a változások előzetes bejelentésének rendje. Ez pótolja a telepítési és üzemeltetési dokumentációt.

b) **A szolgáltató megosztott felelősségi modellje és önértékelése.** A szolgáltató közzétett leírása arról, mely biztonsági feladatokat vállal ő és melyeket hagy az ügyfélre, a CSA

STAR vagy CAIQ önértékeléssel együtt.[2] Ez a rendszerbiztonsági terv követelményenkénti kifejtésének forrása.

c) **A szolgáltató biztonsági intézkedéseinek leírása.** Hitelesítés, jogosultságkezelés, titkosítás az átvitelben és a tárolásban, naplózás és a naplók ügyfél általi elérhetősége, mentés, incidenskezelés, üzletmenet-folytonosság.

d) **Független tanúsítványok és auditjelentések.** ISO/IEC 27001 tanúsítvány az alkalmazhatósági nyilatkozattal, SOC 2 Type II jelentés, ISO/IEC 27017 és 27018, BSI C5 vagy behatolásvizsgálati összefoglaló. Nagy szolgáltatónál helyszíni ellenőrzésre nincs mód, a külső ellenőrzés szerepét ezek töltik be.

e) **Adatkezelési és adattárolási tájékoztatás.** Az adatok feldolgozásának és tárolásának helye, a mentések helye, az al-adatfeldolgozók jegyzéke és az ügyféladatok elkülönítésének módja.

f) **Interfészleírás.** Az API-k és integrációs felületek, a hitelesítés, az adatformátumok, a hibakezelés, valamint a szolgáltatáshoz szükséges funkciók, portok és protokollok jegyzéke. A végpontok és protokollok jegyzékét Alap osztályban a Szervezet a szolgáltató nyilvános dokumentációjából maga állítja össze, Jelentős és Magas osztályban ezt a szolgáltatótól is meg kell követelni.

g) **Felhasználói útmutató és az adminisztrációs felület leírása.** A Szervezet által kezelhető biztonsági beállítások, a jogosultsági szerepkörök, a naplók és riportok elérése.

h) **Kilépési és adatvisszaadási feltételek.** Az export formátuma és módja, a szolgáltatás megszűnése utáni adatvisszaadás és törlés határideje és igazolása.

i) **Incidensbejelentési és értesítési rend.** A szolgáltatót érintő incidensek, sérülékenységek és tervezett változások bejelentésének csatornája, tartalma és vállalt határideje. A nagy szolgáltatók indokolatlan késedelem nélküli értesítést vállalnak, a Szervezet rövidebb határidejéhez igazított egyedi vállalást nem adnak. A Szervezet ezért a vállalt rendet dokumentálja, a saját határidejét pedig az állapotoldalak és az adminisztrátori riasztások figyelésével és belső incidenskezelési eljárással biztosítja, számolva azzal, hogy a szolgáltató kiesése a Szervezet oldalán is bejelentendő incidens lehet.

### 3.3 A Szervezet saját dokumentációja

A szolgáltatói dokumentáció a Szervezet saját dokumentumait nem pótolja, a rendszerbiztonsági terv pedig a szolgáltatói dokumentumot nem helyettesíti, hanem rögzíti, hogy mely dokumentum fedi le az adott követelményt. A legfontosabb ügyféloldali dokumentum a tenant biztonsági alapkonfigurációja, vagyis a hitelesítés, a feltételes hozzáférés, a külső megosztás, a naplózás és megőrzés, az integrációk és az adminisztrátori szerepkörök dokumentált beállítása, a nyilvános viszonyítási alapoktól (CIS,[3] a szolgáltató biztonsági pontszáma) való eltérések indokolásával, az

[2] CSA, Cloud Security Alliance, a felhőbiztonsággal foglalkozó nemzetközi szakmai szervezet. STAR, Security, Trust, Assurance and Risk, a CSA nyilvános nyilvántartása, amelyben a felhőszolgáltatók önértékelésüket vagy harmadik fél által végzett tanúsításukat közzéteszik. CAIQ, Consensus Assessments Initiative Questionnaire, a CSA szabványosított kérdőíve, amelyben a szolgáltató a Cloud Controls Matrix (CCM) kontrolljaira adott válaszaival írja le biztonsági gyakorlatát.

[3] CIS, Center for Internet Security, egy nonprofit szervezet, amelynek CIS Benchmark néven közzétett, konszenzussal kialakított biztonsági beállítási ajánlásai többek között a Microsoft 365 és a Google Workspace tenant

MKIK-58. számú állásfoglalás elvei szerint. Emellett a Szervezet elkészíti a szolgáltatás használatának belső üzemeltetési rendjét, a felhasználó- és jogosultságkezelés szabályait, a saját rendszereihez való kapcsolódás leírását, a kilépési tervet és a rendszerbiztonsági tervet. A tervben az NKI sablon fejezetei szerint, követelményenként rögzíti, mit teljesít a szolgáltató és milyen bizonyítékkal, mit teljesít a Szervezet, és leírja a szolgáltatástól való függést és a más rendszerekkel fennálló kapcsolatokat.

### 3.4 A szolgáltató ellenőrzése és felülvizsgálata

A szolgáltató megfelelését a tanúsítványok hatókörének és érvényességének, az auditjelentések tartalmának és a rendszerbiztonsági tervben a szolgáltatóhoz rendelt követelményeknek az ellenőrzésével kell nyomon követni. A tanúsítvány önmagában nem bizonyíték, ha hatóköre nem terjed ki az igénybe vett szolgáltatásra vagy adatközpontra. A felülvizsgálatot álláspontunk szerint legalább évente és minden jelentős szolgáltatói változás után el kell végezni, az eredményt az ellátási lánc kockázatelemzésében rögzíteni, Jelentős és Magas biztonsági osztályban ez kötelező. A kockázatértékelésnél érdemes az al-adatfeldolgozókat is figyelembe venni, különösen akkor, ha harmadik országban működnek, vagy ha a szolgáltató MI-funkciókhoz külső modellszolgáltatót von be.

### 3.5 Nagy szolgáltató egyedi szerződés nélkül

A nemzetközi SaaS-szolgáltatók többsége a kis és közepes ügyfelekkel nem tárgyal egyedi szerződést, az igénybevétel feltétele az általános szerződési feltételek elfogadása. A tárgyalás helyébe az összevetés, a kiegészítő opciók megrendelése és a dokumentált eltérés lép. Az alábbi eljárást javasoljuk.

a) **A standard feltételcsomag összegyűjtése.** A keretszerződés, a szolgáltatási szint és a biztonsági melléklet, az adatfeldolgozási szerződés, az al-adatfeldolgozói jegyzék, valamint a megfelelőségi portálon elérhető tanúsítványok és jelentések. A csomagot a szerződéskötéskor érvényes verzióban meg kell őrizni, mert a szolgáltató később egyoldalúan módosíthatja.

b) **Összevetés a követelményekkel.** A rendszerbiztonsági terv szolgáltatóhoz rendelt követelményeinél meg kell jelölni, hogy a standard feltételek melyik dokumentuma és pontja fedi le a követelményt. Ez a kifejtés az audit bizonyítéka arra, hogy a szerződéses kötelezettség a szolgáltató oldalán fennáll, még ha azt nem a Szervezet fogalmazta is meg.

c) **A hiányok minősítése.** Minden követelményt teljesül, részben teljesül vagy nem teljesül minősítéssel kell ellátni, a részben teljesülő és a nem teljesülő tételekhez pedig kockázati szintet kell rendelni.

d) **A szolgáltató kiegészítő opcióinak kihasználása.** A nagy szolgáltatók a standard feltételek mellett megrendelhető opciókat kínálnak, például európai adatrégió és adatkezelési határ, ügyfél által kezelt titkosítási kulcs, bővített naplózás és naplótovábbítás, hosszabb adatmegőrzés, üzleti szintű támogatás, megfelelőségi csomag. Ezekkel a hiányok jelentős része tárgyalás nélkül megszüntethető.

beállításaira is elérhetők.

e) **Helyettesítő védelmi intézkedés a maradék hiányra.** Ahol a standard feltételek és az opciók nem adnak megoldást, a Szervezet saját eszközeivel pótolja a védelmet, például a szolgáltatónál tárolt adatok saját kulcsú titkosításával, ahol a szolgáltató ezt kínálja, a szolgáltatás felé irányuló forgalom és a naplók saját felügyeletével, az adatkör szűkítésével, a rendszeres saját exporttal és a kilépési tervvel. A helyettesítés indokát és egyenértékűségét le kell írni, a vezetővel jóvá kell hagyatni, és az eltérések nyilvántartásába fel kell venni.

f) **Döntés az igénybevételről vagy az elvetésről.** Ha a maradványkockázat a biztonsági osztály mellett nem fogadható el, a szolgáltatást el kell vetni vagy alacsonyabb osztályú adatkörre kell korlátozni. A 2026/15. számú iránymutatás a nyílt forráskódnál ugyanezt az elvet alkalmazza.

### 3.6 Külföldi szolgáltató

Ha a szolgáltató nem Magyarországon letelepedett, például egyesült államokbeli cég vagy annak európai leányvállalata, a 3.5. pontban leírt eljárást az alábbiakkal javasoljuk kiegészíteni.

a) **A szerződő fél és a felügyeleti hatóság azonosítása.** Meg kell állapítani, melyik jogi személlyel jön létre a szerződés, az hol letelepedett, és melyik tagállam hatósága felügyeli. A magyar hatóság a külföldi szolgáltató felett rendszerint nem jár el, ezért a követelmények érvényesítése a Szervezet szerződéses és műszaki eszközeire marad.

b) **Az adattovábbítás adatvédelmi feltételeinek biztosítása.** Személyes adatok esetén az adatfeldolgozási szerződés mellett a harmadik országba irányuló továbbítás jogalapját is dokumentálni kell, az Egyesült Államok esetében az adatvédelmi keretrendszer szerinti tanúsítást vagy az általános szerződési feltételeket, kiegészítő intézkedésekkel és adattovábbítási hatásvizsgálattal.[4]

c) **Az adatok helyének megválasztása.** Lehetőség szerint európai adatrégiót és az adatkezelést az Európai Gazdasági Térségre korlátozó opciót kell választani, és a mentések, a támogatási hozzáférés és az al-adatfeldolgozók helyét is meg kell vizsgálni. Az irodai platformoknál ez vállalati csomagban elérhető, az MI-asszisztenseknél gyakran nem, vagy csak meghatározott csomagban, a modellfuttatás helye pedig eltérhet a tárolásétól. Ahol európai régió nincs, ott az adatkör szűkítése és a használati szabályzat a fő kontroll.

d) **A külföldi jog szerinti hozzáférés kockázatának kezelése.** A szolgáltató székhelye szerinti jog a hatóságok számára adatkérést tehet lehetővé az európai adatközpontban tárolt adatokra is.[5] A kockázatot az adatosztályozás alapján kell értékelni, és a bizalmas

[4] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, 28. cikk és V. fejezet. A Bizottság (EU) 2023/1795 végrehajtási határozata az EU–USA adatvédelmi keretrendszer megfelelőségéről, amelyet a Törvényszék a T-553/23. számú ügyben 2025. szeptember 3-án helybenhagyott, a fellebbezés a Bíróság előtt folyamatban van. Az Európai Adatvédelmi Testület 01/2020. számú ajánlása a kiegészítő intézkedésekről. A NAIH tájékoztatói a nemzetközi adattovábbításról.

[5] Az Egyesült Államokban a Clarifying Lawful Overseas Use of Data Act (CLOUD Act, 2018) és a Foreign Intelligence Surveillance Act 702. szakasza. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos 2/2019. számú közös véleménye a CLOUD Act hatásáról.

adatoknál a Szervezet által kezelt kulccsal végzett titkosítással, ahol a szolgáltató ezt kínálja, egyébként az adatkör szűkítésével vagy álnevesítéssel kell csökkenteni.

e) **Incidensértesítés és együttműködés.** A szolgáltató értesítési rendjét a Szervezet magyar bejelentési határidejéhez kell igazítani, és meg kell győződni arról, hogy a szolgáltató elérhető kapcsolattartót biztosít. Nemzetközi szolgáltatónál ez jellemzően angol nyelvű, jegyrendszeren keresztüli támogatás, ami nem hiányosság, ha a belső incidenskezelés erre fel van készülve. A hatósági ellenőrzés során a Szervezetnek kell a szolgáltatóra vonatkozó bizonyítékokat bemutatnia.

f) **Kilépési terv.** A kilépési tervet a rendszeres saját exporttal, az alternatív szolgáltató megjelölésével és a visszaállás költségével együtt kell elkészíteni és évente felülvizsgálni. Az irodai platformoknál a szolgáltató egyben a Szervezet személyazonosság-kezelője is, ezért az identitásszolgáltatást, a levelezést és a dokumentumtárat külön kell kezelni, a kilépés hónapokban mérhető projekt. Az MI-asszisztenseknél a kilépés beszélgetésexport és törlés.

### 3.7 Generatív MI-asszisztensek vállalati előfizetése

A ChatGPT, a Claude, a Copilot vagy a Gemini vállalati előfizetése SaaS, amelyre a fenti eljárás vonatkozik, néhány további elemmel. A szolgáltatótól be kell szerezni a bevitt adatok tanításra használatának kizárásáról szóló nyilatkozatot vagy szerződéses rendelkezést, az adatmegőrzési és törlési beállítások leírását, a naplóexport vagy megfelelőségi felület leírását, valamint az ISO/IEC 42001 tanúsítványt, ha van. A Szervezet maga készíti el a használati szabályzatot a bevihető adatkörről, a kimenetek ellenőrzéséről és a felhasználók oktatásáról. A munkavállalók egyéni, fogyasztói előfizetése nem megfelelő szolgáltatási forma, mert nincs mögötte adatfeldolgozási szerződés és adminisztrátori ellenőrzés, ezért ezt a Szervezetnek szabályzatban kell tiltania vagy vállalati előfizetésbe terelnie. Az MI-rendszerek vállalati használatának kockázatait az MKIK-45. számú, az árnyék-MI kezelését az MKIK-59. számú jogi állásfoglalás tárgyalja részletesen, ezekre csak utalunk.

## 4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

### 4.1 A vizsgálat kiindulópontjai

Az iránymutatás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) vagy e) pontja alá tartozik, kiberbiztonsági felügyeletét a Kiberbiztonsági tv. 23. § (1) bekezdés b) pontja szerint a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) látja el, és rendszereit biztonsági osztályba sorolta. A SaaS-szolgáltatás a Szervezet által használt EIR, amelynek üzemeltetését a szolgáltató végzi, ezért a szolgáltató a Kiberbiztonsági tv. 6. § (5) bekezdés d) pontja szerinti közreműködő, amellyel a kiberbiztonsági követelményeket szerződéses kötelemként kell teljesíttetni. A vezető felelőssége a Kiberbiztonsági tv. 6. § (6) bekezdése szerint a közreműködő igénybevétele esetén is fennmarad.

A dokumentáció megszerzésének törvényi eszköze az elektronikus információs rendszer biztonságáért felelős személy (IBF) tájékoztatáskérési joga, amely a Kiberbiztonsági tv. 11. § (9) bekezdése alapján a közreműködőre is kiterjed.

A jog azonban a Szervezetet jogosítja, a szolgáltatóval szemben önálló kikényszerítési eszközt nem ad, és a nagy nemzetközi szolgáltatók egyedi dokumentumkérésekre jellemzően nem válaszolnak. Adatfeldolgozási szerződésük az ügyfél ellenőrzési jogát rendszerint úgy rendezi, hogy azt a szolgáltató a tanúsítványok, auditjelentések és biztonsági leírások rendelkezésre bocsátásával teljesíti. Ilyen szolgáltatónál a tájékoztatáskérési jog ezért a szolgáltató által kínált csatornákon keresztül, elsősorban a megfelelőségi portálon közzétett dokumentumok beszerzésével gyakorolható.

Ha ezek egy követelmény igazolására nem elegendők, a Szervezet a hiányt a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban „Rendelet") 2. mellékletének 16.15.3. pontja (A) szerint dokumentálja, és az általa meghatározott intézkedésekkel kezeli. Ha nem a dokumentáció, hanem más követelmény, például a 16.49. pont (A) teljesítése marad el, az 1. melléklet 3. pontja szerinti eltérés vagy 4. pontja szerinti helyettesítő védelmi intézkedés alkalmazandó.

### 4.2 A Rendelet SaaS-ra vonatkozó követelményei

A Rendelet a szolgáltatásként igénybe vett rendszerekre a külső elektronikus információs rendszerek szolgáltatásaira vonatkozó követelményeket rendeli alkalmazni.

> *16.49. A szervezet:*
> *16.49.1. Szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.*
> *16.49.2. Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban.*
> *16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont, A]*

A követelmény három dokumentumot feltételez. A szerződés a szolgáltatóra rótt követelményeket tartalmazza, a rendszerbiztonsági terv követelményenkénti kifejtése a feladatokat rögzíti, az ellenőrzési bizonyíték a megfelelést igazolja. Ezt egészíti ki a szolgáltatótól megkövetelt funkció-, port- és protokolljegyzék (16.51. pont, J), az interfészek dokumentálása (5.7.2. pont, A), az információ helyének dokumentálása (6.52.1. pont, J), az értesítési megállapodás (19.19. pont, A), az alvállalkozói láncra továbbadott követelmények (19.7. pont, A), valamint kiegészítő követelményként a helyszín korlátozása és az adatok visszaszolgáltatása.

A 16.15. pont (A) szerinti adminisztrátori, üzemeltetői és felhasználói dokumentáció a rendszerszolgáltatásra is vonatkozik, ezért a szolgáltatásleírás és a felhasználói útmutató nem kiegészítés, hanem a kötelező dokumentáció szolgáltatási formája. A rendszerbiztonsági tervnek

a 13.2.1.8. pont (A) szerint a más rendszerekkel fennálló kapcsolatokat és függőségeket is tartalmaznia kell, ami SaaS-nál a szolgáltatótól való függés dokumentálását jelenti.

### 4.3 Az általános szerződési feltételek mint szerződéses kötelem

A Rendelet 16.49.1. pontja szerződéses kötelezettséget kíván, egyedileg tárgyalt szerződést nem. Az általános szerződési feltételek elfogadásával létrejött szerződés a Polgári Törvénykönyvről szóló 2013. évi V. törvény szerint a felek között kötelmet keletkeztet, az abban vállalt biztonsági intézkedések tehát szerződéses kötelezettségek.

> *(1) Általános szerződési feltételnek minősül az a szerződési feltétel, amelyet az alkalmazója több szerződés megkötése céljából egyoldalúan, a másik fél közreműködése nélkül előre meghatározott, és amelyet a felek egyedileg nem tárgyaltak meg. [2013. évi V. tv. 6:77. § (1) bekezdés]*
> *(1) Az általános szerződési feltétel akkor válik a szerződés részévé, ha alkalmazója lehetővé tette, hogy a másik fél annak tartalmát a szerződéskötést megelőzően megismerje, és ha azt a másik fél elfogadta. [2013. évi V. tv. 6:78. § (1) bekezdés]*

A kérdés ezért nem az, hogy van-e szerződés, hanem az, hogy mit tartalmaz, és hogy a Szervezet a feltételeket a szerződéskötés előtt megismerte és megőrizte-e.

A hiányzó tételekre a Rendelet két eszközt ad. A helyettesítő védelmi intézkedés a Rendelet 1. mellékletének 4.2. pontja szerint akkor alkalmazható, ha a védelmi intézkedések katalógusa nem tartalmaz az adott viszonyok között eredményesen és kockázatarányosan alkalmazható intézkedést, a Szervezet a kockázatot felméri és elfogadja, az egyenértékűséget a vonatkozó dokumentumban bemutatja, és az alkalmazást a vezető vagy a kockázatok felvállalására jogosult személy jóváhagyja.

Az eltérés dokumentálását és indokolását a Rendelet 1. mellékletének 3.1.2. pontja, a vezető vagy a kockázatok felvállalására jogosult személy általi jóváhagyását a 3.1.3. pontja írja elő, az eltérések és helyettesítő intézkedések nyilvántartását pedig az SZTFH auditrendelete az auditálási terv részeként kéri be.[6] A helyszíni ellenőrzési jog hiányát a 2026/10. számú iránymutatás szerint független megfelelőségi jelentések pótolják. A Kiberbiztonsági tv. 6. § (8) bekezdése alapján az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer szerint tanúsított IKT-szolgáltatás, ha rendelkezésre áll, a megfelelés igazolására alkalmazható. Az ISO/IEC 27001, a SOC 2, a BSI C5 vagy a CSA STAR e körön kívül esik, bizonyítékként azonban mérlegelhető, ha hatóköre az igénybe vett szolgáltatásra kiterjed. Ha a Szervezet a 6. § (9) bekezdése alapján az SZTFH elnökének rendeletében meghatározott tanúsított IKT-szolgáltatás használatára köteles, a 2026/3. számú iránymutatás szerint kell eljárnia. Ha a hiány így sem szüntethető meg, a maradványkockázat felvállalásáról a vezető dönt.

### 4.4 A külföldi szolgáltató és a felügyelet

A Kiberbiztonsági tv. hatálya a 2. § (1) bekezdés a) pontja szerint a Magyarország területén letelepedett vagy letelepedett képviselővel rendelkező szervezetekre terjed ki, a

[6] 1/2025. (I. 31.) SZTFH rendelet 5. § (1) bekezdés c) pont és 4. melléklet.

felhőszolgáltatókra pedig a 2. § (1) bekezdés c) pontja és (2) bekezdése szerint akkor, ha üzleti tevékenységük fő helye Magyarországon van. A más tagállamban letelepedett felhőszolgáltatót a NIS2 irányelv szerint a fő tevékenységi helye szerinti tagállam felügyeli, az Unión kívüli szolgáltató képviselőt jelöl ki.[7] A magyar hatóság jogköre a külföldi szolgáltatóval szemben szűk.

> *b) a kijelölt képviselővel egyik európai uniós tagállamban sem rendelkező, de Magyarországon szolgáltatást nyújtó szervezetek vonatkozásában. [2024. évi LXIX. tv. 24. § (7) bekezdés b) pont]*

Az európai leányvállalattal vagy képviselővel rendelkező nemzetközi szolgáltató tehát nem az SZTFH, hanem más tagállam hatóságának felügyelete alatt áll. Ebből két következtetés adódik. A Szervezet a követelményeket a szolgáltatóval szemben csak szerződéssel és műszaki eszközökkel érvényesítheti, és a hatósági ellenőrzés során a szolgáltatóra vonatkozó bizonyítékot a Szervezetnek kell bemutatnia, mert az SZTFH a 24. § (5) bekezdés e) pont ea) alpontja alapján a biztonsági intézkedések megfelelőségét alátámasztó dokumentumokat a Szervezettől kéri be. A 2026/12. számú iránymutatás szerint bizonyíték hiányában a kontroll nem tekinthető igazoltan teljesítettnek.

### 4.5 Adatvédelem és a külföldi jog szerinti hozzáférés

A SaaS-szolgáltató személyes adatoknál adatfeldolgozó, a szerződés tartalmát és a harmadik országba irányuló továbbítás feltételeit az általános adatvédelmi rendelet határozza meg. A nem személyes üzleti adatokra az adatvédelmi szabályok nem adnak védelmet, ezért a külföldi jog szerinti hozzáférés kockázatát a Rendelet kockázatelemzési követelményei (15.4. és 15.5. pont, A) alapján kell értékelni. A Rendelet a külső rendszerekben tárolt titkos adatok kriptográfiai kulcsai feletti kizárólagos ellenőrzést kiegészítő követelményként ismeri (16.55. pont, O).

Álláspontunk szerint a saját kulcsú titkosítás a külföldi szolgáltatónál tárolt bizalmas adatok esetében a leghatékonyabb helyettesítő intézkedés, mert a helyszín korlátozásával el nem érhető védelmet ad. Az irodai platformok felső csomagjai kínálják, a generatív MI-asszisztenseknél azonban a szolgáltatás természete miatt rendszerint nem érhető el, mert a modellnek olvasnia kell a bevitt adatot. Ilyenkor a tanításra felhasználás kizárása, a megőrzési idő beállítása, az adatszivárgás-megelőzés és a használati szabályzat együttese a helyettesítő intézkedés.

### 4.6 A közszférába tartozó szervezetek

A Kiberbiztonsági tv. 9. § (4) bekezdése szerint az 1. § (1) bekezdés a), b) és c) pontja, valamint honvédelmi célú elektronikus információs rendszerei vonatkozásában az f) pontja szerinti szervezet nem privát felhőszolgáltatást kizárólag az adatosztályozás eredményére figyelemmel vehet igénybe. A 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Korm.rendelet) a döntést kilépési tervhez, az a) pont szerinti szervezetnél költség-haszon elemzéshez is köti.

> *(2) A szervezet vezetőjének a tervezett külföldi adatkezelésre vagy nem privát felhőhasználatra irányuló döntését megelőzően*
> *a) a Kiberbiztonsági tv. 1. § (1) bekezdés a) pontja szerinti szervezet költség-haszon elemzést és kilépési tervet,*

[7] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve, 26. cikk (1) bekezdés b) pont és (3) bekezdés.

*b) a Kiberbiztonsági tv. 1. § (1) bekezdés b) és c) pontja, valamint a honvédelmi célú elektronikus információs rendszerei vonatkozásában az f) pontja szerinti szervezet legalább kilépési tervet készít. [418/2024. (XII. 23.) Korm. rendelet 3. § (2) bekezdés]*

A Korm. rendelet 1. mellékletének 4.2.2. pontja a bizalmassági (B) és a sértetlenségi és rendelkezésre állási (SR) szintből képzett F1 és F4 közötti kategóriához köti a tárolás helyét. Az F1 adat korlátozás nélkül kezelhető. Az F2 adat SR1 besorolásnál földrajzi korlátozás nélkül, SR2 besorolásnál csak az EGT-ben, nem privát felhőben az EGT-n kívül csak harmadik fél által tanúsított felhőben kezelhető. Az F3 adat kizárólag az EGT területén, nem tanúsított nem privát felhőben pedig kizárólag Magyarországon kezelhető. Az F4 adat kizárólag Magyarországon, felhőszolgáltatás esetén csak tanúsított privát felhőben vagy kormányzati felhőben kezelhető. A 4.2.1. pont szerint az SR2 besorolású adat csak EGT-tagállam területén tárolható, külföldi tárolásnál pedig az adatnak Magyarország területén is rendelkezésre kell állnia. A 4.1. pont szerint külföldi adatkezelés vagy nem privát felhő igénybevétele esetén a B2 szintű adatot, ha ez technológiailag lehetséges, a B3 és B4 szintű adatot minden esetben titkosítani kell. A harmadik fél által tanúsított felhő fogalmát az NKI felhőszolgáltatásokról szóló tájékoztatója tölti meg tartalommal, amely az elfogadott keretrendszereket (CSA CCM, ISO/IEC 27017, ISO/IEC 27018, BSI C5, SOC 2) és a hivatkozott nyilvántartásokat sorolja fel, és kimondja, hogy a tanúsítottság önmagában nem jelenti a biztonsági osztály követelményeinek teljesítését.[8] A közszférabeli Szervezet számára ezért a SaaS-szolgáltató adattárolási tájékoztatása és tanúsítványa az adatosztályozás dokumentációjának része, az F4 adatkörnél a külföldi szolgáltató igénybevétele rendszerint kizárt, az F3 adatkörnél pedig csak az EGT-n belül, harmadik fél által tanúsított felhőben jöhet szóba.

### 4.7 A dokumentáció mint audit bizonyíték

Az auditor a szolgáltatónál nem vizsgálódik, ezért a követelmények teljesítését a Szervezetnél a szerződés vagy az elfogadott általános feltételek, a rendszerbiztonsági terv követelményenkénti kifejtése, a tanúsítványok és jelentések, a tenant alapkonfigurációja és az eltérések nyilvántartása alapján értékeli. Bizonyíték hiányában a követelmény nem teljesített, a bizonyítékokat a Szervezet öt évig megőrzi.[9]

## 5. GYAKORI KÉRDÉSEK

### 5.1 Milyen dokumentációt kell kérni SaaS szolgáltatásnál?

A szolgáltatásleírást, a szolgáltató megosztott felelősségi modelljét, a biztonsági intézkedéseinek leírását, a független tanúsítványokat és auditjelentéseket, az adattárolás helyét és az al-adatfeldolgozók jegyzékét, az interfészleírást, a kilépési feltételeket és az incidensértesítési rendet. A Szervezet saját tenant-alapkonfigurációja, üzemeltetési rendje, követelményenként kifejtett rendszerbiztonsági terve és kilépési terve ezen felül szükséges. (3.2. és 3.3. pont)

[8] NBSZ Nemzeti Kibervédelmi Intézet, Felhő, hatósági tájékoztató, https://nki.gov.hu/hatosag/tartalom/felho/ (2025. április 8.).

[9] 1/2025. (I. 31.) SZTFH rendelet 1. § (2) bekezdés, 4. § (2) bekezdés, 6. § (3) bekezdés és 5. melléklet 1.1.4. pont.

### 5.2 Megfelel-e a követelményeknek az általános szerződési feltételek elfogadása?

A Rendelet szerződéses kötelezettséget kíván, nem egyedileg tárgyalt szerződést, ezért az általános szerződési feltételek is szerződéses kötelmet jelentenek, de csak azt, ami bennük áll. A feltételeket tételesen össze kell vetni a követelményekkel, a hiányokat opciókkal, helyettesítő intézkedéssel és dokumentált eltéréssel kell kezelni. (4.3. pont)

### 5.3 Mi a teendő, ha a nagy szolgáltató nem köt egyedi szerződést?

A standard feltételcsomagot össze kell gyűjteni és meg kell őrizni, a követelmények teljesülését a rendszerbiztonsági tervben kifejteni, a kiegészítő opciókat megrendelni, a maradék hiányra helyettesítő intézkedést alkalmazni, és ha a maradványkockázat nem fogadható el, a szolgáltatást el kell vetni. (3.5. pont)

### 5.4 Mi a teendő, ha a szolgáltató külföldi, például egyesült államokbeli cég?

A megfelelés a Szervezet felelőssége, mert a magyar hatóság a külföldi szolgáltató felett rendszerint nem jár el. A szerződő felet azonosítani, az adattovábbítás jogalapját dokumentálni, európai adatrégiót választani, ahol elérhető, a bizalmas adatokat saját kulccsal titkosítani vagy az adatkört szűkíteni, és kilépési tervet készíteni kell. (3.6. pont)

### 5.5 Használható-e vállalati célra a munkatársak egyéni ChatGPT vagy Claude előfizetése?

Nem, mert az egyéni előfizetés mögött nincs adatfeldolgozási szerződés és adminisztrátori ellenőrzés. Vállalati vagy üzleti előfizetés szükséges, a tanításra felhasználás kizárásával, használati szabályzattal és a bevihető adatkör meghatározásával. (3.7. pont)

## 6. FELHASZNÁLT FORRÁSOK


- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet, GDPR)
- A Bizottság (EU) 2023/1795 végrehajtási határozata az EU–USA adatvédelmi keretrendszer által biztosított megfelelő védelmi szintről
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- 2013. évi V. törvény a Polgári Törvénykönyvről
- ENISA, Technical implementation guidance on cybersecurity risk management measures (1.0 verzió, 2025. június)
- Európai Adatvédelmi Testület, 01/2020. számú ajánlás az adattovábbítási eszközöket kiegészítő intézkedésekről (2.0 verzió, 2021)
- Európai Adatvédelmi Testület, 07/2020. számú iránymutatás az adatkezelő és az adatfeldolgozó fogalmáról (2.0 verzió, 2021)

- **MKIK-28 jogi állásfoglalás, Mit tehet egy NIS2 kötelezett cég, ha egy szerződött közreműködő megtagadja az együttműködést?**
- **MKIK-30 jogi állásfoglalás, A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása**
- **NBSZ Nemzeti Kibervédelmi Intézet, A 7/2024. MK rendelet alapján aktualizált rendszerbiztonsági terv sablonok (Alap, Jelentős, Magas, V.1.0)**
- **NBSZ Nemzeti Kibervédelmi Intézet, Felhő, hatósági tájékoztató a felhőszolgáltatások igénybevételéről (2025. április 8.)**

## 7. KAPCSOLÓDÓ MKIK-ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- **2026/16, Milyen szoftverdokumentációt várjon el egy NIS2 kötelezett szervezet a beszállítóitól on-premise szoftver esetén?**
- **2026/10, A közreműködővel kötött szerződés tartalma**
- **2026/12, Anyavállalat, mint EIR beszállító kezelése a NIS2 audit felkészülés során**
- **2026/15, Nyílt forráskódú szoftverek használata NIS2-kötelezett szervezeteknél**
- **2026/3, Mikor kell alkalmazni a tanúsított IKT-termékeket**
- **MKIK-45, Milyen információbiztonsági kockázatok merülnek fel általános célú MI-rendszerek (LLM) vállalati használatánál? NIS2 és AI Act előírások a kockázatok kezelésére**
- **MKIK-59, A Shadow AI jelentette kockázatok és intézkedések a csökkentésükre. NIS2 és AI Act előírások a kockázatok kezelésére**
- **MKIK-58, Hardening. Mennyire ellenálló a rendszerünk? Hogyan határozzuk meg, vezessük be és tartsuk fenn rendszereink biztonsági alapkonfigurációját?**
- **MKIK-18, Hogyan ellenőrizheti egy NIS2 kötelezett cég az általa megbízott közreműködő kiberbiztonsági megfelelését?**

## 8. AJÁNLOTT HIVATKOZÁS

Magyar Kereskedelmi és Iparkamara (2026). Milyen szoftverdokumentációra van szükség NIS2 kötelezett szervezetnél SaaS szolgáltatás igénybevétele esetén? Iránymutatás, 2026/17.

NIS2-Tudástár, **https://nis2.mkik.hu/iranymutatasok/milyen-szoftverdokumentaciora-van-szukseg-nis2-kotelezett-szervezetnel-saas-szolgaltatas/**

Közzétéve: 2026.11.18. Hatályos állapot: 2026.10.22. További anyagok: **https://nis2.mkik.hu/**

## 1. MELLÉKLET

A SaaS szolgáltatás dokumentációjához kapcsolódó követelmények a 7/2024. (VI. 24.) MK rendelet 2. melléklete alapján

A biztonsági osztály jelölése azt a legalacsonyabb biztonsági osztályt mutatja, amelytől kezdve a követelmény kötelező. Az (A) jelölésű követelmény Alap, Jelentős és Magas biztonsági osztályban, a (J) jelölésű Jelentős és Magas biztonsági osztályban, az (M) jelölésű csak Magas biztonsági osztályban kötelező, az (O) jelölés pedig egyik osztályban sem kötelező, kiegészítő követelményt jelent. A táblázat a Rendelet 2025. január 2-től hatályos szövege alapján készült, és nem helyettesíti a teljes követelménykatalógus alkalmazását. Az utolsó oszlopban szereplő RBT-sablon hivatkozások az NKI rendszerbiztonsági terv sablonjainak 2025-ös, V.1.0 változatát

követik (Alap, Jelentős és Magas biztonsági osztály sablon pontszáma), a számozás későbbi változatokban módosulhat.

| Pont | Követelmény | Osztály | Iránymutatás pontja | Teljesítés SaaS esetén |
|---|---|---|---|---|
| **Tervezés, értékelés, kockázatkezelés** | | | | |
| 1.5. | Elektronikus információs rendszerek nyilvántartása | A | 3.1. | A SaaS-szolgáltatás nyilvántartása EIR-ként vagy rendszerelemként. |
| 5.7. | Információcsere | A | 3.2., 4.2. | Interfészleírás és integrációs megállapodás. RBT-sablon 5.2.4.; 8.3.4. (A), 8.3.5. (J), 8.3.6. (M). |
| 13.2. | Rendszerbiztonsági terv | A | 3.1., 3.3., 4.2. | A követelmények teljesülésének követelményenkénti kifejtése az NKI sablon szerint, a függőségekkel. |
| 15.4. | Kockázatelemzés | A | 4.5. | A külföldi jog szerinti hozzáférés kockázatának értékelése. |
| 15.5. | Kockázatelemzés, ellátási lánc | A | 3.4., 3.5. | A szolgáltató értékelése, az al-adatfeldolgozók figyelembevételével. |
| **Konfigurációkezelés** | | | | |
| 6.2. | Alapkonfiguráció | A | 3.3. | A tenant biztonsági alapkonfigurációjának dokumentálása. RBT-sablon 8.4.2. (A, J, M). |
| 6.23. | Konfigurációs beállítások | A | 3.3. | A tenant beállításai és az eltérések indokolása. RBT-sablon 8.4.5. (A), 8.4.11. (J), 8.4.15. (M). |
| 6.52. | Információ helyének azonosítása és dokumentálása | J | 3.2., 3.6. | Adattárolási tájékoztatás és adatrégió. RBT-sablon 4.1.; 8.4.21. (J), 8.4.30. (M). |
| **Rendszer- és szolgáltatásbeszerzés** | | | | |
| 16.7. | Beszerzések | A | 3.2., 3.5. | A felelősségmegosztás és a dokumentációs követelmények szerződéses tartalom. RBT-sablon 8.8.1. (A, J, M). |
| 16.8. | Alkalmazandó védelmi intézkedések funkcionális tulajdonságai | A | 3.2. | A szolgáltató biztonsági intézkedéseinek leírása. RBT-sablon 8.8.2. (A, J, M). |
| 16.14. | Adatgazda szerepkör | O | 3.2. | Az adatok visszaszolgáltatásának és törlésének feltételei. |
| 16.15. | Az elektronikus információs rendszerre vonatkozó dokumentáció | A | 3.2., 4.2. | Szolgáltatásleírás, felhasználói útmutató, a hiány dokumentálása. RBT-sablon 8.8.3. (A), 8.8.5. (J), 8.8.6. (M). |
| 16.49. | Külső elektronikus információs rendszerek szolgáltatásai | A | 3.2., 3.5., 4.2. | Szerződés vagy ÁSZF, a felelősségmegosztás a rendszerbiztonsági tervben, a szolgáltató ellenőrzése. Az NKI RBT-sablon nem tartalmazza, kiegészítő pontként kell felvenni. |
| 16.50. | Kockázatelemzések és szervezeti jóváhagyások | O | 3.5. | A szolgáltatás igénybevételének jóváhagyása. |
| 16.51. | Funkciók, portok, protokollok és szolgáltatások azonosítása | J | 3.2. | A szolgáltató végpontjainak és protokolljainak jegyzéke. RBT-sablon 8.8.6. (J), 8.8.7. (M). |

| Pont | Követelmény | Osztály | Iránymutatás pontja | Teljesítés SaaS esetén |
|---|---|---|---|---|
| 16.54. | Feldolgozás, tárolás és szolgáltatási helyszín | O | 3.6., 4.2. | Európai adatrégió választása. |
| 16.55. | Felügyelt kriptográfiai kulcsok | O | 3.6., 4.5. | Ügyfél által kezelt titkosítási kulcs, ahol a szolgáltató kínálja. |
| 16.57. | Feldolgozási és tárolási helyszín, Magyarország joghatósága | O | 3.6. | Magyarországra korlátozott tárolás, ha elérhető. |
| 16.99. | Támogatással nem rendelkező rendszerelemek | A | 3.6. | A szolgáltatás kivezetésének bejelentése és a kilépési terv. RBT-sablon 8.8.4. (A), 8.8.9. (J), 8.8.10. (M). |
| **Ellátási lánc kockázatkezelése** | | | | |
| 19.7. | Alvállalkozók | A | 3.2. | Al-adatfeldolgozói jegyzék és a továbbadott követelmények. |
| 19.13. | Beszerzési stratégiák, eszközök és módszerek | A | 3.5. | A standard feltételek megfeleltetése és az opciók. |
| 19.16. | Beszállítók értékelése és felülvizsgálata | J | 3.4. | A tanúsítványok és jelentések rendszeres felülvizsgálata. |
| 19.19. | Értesítési megállapodások | A | 3.2. | Incidens-, sérülékenység- és változásértesítés rendje. |

## 2. MELLÉKLET

SaaS dokumentációs követelményjegyzék

A K jelölés a követelmények teljesítéséhez szükséges, az iránymutatás szerint minden esetben megkövetelendő, az Aj jelölés a kockázatelemzés alapján ajánlott dokumentumot jelent. A Nagy szolgáltatónál oszlop azt mutatja, hogy egyedi szerződés hiányában a dokumentum jellemzően hol található. Az RBT oszlop azt jelzi, hogy a tétel az NKI sablon szerinti rendszerbiztonsági tervben teljesíthető-e. Igen, ha a tartalom a terv megfelelő fejezetében kifejthető, Részben, ha a terv a lényeget rögzíti és a részletes dokumentum mellékletként kapcsolódik, Nem, ha önálló szolgáltatói vagy szervezeti dokumentumról van szó, amelyre a terv csak hivatkozik.

| Dokumentum | Elvárt tartalom | Alap | Jelentős | Magas | Nagy szolgáltatónál | RBT-ben teljesíthető |
|---|---|---|---|---|---|---|
| Szolgáltatásleírás és szolgáltatási szint | Funkciók, rendelkezésre állás, karbantartási ablakok, támogatási csatornák és válaszidők, változások bejelentése | K | K | K | Szolgáltatási szint melléklet, termékdokumentáció | Részben, a rendszer hatóköre és szolgáltatásai fejezetben a lényeg, a leírás melléklet |
| A szolgáltató megosztott felelősségi modellje és önértékelése | Mely biztonsági feladatokat vállal a szolgáltató és melyeket hagy az ügyfélre, CSA STAR vagy CAIQ önértékelés | K | K | K | Megfelelőségi portál, biztonsági dokumentáció | Részben, a követelményenkénti kifejtés forrása, a szolgáltatói dokumentum melléklet |
| Rendszerbiztonsági terv követelményenkénti kifejtéssel | Az NKI sablon fejezetei szerint követelményenként, hogy a szolgáltató, a Szervezet vagy mindkettő teljesíti, és milyen bizonyítékkal | K | K | K | A Szervezet készíti | Igen, ez maga a terv |

| Dokumentum | Elvárt tartalom | Alap | Jelentős | Magas | Nagy szolgáltatónál | RBT-ben teljesíthető |
|---|---|---|---|---|---|---|
| A tenant biztonsági alapkonfigurációja | Hitelesítés, feltételes hozzáférés, külső megosztás, naplózás és megőrzés, integrációk, adminisztrátori szerepkörök, eltérések a viszonyítási alaptól | K | K | K | A Szervezet készíti a szolgáltató biztonsági ajánlásai és a CIS viszonyítási alap szerint | Részben, a konfigurációkezelési fejezet a beállítási elveket rögzíti, a beállításjegyzék melléklet |
| A szolgáltató biztonsági intézkedéseinek leírása | Hitelesítés, jogosultságkezelés, titkosítás, naplózás és naplóhozzáférés, mentés, incidenskezelés, üzletmenet-folytonosság | K | K | K | Biztonsági melléklet, megfelelőségi portál | Részben, a védelmi intézkedések fejezetében a szolgáltatói teljesítés megjelölése, a leírás melléklet |
| Független tanúsítványok és auditjelentések | ISO/IEC 27001 az alkalmazhatósági nyilatkozattal, SOC 2 Type II, ISO/IEC 27017 és 27018, európai felhőtanúsítás, ha rendelkezésre áll, behatolásvizsgálati összefoglaló, hatókör és érvényesség | K | K | K | Megfelelőségi portál, titoktartás mellett letölthető | Nem, szolgáltatói bizonyíték, a terv a hatókörre és érvényességre hivatkozik |
| Adatkezelési és adattárolási tájékoztatás | Feldolgozás és tárolás helye, mentések helye, al-adatfeldolgozók jegyzéke és változásuk bejelentése, adatelkülönítés | K | K | K | Adatfeldolgozási szerződés és al-adatfeldolgozói lista | Részben, az információtípusok és a működési környezet fejezetében a hely és az al-adatfeldolgozók, a tájékoztató melléklet |
| Interfészleírás | API-k, hitelesítés, adatformátumok, hibakezelés, végpontok és protokollok jegyzéke (Alap osztályban a Szervezet állítja össze) | K | K | K | Fejlesztői dokumentáció | Részben, a rendszerkapcsolatok és függőségek fejezetében a kapcsolatok, az API-dokumentáció melléklet |
| Felhasználói útmutató és adminisztrációs felület leírása | Ügyfél által kezelhető biztonsági beállítások, szerepkörök, naplók és riportok elérése | K | K | K | Súgóközpont, adminisztrátori dokumentáció | Nem, szolgáltatói dokumentum, a terv hivatkozik rá |
| Kilépési és adatvisszaadási feltételek | Export formátuma és módja, adatvisszaadás és törlés határideje és igazolása | K | K | K | Keretszerződés és adatfeldolgozási szerződés megszűnési pontjai | Nem, szerződéses dokumentum, a terv a készenléti tervezés fejezetében hivatkozik rá |
| Incidensbejelentési és értesítési rend | Csatorna, tartalom, határidő, kapcsolattartó, tervezett változások bejelentése | K | K | K | Adatfeldolgozási szerződés és biztonsági melléklet | Igen, a biztonsági események kezelése fejezetben a szolgáltatói értesítés rendje rögzíthető |
| A standard feltételek lefedettségének kimutatása | A rendszerbiztonsági terv szolgáltatói tételeinél a lefedő dokumentum és pont, a hiány minősítése és kockázata | K | K | K | A Szervezet készíti | Igen, a követelményenkénti kifejtésben a lefedő dokumentum és pont megjelölésével |
| MI-asszisztensnél a tanításra felhasználás kizárása és a megőrzési beállítások | Szerződéses rendelkezés vagy nyilatkozat, megőrzési és törlési beállítások leírása, naplóexport | K | K | K | Üzleti feltételek, adatfeldolgozási szerződés, adminisztrátori dokumentáció | Részben, a követelményenkénti kifejtésben a beállítás rögzítése, a nyilatkozat melléklet |

| Dokumentum | Elvárt tartalom | Alap | Jelentős | Magas | Nagy szolgáltatónál | RBT-ben teljesíthető |
|---|---|---|---|---|---|---|
| Adattovábbítási dokumentáció | Adatfeldolgozási szerződés, személyes adat harmadik országba továbbítása esetén a továbbítás jogalapja, adattovábbítási hatásvizsgálat, kiegészítő intézkedések | K | K | K | Adatfeldolgozási szerződés, keretrendszer szerinti tanúsítás, a hatásvizsgálatot a Szervezet készíti | Nem, adatvédelmi dokumentum, a terv a működési környezet fejezetében hivatkozik rá |
| Saját kulcsú titkosítás leírása | Kulcskezelés, a kulcs feletti ellenőrzés, visszavonás hatása | Aj | Aj | K, ha elérhető, egyébként adatkör-szűkítés | Ügyfél által kezelt kulcs opció dokumentációja, MI-asszisztensnél rendszerint nincs | Részben, a rendszer- és kommunikációvédelem fejezetében a kulcskezelés elve, a leírás melléklet |
| Kilépési terv | Alternatív szolgáltató, rendszeres export, visszaállás lépései és költsége, felülvizsgálat | K | K | K | A Szervezet készíti | Részben, a készenléti tervezés fejezete utal rá, a terv önálló dokumentum |
| Eltérések és helyettesítő intézkedések nyilvántartása | Nem teljesülő követelmény, helyettesítő intézkedés, egyenértékűség indokolása, maradványkockázat, vezetői jóváhagyás | K | K | K | A Szervezet készíti | Nem, az SZTFH auditrendelete szerinti önálló nyilvántartás, a terv hivatkozik rá |

## 3. MELLÉKLET

Példa a dokumentumok fellelhetőségére hét elterjedt szolgáltatásnál

Figyelmeztetés. A táblázat kizárólag tájékoztató jellegű, a szolgáltatók nyilvános dokumentációjának 2026. október 25-i állapotát tükrözi, és nem minősül a szolgáltatások értékelésének vagy ajánlásának. A szolgáltatók a feltételeiket, tanúsítványaikat és funkcióikat gyakran módosítják, ezért a Szervezetnek minden adatot a szolgáltató megfelelőségi portálján és jogi dokumentumaiban a szerződéskötés előtt ellenőriznie, a letöltött dokumentumokat pedig dátummal megőriznie kell. A táblázat nem helyettesíti az iránymutatás 3.5. pontja szerinti összevetést.

| Szolgáltatás | Megfelelőségi portál és tanúsítványok | Adatfeldolgozási szerződés és al-adatfeldolgozók | Adatrégió opció | Saját kulcs | Napló és export | Megjegyzés |
|---|---|---|---|---|---|---|
| Microsoft 365 (Microsoft) | Service Trust Portal, SOC 1, 2, 3, ISO/IEC 27001, 27017, 27018, BSI C5 | Microsoft Products and Services Data Protection Addendum, al-adatfeldolgozói lista a Trust Centerben | EU Data Boundary, európai tárolás és feldolgozás, támogatási hozzáférés jóváhagyása (Customer Lockbox) felső csomagban | Customer Key és Double Key Encryption felső csomagban | Purview egységes naplózás és naplóexport, tartalomkeresés és exportálás, Secure Score | Viszonteladói (CSP) vásárlás gyakori, delegált adminisztrátori jog dokumentálandó |
| Google Workspace (Google) | Cloud Compliance Resource Center, SOC 2, 3, ISO/IEC 27001, 27017, 27018, 27701 | Cloud Data Processing Addendum, al-adatfeldolgozói lista közzétéve | Adatrégió választás Enterprise csomagban | Ügyféloldali titkosítás (CSE) Enterprise Plus csomagban | Adminisztrátori naplók és Reports API, Data Export eszköz | Az identitásszolgáltatás is a platform része, a kilépési tervben külön kezelendő |

| Szolgáltatás | Megfelelőségi portál és tanúsítványok | Adatfeldolgozási szerződés és al-adatfeldolgozók | Adatrégió opció | Saját kulcs | Napló és export | Megjegyzés |
|---|---|---|---|---|---|---|
| Claude Team és Enterprise (Anthropic) | trust.anthropic.com, SOC 2 Type II, ISO/IEC 27001, ISO/IEC 42001 | Adatfeldolgozási szerződés és al-adatfeldolgozói lista a trust centerben, EU–USA adatvédelmi keretrendszer szerinti tanúsítás | Európai adatrégió a vállalati előfizetésben nem elérhető, tárolás és futtatás az Egyesült Államokban, európai futtatás csak felhőpiactéren keresztül (API) | Nincs | Enterprise csomagban naplók, SSO, beállítható megőrzés, beszélgetésexport | Tanításra felhasználás a vállalati csomagban kizárt, használati szabályzat és adatkör-szűkítés a fő kontroll |
| ChatGPT Business és Enterprise (OpenAI) | trust.openai.com, SOC 2 Type 2, ISO/IEC 27001, 27017, 27018, 27701, CSA STAR | Adatfeldolgozási szerződés aláírható, al-adatfeldolgozói lista a trust portálon | Európai adattárolás és európai futtatás jogosult Enterprise ügyfeleknek, új munkaterületnél | Enterprise Key Management (ügyfél által kezelt kulcs) a szolgáltató közlése szerint | Megfelelőségi és napló API, SCIM Enterprise csomagban, beszélgetésexport | Tanításra felhasználás kizárt, megőrzés beállítható, a csomagok közötti különbség jelentős |
| Számlázz.hu (KBOSS.hu Kft.) | Biztonság és megfelelőség oldal, ISO/IEC 27001:2022 tanúsítvány letölthető, független behatolásvizsgálat | ÁSZF és adatkezelési tájékoztató, adatfeldolgozói jogviszony az ÁSZF szerint, al-adatfeldolgozó az AWS | Adatok az AWS európai régiójában | Nincs | Számla Agent API, számlák letöltése és archiválása | Magyar nyelvű támogatás, NAV online adatszolgáltatás a szolgáltatás része |
| Billingo (Billingo Technologies Zrt.) | Jogi dokumentumok oldal, tanúsítvány a honlapon nem szerepel, a szolgáltatótól kérendő | ÁSZF és adatkezelési tájékoztató szolgáltatásonként, külön adatfeldolgozási megállapodás a honlapon nem szerepel | Tárhelyszolgáltató az AWS EMEA, a konkrét régió a szolgáltatótól kérendő | Nincs | API dokumentáció, export és könyvelői adatkapcsolat | A hiányzó elemeket a szolgáltatótól írásban kell kérni, a kérést és a választ dokumentálni |
| MiniCRM (MiniCRM Zrt.) | Adatkezelési tájékoztató, OWASP és CSA CCM elvek, külső biztonsági auditok, tanúsítvány nem szerepel | Adatfeldolgozás az ÁSZF szerint, részletes al-adatfeldolgozói jegyzék (elsődleges szerverek Budapesten, mentés AWS Luxemburg, MI-funkciókhoz OpenAI, Anthropic, Mistral, Google) | Elsődleges tárolás Magyarországon, mentés az EU-ban | Nincs | Export a súgó szerint, API az integrációs leírásban | Az MI-funkciók harmadik országbeli al-adatfeldolgozót vonnak be, a kockázatértékelésben külön vizsgálandó |

Az MKIK a NIS2-kötelezett vállalkozásoknak díjmentes workshopokat és egyedi konzultációt kínál. Az időpontok és a jelentkezés a **workshopok oldalán** érhetők el, további állásfoglalások és iránymutatások pedig a **NIS2-Tudástárban**.