

Nyílt forráskódú szoftverek használata NIS2- kötelezett szervezeteknél

VFP3 KiberVéd - NIS2 Audit felkészítés szakmai
iránymutatás 2026/15

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.10.14	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

*A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum
Megjelent az MKIK [NIS2-Tudástárban](#). A témához kapcsolódó alkalmakat a [workshopok
oldala](#) sorolja fel. A [dokumentum oldala a Tudástárban](#).*

1. VEZETŐI ÖSSZEFOGLALÓ

- **A nyílt forráskódú szoftver használata NIS2-kötelezett szervezetnél is megengedett, a jogszabály a kockázatkezelést szabályozza, nem a licencmodellt.** A 7/2024. (VI. 24.) MK rendelet egyetlen, egyik biztonsági osztályban sem kötelező pontja nevesíti a nyílt forráskódot. Minden más követelmény ugyanúgy érvényes rá, mint a megvásárolt szoftverre, a gyártótól megszokott garanciákat azonban a Szervezetnek magának kell pótolnia.
- **A besorolást a szoftver funkciója dönti el, nem az ára.** Az üzleti adatot tároló és az alaptevékenységet közvetlenül kiszolgáló alkalmazás a Szervezet elektronikus információs rendszere, amelyet nyilvántartani, biztonsági osztályba sorolni és védeni kell. A felügyeleti, naplógyűjtő, mentő vagy virtualizációs szoftver jellemzően támogató rendszer.
- **A támogató rendszer könnyítése eljárási természetű, a védelem szintjét nem csökkenti.** Önálló osztályba sorolást és hatáselemzést a törvény nem ír elő rá, a kiszolgált rendszernek megfelelő védelmet viszont igen, ha az intézkedés kockázatarányosan alkalmazható. A mentőrendszer és a címtár sokszor a támadók legértékesebb célpontja.
- **Az ellátási lánc kockázatelemzése minden osztályban kötelező, és közösségi projektekre is elvégezhető.** A vizsgálat tárgya a projekt életképessége, biztonsági gyakorlata, licence, a letöltési forrás megbízhatósága és a saját üzemeltetési képesség. Licencváltás, a karbantartók cseréje, a támogatás lejárta vagy súlyos sérülékenység esetén az elemzést frissíteni kell.
- **Szerződés nélkül a szerződéses követelmények célját belső eszközökkel kell elérni.** A fejlesztői közösség álláspontunk szerint nem közreműködő, a díjazásért támogatást nyújtó gyártó és az integrátor viszont az. Ahol nincs kivel szerződni, ott belső követelményjegyzék, átvételi vizsgálat és jóváhagyott, dokumentált eltérés lép a szerződéses kikötés helyébe.
- **A jogszerű használathoz licencnyilvántartás, támogatott verzió és vezetői döntés kell.** A licenc felhasználási szerződés feltételeit a Szervezetnek ismernie és követnie kell. A támogatás nélkül maradt elemet le kell cserélni, vagy alternatív támogatásról kell gondoskodni, a használatbavételről pedig a Szervezet vezetője dönt.

2. A VIZSGÁLANDÓ KÉRDÉS

A vizsgálandó kérdés az, hogy a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban „Kiberbiztonsági tv.”) ezáltal a 7/2024. (VI. 24.) MK rendelet (a továbbiakban „Rendelet”) hatálya alá tartozó szervezet (a továbbiakban „Szervezet”) milyen feltételekkel használhat nyílt forráskódú szoftvert saját telephelyén, saját üzemeltetésben. Ezen belül azt vizsgáljuk, milyen szempontokat kell mérlegelni a bevezetés előtt, hogyan végezhető el a

beszállítói kockázatelemzés, miként teljesíthetők a közreműködővel kötött szerződésre előírt követelmények, milyen helyettesítő (kompenzációs) intézkedések jöhetnek szóba, és mi szükséges még a jogszerű használathoz. Külön kérdés, hogy milyen könnyítések illetik meg a támogató rendszereket.

Az állásfoglalás a változtatás nélkül, saját infrastruktúráján futtatott szoftverekre vonatkozik, és két csoportot határol el egymástól. Az egyikbe az üzleti adatot tároló, elektronikus információs rendszernek (a továbbiakban „EIR”) minősülő alkalmazások tartoznak, a másikba a támogató rendszerek. A felhőszolgáltatásként igénybe vett megoldások, a forráskód módosítása és a saját fejlesztésbe beépített nyílt forráskódú komponensek nem tárgyai az állásfoglalásnak.

3. GYAKORLATI JAVASLATOK

3.1 Az EIR és a támogató rendszer elhatárolása

A besorolást három szempont vizsgálatával javasoljuk elvégezni és írásban rögzíteni.

- a) Adattartalom. Ha a szoftver üzleti adatot, ügyféladatot vagy a termelés, a szolgáltatás adatait tárolja, EIR-ként kell nyilvántartani és biztonsági osztályba sorolni.
- b) Szerep az alaptevékenységben. Ha a szoftver kiesése közvetlenül megállítja az alaptevékenységet, EIR-ről van szó. Ha csupán más rendszerek működését szolgálja, támogató rendszer.
- c) Önállóság. Az adatbázis-kezelő, az operációs rendszer és a webkiszolgáló többnyire annak az EIR-nek a rendszereleme, amelyet kiszolgál, és annak biztonsági osztályát követi.

Kétség esetén az EIR-ként való kezelést javasoljuk. A mentőrendszer, a naplógyűjtő és a címtár szerepe ugyan támogató, de üzleti adatok másolatát és hozzáférési adatokat tartalmaznak, ezért védelmük nem maradhat el a kiszolgált rendszerekétől.

3.2 Mérlegelési szempontok a bevezetés előtt

A döntés előtt az alábbi szempontokat javasoljuk megvizsgálni, az eredményt pedig a bevezetési döntés mellékleteként megőrizni.

- a) A projekt életképessége. Vizsgálni kell az aktív karbantartók számát, a kiadások rendszerességét, valamint azt, hogy a projekt mögött alapítvány, több független vállalat vagy egyetlen cég áll.
- b) Biztonsági gyakorlat. A projektnek legyen közzétett sérülékenységkezelési rendje, biztonsági értesítési csatornája és aláírt kiadása.
- c) Licenc. A licencet szükséges azonosítani és nyilvántartásba kell venni. A felhasználást korlátozó licencek (például SSPL, BSL) és a közösségi kiadásból hiányzó funkciók külön figyelmet igényelnek.
- d) Támogatási modell. El kell dönteni, hogy a Szervezet kizárólag a közösségre támaszkodik, gyártói előfizetést vásárol vagy integrátort von be. Jelentős és magas osztályú EIR-nél a szerződéses támogatást javasoljuk.

- e) Saját üzemeltetési képesség. Legalább két, a szoftvert ismerő vagy a szükséges ismeretek gyors elsajátítására képes üzemeltető és írásos üzemeltetési dokumentáció nélkül a bevezetést nem javasoljuk.
- f) Életciklus. Csak támogatott, lehetőleg hosszú támogatási idővel rendelkező kiadás telepíthető, a támogatás lejárat dátumát a nyilvántartásban rögzíteni kell.
- g) Forrás és sértetlenség. A telepítőkészlet a projekt hivatalos tárolójából vagy a disztribúció csomagtárából származzon, az aláírás vagy az ellenőrző összeg vizsgálata mellett.
- h) Kilépési lehetőség. Az adatok legyenek szabványos formátumban exportálhatók, és készüljön terv arra az esetre, ha a projekt megszűnik vagy licencet vált.

Az ingyenes licenc nem jelent ingyenes üzemeltetést. A frissítés, a felügyelet és a szakértelem költségét a beruházás tervezésekor elkülönített tételként kell szerepeltetni (Rendelet 16.2. pont, A, J, M).

3.3 A beszállítói kockázatelemzés lépései

A kockázatelemzést a következő lépésekben javasoljuk elvégezni.

- a) Leltár. A szoftvert, a verzióját, a licencét és a főbb függőségeit fel kell venni a rendszerelemek leltárába, lehetőség szerint szoftverösszetevő-jegyzék (SBOM) formájában.
- b) A lánc szereplői. Azonosítani kell a fejlesztői közösséget vagy alapítványt, a projekt mögött álló céget, a csomagtárat vagy disztribúciót, valamint az esetleges támogatót és integrátort.
- c) Értékelés. A projektet a 3.2. pont szempontjai szerint minősíteni kell, amihez nyilvános mutatók is segítséget adnak.¹
- d) Fenygetések. A Rendelet fenygetéskatalógusából legalább a beszállítói lánc zavarát, a szoftver hamisítását, a szoftverek sérülékenységeit, az erőforrások hiányát, a szerződésszegést és a személyi állomány elvesztését, mint kritériumot vizsgálni kell.
- e) Kockázati szint és kezelés. A kockázatokat legalább négyfokozatú skálán kell minősíteni, és mindegyikhez intézkedést vagy indokolt felvállalást kell rendelni.
- f) Döntés. Az elemzést az elektronikus információs rendszer biztonságáért felelős személy készíti elő, a maradványkockázatot a vezető vagy a kockázat felvállalására jogosult személy fogadja el.
- g) Frissítés. Licencváltás, tulajdonos- vagy karbantartóváltás, a támogatás lejárt és súlyos sérülékenység esetén soron kívül, egyébként a Szervezet által meghatározott időközönkénti felülvizsgálat szükséges.

3.4 Intézkedések a szerződéses garanciák pótlására

Ha a szoftver mögött nincs szerződő fél, a hiányzó szerződéses garanciákat az alábbi intézkedésekkel javasoljuk ellensúlyozni.

¹ Ilyen például az OpenSSF Scorecard (scorecard.dev), a támogatási ciklusokat követő endoflife.date és az OSV sérülékenységi adatbázis (osv.dev).

- a) Belső biztonsági követelményjegyzék és dokumentált átvételi vizsgálat a szerződéses követelmények helyett.
- b) Verziórögzítés és saját, ellenőrzött csomagtár, a frissítések tesztkörnyezetben történő kipróbálásával.
- c) Feliratkozás a projekt biztonsági értesítéseire, valamint a sérülékenységi adatbázisok rendszeres figyelése.
- d) Megerősített alapkonfiguráció, a szükségtelen modulok kikapcsolása, hálózati elkülönítés és a kimenő forgalom korlátozása.
- e) Fokozott naplózás és felügyelet az érintett rendszeren.
- f) Rendszeres mentés és kipróbált visszaállítás, kilépési tervvel kiegészítve.
- g) Képzett, egymást helyettesíteni képes üzemeltetők, valamint eseti szakértői keretszerződés a közösségi támogatás kiegészítésére.

Az intézkedéseket a rendszerbiztonsági tervben, a szerződéses követelményektől való eltérést pedig az eltérések nyilvántartásában kell rögzíteni, és a vezetővel vagy a kockázat felvállalására jogosult személlyel jóvá kell hagyni.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) vagy e) pontja alá tartozik, kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el,² a szoftvert pedig változtatás nélkül, saját eszközein futtatja. A közsféra eltéréseit a 4.8. pont foglalja össze.

A Rendelet a nyílt forráskódú szoftvert egyetlen helyen nevesíti, mégpedig egy olyan pontban, amely egyik biztonsági osztályban sem kötelező.

6.48. A szervezet meghatározott korlátozásokat alkalmaz a nyílt forráskódú szoftverek használatára vonatkozóan. [7/2024. (VI. 24.) MK rendelet 2. melléklet 6.48. pont] (O)

Ebből két következtetés adódik. A jogalkotó nem tiltja a nyílt forráskódú szoftverek használatát, a korlátozások meghatározását pedig a Szervezet kockázatelemzésére bízta. A szoftverre vonatkozó többi követelmény ugyanakkor a licencmodelltől függetlenül alkalmazandó, hiszen a törvény a védelem tárgyai között a szoftvert általánosan megnevezi.³ A valódi különbség az, hogy a közösségi projektnél nincs olyan gyártó, amely szerződésben vállalna kötelezettséget a hibák javítására.

4.2 Mikor EIR és mikor támogató rendszer a szoftver

A törvény fogalomrendszerében minden szoftveres megoldás elektronikus információs rendszer vagy annak része, mert az EIR fogalma a program alapján adatot kezelő eszközöket és az általuk

² 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

³ 2024. évi LXIX. tv. 5. § (2) bekezdés b) pont

kezelt adatokat egyaránt felöleli.⁴ A támogató rendszer sem áll ezen a körön kívül, hanem az EIR-ek egyik fajtája.

92. támogató rendszer: az 1. § (1) bekezdés a)–c) pontja szerinti szervezet alapfeladatainak ellátásában közvetlenül nem részt vevő elektronikus információs rendszer, amely szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el; [2024. évi LXIX. tv. 4. § 92. pont]

Az elhatárolás ismérve tehát az alapfeladat ellátásában való közvetlen részvétel. Álláspontunk szerint az a nyílt forráskódú alkalmazás, amely a Szervezet üzleti adatait tárolja és az alaptevékenység folyamatait közvetlenül kiszolgálja (például a vállalatirányítási, az ügyfélkezelő vagy a dokumentumkezelő rendszer), a Szervezet rendelkezésében lévő EIR. A felügyeleti, naplógyűjtő, mentő, virtualizációs vagy azonosító megoldás ezzel szemben más rendszerek működéséhez szükséges, ezért támogató rendszer.

A megkülönböztetésnek a nyilvántartásban és az eljárási kötelezettségekben van közvetlen következménye. Az EIR-ekről és központi szolgáltatásokról vezetett nyilvántartás külön sorolja fel a Szervezet rendelkezésében lévő EIR-eket és az egyéb támogató rendszereket.⁵ A hatáselemzést, a biztonsági osztályba sorolást és a védelmi intézkedések meghatározását a törvény szövege kizárólag az előbbi körre, azaz az EIR-ekre írja elő.⁶

Két bizonytalanságra fel kell hívnunk a figyelmet. A fentiekben írt támogató rendszer jogszabályi meghatározása szó szerint csak a Kiberbiztonsági tv. 1. § (1) bekezdés a), b) és c) pontja szerinti szervezetek rendszereire utal, miközben a nyilvántartási szabály és a 17. § általában a szervezetről szól. Álláspontunk szerint a támogató rendszerre vonatkozó szabályok az SZTFH felügyelete alá tartozó Szervezetenél is alkalmazhatók. A kérdésben közzétett hatósági állásfoglalásról azonban nincs tudomásunk, ezért a besorolás indokait írásban rögzíteni kell. A másik bizonytalanság a vegyes szerepű rendszereket érinti. Ha egy támogató rendszerként bevezetett megoldásban üzleti adat is megjelenik, azt EIR-ként javasoljuk kezelni.

4.3 A támogató rendszerek könnyítése

A támogató rendszerekre a törvény külön alcímben, egyetlen szakaszban állapít meg szabályokat.

(1) A szervezetnek gondoskodnia kell arról, hogy a támogató rendszer is az általa támogatott elektronikus információs rendszernek megfelelő szintű védelemben részesüljön az informatikáért felelős miniszter rendeletében foglaltak alapján, ha az adott védelmi intézkedések kockázatarányosan alkalmazhatók az érintett támogató rendszer vonatkozásában. A szervezet köteles felmérni a támogató rendszerben használt védelmi intézkedéseket.

⁴ 2024. évi LXIX. tv. 4. § 24. pont b) és c) alpont

⁵ 2024. évi LXIX. tv. 6. § (3) bekezdés 1. pont a) és d) alpont

⁶ 2024. évi LXIX. tv. 6. § (3) bekezdés 4., 5. és 6. pont

*(3) Kizárólag olyan támogató rendszer vehető igénybe, amely megfelel az általa támogatott elektronikus információs rendszer védelmi igényeinek.
[2024. évi LXIX. tv. 17. § (1) és (3) bekezdés]*

A rendelkezésből és a 4.2. pontban írtakból három könnyítés olvasható ki. A támogató rendszert nem kell önállóan biztonsági osztályba sorolni, védelmi szintje a kiszolgált rendszerhez igazodik. Az egyes védelmi intézkedések csak akkor kötelezők, ha kockázatarányosan alkalmazhatók, vagyis az elhagyásukat az arányosság mércéje szerint kell megindokolni, nem pedig a helyettesítő intézkedés szigorúbb feltételei szerint. Végül a Rendelet általános szabályai szerint az intézkedéseket csak az adott biztonsági képességet hordozó komponensekre kell alkalmazni, a dokumentáltan elkülönített rendszerelemekre pedig határvédelem mellett egyedi eltérések állapíthatók meg.⁷

A könnyítés határai legalább ilyen fontosak. A védelmi intézkedések felmérése kötelező, tehát a támogató rendszerről is készülnie kell olyan dokumentumnak, amely bemutatja az alkalmazott intézkedéseket, valamint a nem alkalmazott védelmi intézkedések indokát. Több EIR-t kiszolgáló támogató rendszernél álláspontunk szerint a legmagasabb biztonsági osztályú kiszolgált rendszer az irányadó, mert csak így teljesül a 17. § (3) bekezdése. A nyilvántartás és a 4.4. pont szerinti kockázatelemzés alól a támogató rendszer sem mentesül. A kétévente esedékes kiberbiztonsági auditon az auditor várhatóan ezt a felmérést és a besorolás indokolását is kéri.⁸

4.4 Az ellátási lánc kockázatelemzése

A beszállítói kockázatelemzés jogalapja a Rendelet 15.5. pontja, amely minden biztonsági osztályban kötelező.

15.5.1. Felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.

15.5.2. Meghatározott időközönként frissíti az ellátási lánc kockázatelemzését, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatására. [7/2024. (VI. 24.) MK rendelet 2. melléklet 15.5. pont] (A, J, M)

A követelmény ellátási láncról szól, nem szerződő partnerről, ezért akkor is alkalmazni kell, ha a Szervezet a szoftverhez ellenérték és szerződés megtárgyalása nélkül jut hozzá. Az elemzés keretét a szervezeti szintű stratégia és a kritikus beszállítók azonosítása adja, a részletszabályokat a 19. követelménycsoport tartalmazza. Jelentős és magas osztályban ehhez a beszállítók rendszeres értékelése és a rendszerelemek kritikussági elemzése társul.

Nyílt forráskódú szoftvernél a beszállító szó a fejlesztői közösséget, a projektet irányító céget, a csomagot terjesztő tárolót és a szoftver saját függőségeit egyaránt takarja. Az utóbbi évek incidensei éppen ezeket a pontokat érték. Az XZ Utils tömörítőkönyvtárba 2024-ben egy

⁷ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.4.2. és 3.2.7. pont

⁸ 2024. évi LXIX. tv. 16. § (1) bekezdés

fokozatosan bizalmat szerző karbantartó épített hátsó kaput, 2025-ben és 2026-ban pedig csomagtárakon és fejlesztőeszközökön keresztül terjedő támadások érintettek széles kört.⁹

A fenyegetések azonosításához a Rendelet 3. melléklete ad kötelező kiindulópontot.¹⁰ A katalógusból a nyílt forráskódú szoftvernél jellemzően a beszállítói láncok megszakadása vagy zavara, a hardver vagy szoftver hamisítása, a szoftverek sérülékenységei vagy hibái, az erőforrások hiánya, a jogszabályok vagy szerződések megszegése és a személyi állomány elvesztése releváns. Az utolsó kettő gyakran kimarad, pedig a licencfeltételek megsértése és a szoftvert egyedül ismerő rendszergazda távozása nagyon is valós kockázat.

A kockázatokat legalább négyfokozatú skálán kell minősíteni. A legalacsonyabb kategória feletti kockázat felvállalását a vezető vagy a kockázatok kezeléséért felelős személy kockázatonként indokolva hagyja jóvá.¹¹ Az elemzést a 15.5.2. pont értelmében frissíteni kell, ha az ellátási láncban jelentős változás történik. Ilyen változás a licencváltás, a tulajdonos vagy a vezető karbantartók cseréje, a közösségi kiadás megszüntetése és a támogatási ciklus lejárta. Az értékelési szempontokhoz az ENISA és a Nemzeti Kiberbiztonsági Intézet útmutatói adnak további támpontot.¹²

4.5 A közreműködői szerződés követelményei

A törvény a közreműködő igénybevételéhez szerződéses kötelezettséget kapcsol.

d) ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek; [2024. évi LXIX. tv. 6. § (5) bekezdés d) pont]

A Rendelet ezt a beszerzési szerződések kötelező tartalmával egészíti ki. A 16.7. pont (A, J, M) szerint a Szervezet a szerződéseiben követelményként rögzíti többek között a funkcionális biztonsági követelményeket, a biztonság garanciális követelményeit, az EIR biztonsági osztályát és az ahhoz tartozó védelmi intézkedéseket, a dokumentációs követelményeket, a felelősség megosztását és a teljesítési kritériumokat. A 16.8. pont (A, J, M) a fejlesztőtől a védelmi intézkedések funkcionális leírását kívánja meg, a 19.19. pont (A, J, M) pedig megállapodásokat és eljárásokat ír elő az ellátási lánc szereplőivel.

A közreműködő fogalmát a törvény közvetve határozza meg. A rendelkezés szövege alapján közreműködő az, akit a Szervezet igénybe vesz, és aki a Szervezet rendszerével kapcsolatban

⁹ CVE-2024-3094 (XZ Utils, 2024. március); a CISA 2025. szeptember 23-i riasztása az npm csomagtárat érintő ellátásilánc-támadásról; CVE-2026-33634 (Trivy, 2026. március)

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. § (4) bekezdés

¹¹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 5.1.1.5. és 5.1.2.2. pont

¹² ENISA, Good Practices for Supply Chain Cybersecurity (2023. június); NBSZ Nemzeti Kiberbiztonsági Intézet, Alkalmazási Útmutató, 19. Ellátási lánc kockázatkezelése, V.1.2 (2026). Elérhető az NKI honlapján.

tevékenységet lát el.¹³ Álláspontunk szerint a nyílt forráskódú projekt közössége ennek nem felel meg, mert a Szervezet megbízásából semmilyen tevékenységet nem végez a Szervezet rendszerén. A licenc ugyan szerződés, de egyoldalúan meghatározott, a szavatosságot jellemzően kizáró felhasználási engedély, amelybe biztonsági kikötés nem illeszthető. A gyakorlatban három esetkör különíthető el.

- a) Tisztán közösségi használat. Közreműködő nincs, ezért szerződés sincs, amelybe a 16.7. pont elemei bekerülhetnének. A követelmény célját a Szervezet belső követelményjegyzékkel és átvételi vizsgálattal éri el, a hiányzó szerződéses elemeket pedig eltérésként dokumentálja.
- b) Gyártói előfizetés. A díjas támogatást nyújtó cég a karbantartás és a javítás körében közreműködő. Általános szerződési feltételein a Szervezet ritkán tud változtatni, ezért azokat össze kell vetni a 16.7. pont elemeivel, a hiányokat pedig kockázatként kell kezelni.
- c) Integrátor vagy üzemeltetési támogató. A bevezetést vagy a karbantartást végző vállalkozás minden kétséget kizáróan közreműködő. [A szerződésnek tartalmaznia kell a 16.7. pont teljes körét](#), a távoli karbantartás szabályait és a követelmények alvállalkozókra való továbbhárítását.

A vezető felelőssége egyik esetben sem csökken, a törvény azt a közreműködő bevonása esetére is fenntartja.¹⁴ A dokumentáció hiányára a Rendelet maga ad kiegészítő szabályt. Ha a rendszerelemhez nem áll rendelkezésre adminisztratori, üzemeltetői vagy felhasználói dokumentáció, a Szervezet dokumentálja a beszerzésére tett kísérleteket, és végrehajtja a saját maga által meghatározott intézkedéseket. A rendszerelemek és kapcsolódó adatok eredetiségének azonosítására vonatkozó követelmény közösségi projektnél úgy teljesíthető, hogy a Szervezet feliratkozik a projekt biztonsági értesítéseire, és eljárásrendben rögzíti az értékelésük felelősét és határidejét, ami a biztonsági riasztások és tájékoztatások figyelésével kapcsolatos követelmény (18.37.) teljesítését is szolgálja.

4.6 Helyettesítő védelmi intézkedések

A kompenzációs kontroll a Rendelet szóhasználatában helyettesítő védelmi intézkedés.

*4.1. A helyettesítő védelmi intézkedés alkalmazása olyan eljárás, amelyet a szervezet az adott biztonsági osztályhoz tartozó védelmi intézkedés helyett kíván alkalmazni, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például jogszabályoknak vagy szervezeti szintű szabályozóknak) való megfelelést.
[7/2024. (VI. 24.) MK rendelet 1. melléklet 4.1. pont]*

¹³ A fogalom értelmezéséről lásd az MKIK-30 jogi állásfoglalást ([A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása](#)).

¹⁴ 2024. évi LXIX. tv. 6. § (6) bekezdés

Helyettesítő intézkedés négy együttes feltétellel alkalmazható. A katalógus nem tartalmaz az adott viszonyok között eredményesen és kockázatarányosan alkalmazható intézkedést. A Szervezet felméri és elfogadja a helyettesítéssel járó kockázatot. Dokumentumban bemutatja az egyenértékű védelmet, valamint azt, hogy az eredeti intézkedés miért nem használható. Végül az alkalmazást a vezetővel vagy a kockázatok felvállalására jogosult személlyel jóváhagyatja.¹⁵

Nyílt forráskódú szoftvernél a helyettesítés tipikus tárgya a beszerzések (16.7.) és a beszerzések során alkalmazandó védelmi intézkedések funkcionális tulajdonságai (16.8.) pontok, mert szerződő fél hiányában ezek betű szerint nem teljesíthetők. A szerződéses garanciát a saját átvételi vizsgálat és a verziók ellenőrzött kezelése pótolja, a gyártói hibajavítási kötelezettséget a sérülékenységek figyelése és a határidőhöz kötött frissítés (15.9. és 18.2.), a gyártói támogatást pedig a saját szakértelem és az eseti szakértői szerződés.

Nem minden intézkedés helyettesítő azonban, amelyet a Szervezet a nyílt forráskód miatt vezet be. A biztonságos konfigurációs beállítások (6.23.), a legszűkebb funkcionalitás (6.26.) és a kártékony kódok elleni védelem (18.8.) egyébként is kötelező, ezek a rendes kockázatkezelés eszközei. Formális helyettesítésre és jóváhagyásra csak ott van szükség, ahol egy kötelező követelmény az adott viszonyok között nem alkalmazható. A szoftverek sértetlenségének ellenőrzését a Rendelet jelentős és magas osztályban külön előírja (18.42.), alap osztályban ajánlott jó gyakorlat.

Az SZTFH auditrendelete az eltérésekről és a helyettesítő intézkedésekről külön nyilvántartást vár el, amely az érintett rendszert, a helyettesített követelményt, az eltérés okát, a releváns fenyegetéseket és a maradványkockázat felvállalásának indokát tartalmazza.¹⁶ Ezt a nyilvántartást a bevezetéssel egy időben érdemes kitölteni.

4.7 A jogszerű használat további feltételei

A szoftver szerzői jogi védelem alatt áll, felhasználásához engedély szükséges, amelyet nyílt forráskódú szoftvernél a licenc ad meg.¹⁷ A licenc elfogadásával felhasználási szerződés jön létre, amelyet a törvény ebben a körben nem köt írásbeli alakhoz.¹⁸ A licencfeltételek túllépése jogosulatlan felhasználás, és egyúttal a Rendelet megsértése is.

*6.47.1. Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak.
[7/2024. (VI. 24.) MK rendelet 2. melléklet 6.47.1. pont] (A, J, M)*

Változtatás nélküli, belső használatnál a legtöbb licenc kevés kötelezettséget ró a felhasználóra, mert a forráskód közzétételének kötelezettsége jellemzően a terjesztéshez vagy a módosított változat hálózati szolgáltatásként való nyújtásához kapcsolódik. A Szervezetnek ennek ellenére nyilvántartania kell a használt szoftvereket és licenceiket, különben nem tudja igazolni a megfelelést, és azt sem veszi észre, ha egy új verzió már más feltételekkel jelenik meg. Javasoljuk

¹⁵ 7/2024. (VI. 24.) MK rendelet 1. melléklet 4.2. pont

¹⁶ 1/2025. (I. 31.) SZTFH rendelet 5. § (1) bekezdés c) pont és 4. melléklet

¹⁷ 1999. évi LXXVI. tv. 1. § (2) bekezdés c) pont és 16. § (1) bekezdés

¹⁸ 1999. évi LXXVI. tv. 45. § (2) bekezdés c) és d) pont

a 6.48. pont (O) önkéntes alkalmazását, vagyis annak szabályozását, hogy ki, milyen forrásból és milyen licenccel vezethet be nyílt forráskódú szoftvert. A felhasználók általi szoftvertelepítés szabályozása minden osztályban kötelező (6.49.).

A jogszerű használat műszaki feltétele a támogatott állapot.

16.99. A szervezet:

16.99.1. lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve

16.99.2. a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.

[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.99. pont] (A, J, M)

Nyílt forráskódú szoftvernél a támogatás a közösség vagy a gyártó által karbantartott kiadási ágat jelenti. Ha az ág támogatása megszűnik, a Szervezetnek verziót kell váltania, vagy a 16.99.2. pont szerint alternatív támogatásról kell gondoskodnia. Ezt a forráskód hozzáférhetősége lehetővé teszi, de komoly szakértelmet kíván.

A kiberrezilienciáról szóló (EU) 2024/2847 rendelet nem a felhasználó Szervezetet, hanem a kereskedelmi tevékenység keretében forgalmazott termékek gyártóit kötelezi. A nem kereskedelmi céllal fejlesztett nyílt forráskódú szoftver kívül marad a hatályán, a projekteket fenntartó szervezetekre, vagyis a nyílt forráskódú szoftverek támogatóira pedig könnyített szabályok vonatkoznak.¹⁹ A gyártók bejelentési kötelezettsége 2026. szeptember 11. óta alkalmazandó, a rendelet egésze 2027. december 11-től.²⁰ A Szervezet ezért a közösségi projekteknél a jövőben sem számíthat CE-jelölésre, a kereskedelmi kiadásoknál viszont igen.

A bevezetés általános feltételei a nyílt forráskódú szoftverre is érvényesek. A változtatás előtt biztonsági hatásvizsgálat szükséges (6.15.), a használatbavételről pedig a vezető át nem ruházható feladatkörében, jegyzőkönyvben dönt.²¹ Személyes adatok kezelése esetén a szoftver kiválasztására és beállítására a beépített adatvédelem és az adatbiztonság követelménye is vonatkozik.²² Ha a támogatást nyújtó cég hozzáfér a személyes adatokhoz, adatfeldolgozói szerződést is kötni kell.²³

4.8 A közzsférába tartozó szervezetek

A Kiberbiztonsági tv. 1. § (1) bekezdés a), b), c) és f) pontja szerinti szervezetekre a 418/2024. (XII. 23.) Korm. rendelet szervezeti kötelezettségei is vonatkoznak, az SZTFH felügyelete alá tartozó Szervezetre főszabály szerint nem.²⁴ A támogató rendszer fogalma az a), b) és c) pont szerinti szervezeteknél kétség nélkül alkalmazható. A védelmi intézkedések meghatározásakor

¹⁹ (EU) 2024/2847 rendelet (18) és (19) preambulumbekzdés, 24. cikk

²⁰ (EU) 2024/2847 rendelet 71. cikk (2) bekezdés. Az alkalmazáshoz az Európai Bizottság 2026. július 27-én iránymutatást tett közzé, C(2026) 5252.

²¹ 2024. évi LXIX. tv. 6. § (3) bekezdés 12. pont; 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.6. pont

²² (EU) 2016/679 rendelet (GDPR) 25. és 32. cikk; Európai Adatvédelmi Testület, 4/2019. számú iránymutatás a beépített és alapértelmezett adatvédelemről, 2.0 verzió (2020. október 20.)

²³ (EU) 2016/679 rendelet (GDPR) 28. cikk (3) bekezdés

²⁴ 418/2024. (XII. 23.) Korm. rendelet 1. § (1) bekezdés

ebben a körben figyelembe kell venni a kritikus ellátási láncokra készült uniós összehangolt kockázatértékelések eredményeit.²⁵ A helyettesítő védelmi intézkedéseket be kell jelenteni a nemzeti kiberbiztonsági hatóságnak,²⁶ a vezető használatbavételi döntésének hatósági jóváhagyását pedig kérelmezni kell.²⁷ A 4.4., 4.5., 4.6. és 4.7. pontban írtak egyebekben rájuk is irányadók.

5. FELHASZNÁLT FORRÁSOK

- [Az Európai Parlament és a Tanács \(EU\) 2022/2555 irányelve \(NIS 2 irányelv\)](#)
- [Az Európai Parlament és a Tanács \(EU\) 2024/2847 rendelete \(kiberrezilienciáról szóló rendelet, CRA\)](#)
- [Az Európai Parlament és a Tanács \(EU\) 2016/679 rendelete \(általános adatvédelmi rendelet, GDPR\)](#)
- [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](#)
- [1999. évi LXXVI. törvény a szerzői jogról](#)
- [NBSZ Nemzeti Kiberbiztonsági Intézet, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, 16. Rendszer- és szolgáltatásbeszerzés \(V.1.3, 2026\) és 19. Ellátási lánc kockázatkezelése \(V.1.2, 2026\)](#)
- [ENISA, Good Practices for Supply Chain Cybersecurity \(2023. június\)](#)
- [ENISA, Technical implementation guidance on cybersecurity risk management measures \(1.0 verzió, 2025. június\)](#)
- [Európai Bizottság, iránymutatás a kiberrezilienciáról szóló rendelet alkalmazásáról, C\(2026\) 5252 \(2026. július 27.\)](#)
- [Európai Adatvédelmi Testület, 4/2019. számú iránymutatás a beépített és alapértelmezett adatvédelemről \(2.0 verzió, 2020\)](#)
- [NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations \(2022, frissítve 2024\)](#)
- [BSI TR-03183, Cyber Resilience Requirements for Manufacturers and Products, Part 2 Software Bill of Materials \(SBOM\)](#)
- [OpenSSF Scorecard](#)

²⁵ 418/2024. (XII. 23.) Korm. rendelet 4. § (1) bekezdés

²⁶ 418/2024. (XII. 23.) Korm. rendelet 8. § (2) bekezdés b) pont

²⁷ 418/2024. (XII. 23.) Korm. rendelet 14. § (1) bekezdés

- [MKIK-30 jogi állásfoglalás, A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása](#)

6. KAPCSOLÓDÓ MKIK-ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- [MKIK-30 – A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása](#)
- [2026/10 - A KÖZREMŰKÖDŐVEL KÖTÖTT SZERZŐDÉS TARTALMA](#)
- [MKIK-49 – Milyen vonzatai vannak egy szerverbeszerzésnek NIS2-kötelezett vállalkozás esetén? Lehetséges-e használt szervert vásárolni?](#)
- [MKIK-38 – Nem támogatott operációs rendszerek NIS2-kompatibilis használata](#)
- [MKIK-58 – Hardening - MENNYIRE ELLENÁLLÓ A RENDSZERÜNK? Hogyan határozzuk meg, vezessük be és tartsuk fenn rendszereink biztonsági alapkonfigurációját?](#)

További MKIK NIS2 jogi állásfoglalások és szakmai iránymutatások (az oldal alján lapozva) elérhetőek a Tudásközpontban.

[MKIK Jogi állásfoglalások](#) és [MKIK Iránymutatások](#)

1. MELLÉKLET

A nyílt forráskódú szoftverek használatához kapcsolódó követelmények a 7/2024. (VI. 24.) MK rendelet 2. melléklete alapján

A táblázat a nyílt forráskódú szoftverek saját üzemeltetésű használatánál érintett követelményeket tartalmazza, a követelmény rendeletbeli megnevezésével és a biztonsági osztály jelölésével. A jelölés Alap (A), Jelentős (J) és Magas (M) osztályban kötelező, illetve egyik osztályban sem kötelező, kiegészítő (O) követelményt jelent. Az Állásfoglalás pontja oszlop azt mutatja, hogy az állásfoglalás mely pontja tárgyalja a követelményt, a kötőjel azt, hogy a követelményt csak a táblázat említi. A táblázat a Rendelet 2025. január 2-től hatályos szövege alapján készült, és nem helyettesíti a rendszerre vonatkozó teljes követelménykatalógus alkalmazását.

Pont	Követelmény	Osztály	Állásfoglalás pontja	Teljesítés nyílt forráskódú szoftver esetén
Szervezeti keretek				
1.5.	Elektronikus információs rendszerek nyilvántartása	A, J, M	4.2.	Az EIR-ek nyilvántartása a támogató rendszerek elkülönített feltüntetésével.
1.21.	Ellátási lánc kockázatmenedzsment stratégiája	A, J, M	4.4.	A nyílt forráskódú projektekre is kiterjedő ellátásilánc-stratégia.
1.22.	Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói	A, J, M	4.4.	A kritikus EIR-ek mögött álló projektek és támogatók azonosítása és rangsorolása.
16.1.	Szabályzat és eljárásrendek	A, J, M	-	A beszerzési szabályzat kiterjesztése az ellenérték nélkül megszerzett szoftverekre.
16.2.	Erőforrások rendelkezésre állása	A, J, M	3.2.	Az üzemeltetés, a frissítés és a szakértelem költségének elkülönített tervezése.
19.1.	Szabályzat és eljárásrendek	A, J, M	-	Az ellátási láncra vonatkozó szabályzat és eljárásrend.
19.2.	Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	A, J, M	4.4.	A nyílt forráskódú szoftverek kiválasztásának és kivezetésének szabályai.
Kockázatelemzés és ellátási lánc				
15.4.	Kockázatelemzés	A, J, M	4.4.	Rendszerszintű kockázatelemzés a nyílt forráskódú elemekre is.
15.5.	Kockázatelemzés – Ellátási lánc	A, J, M	3.3., 4.4.	A projekt, a terjesztési csatorna és a függőségek kockázatainak felmérése, változás esetén frissítése.
15.21.	Rendszerelemek kritikusságának elemzése	J, M	4.4.	A kritikus nyílt forráskódú rendszerelemek azonosítása.
19.4.	Ellátási láncra vonatkozó követelmények és folyamatok	A, J, M	4.4.	Folyamat az ellátási lánc gyengeségeinek azonosítására és kezelésére.
19.13.	Beszerzési stratégiák, eszközök és módszerek	A, J, M	3.2.	A támogatási modell megválasztása mint beszerzési stratégia.
19.16.	Beszállítók értékelése és felülvizsgálata	J, M	4.4.	A projektek és a támogatók rendszeres újraértékelése.

Pont	Követelmény	Osztály	Állásfoglalás pontja	Teljesítés nyílt forráskódú szoftver esetén
19.19.	Értesítési megállapodások	A, J, M	4.5.	Feliratkozás a projekt biztonsági értesítéseire, belső értékelési eljárásrend.
Szerződés és dokumentáció				
16.7.	Beszerzések	A, J, M	4.5., 4.6.	Szerződés a támogatóval vagy az integrátorral, ennek hiányában belső követelményjegyzék és dokumentált eltérés.
16.8.	Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai	A, J, M	4.5., 4.6.	A védelmi funkciók leírásának összegyűjtése a projekt dokumentációjából.
16.9.	Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez	J, M	-	Tervezési információk a nyilvános forráskódból és dokumentációból.
16.15.	Az elektronikus információs rendszerre vonatkozó dokumentáció	A, J, M	4.5.	Üzemeltetői és felhasználói dokumentáció beszerzése vagy saját kidolgozása.
19.7.	Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók	A, J, M	4.5.	A követelmények továbbhárítása az integrátor alvállalkozóra.
10.11.	Távoli karbantartás	A, J, M	4.5.	A támogató távoli hozzáféréseinek jóváhagyása és ellenőrzése.
Szoftverhasználat és konfiguráció				
6.47.	A szoftverhasználat korlátozásai	A, J, M	4.7.	Licencnyilvántartás, a licencfeltételek betartása.
6.48.	A szoftverhasználat korlátozásai – Nyílt-forráskódú szoftver	O	4.1., 4.7.	Szabályzat az engedélyezett forrásokról, licencekről és a bevezetés rendjéről.
6.49.	Felhasználó által telepített szoftver	A, J, M	4.7.	A felhasználók általi telepítés szabályozása és ellenőrzése.
6.53.	Aláírt rendszerelemek	O	-	Csak ellenőrzött aláírási csomagok telepítése.
6.2.	Alapkonfiguráció	A, J, M	3.4.	Dokumentált alapkonfiguráció a telepített verzióról.
6.15.	Biztonsági hatásvizsgálatok	A, J, M	4.7.	Biztonsági hatásvizsgálat a bevezetés és a főverzióváltás előtt.
6.23.	Konfigurációs beállítások	A, J, M	4.6.	Megerősített konfigurációs beállítások.
6.26.	Legszűkebb funkcionalitás	A, J, M	4.6.	A szükségtelen modulok és szolgáltatások kikapcsolása.
6.36.	Rendszerelem leltár	A, J, M	3.3., 4.2.	A szoftver, a verzió, a licenc és a függőségek szerepeltetése a leltárban.
Sérülékenységek, frissítés és sértetlenség				
15.9.	Sérülékenységek ellenőrzése	A, J, M	4.6.	A projekt és a függőségek sérülékenységeinek figyelése és javítása határidőre.
15.10.	Sérülékenységhozzájárulás	J, M	-	Automatizált sérülékenységvizsgálat.
18.2.	Hibajavítás	A, J, M	4.6.	Tesztelt, határidőhöz kötött frissítés.
18.37.	Biztonsági riasztások és tájékoztatások	A, J, M	4.5.	A projekt és a hatóságok biztonsági riasztásainak fogadása.
16.99.	Támogatással nem rendelkező rendszerelemek	A, J, M	4.7.	Verzióváltás a támogatás lejártá előtt, vagy alternatív támogatás.

Pont	Követelmény	Osztály	Állásfoglalás pontja	Teljesítés nyílt forráskódú szoftver esetén
18.8.	Kártékony kódok elleni védelem	A, J, M	4.6.	A letöltött telepítőkészletek kártevő-ellenőrzése.
18.42.	Szoftver- és információsértetlenség	J, M	4.6.	Aláírás és ellenőrző összeg vizsgálata, sértetlenségellenőrzés.
19.22.	Rendszerek vagy rendszerelemek vizsgálata	A, J, M	-	A telepítőkészletek eredetiségének eseti ellenőrzése.
19.23.	Rendszerelem hitelessége	A, J, M	-	Eljárás a hamisított csomagok észlelésére és jelentésére.

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](#). További információ a nis2.mkik.hu weboldalon található. A dokumentum oldala a Tudástárban [\[URL később kitöltendő\]](#)