

Külső adathordozók NIS2-kompatibilis használata

VFP3 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/62

Kiadó: Magyar Kereskedelmi és Iparkamara. Készítette: Kálmán és Társa Ügyvédi Iroda. Közzétéve: 2026.
szeptember 30. Elérhető az [MKIK NIS2-Tudástárban](#).

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.30	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

- **A külső adathordozó a NIS2 hatálya alatt sem tilos, de csak szabályozott kivétel lehet. A Kiberbiztonsági tv. védelmi intézkedéseit részletező 7/2024. (VI. 24.) MK rendelet nem tiltja a pendrive, a külső SSD vagy a külső merevlemez használatát. Minden biztonsági osztályban elvárja viszont, hogy a Szervezet eldöntse, mely eszközöket, mely rendszereken és milyen mechanizmussal korlátoz vagy tilt, és a döntést technikailag is érvényesítse.**
- **Az alapállás a technikai tiltás, a használatához szervezeti indok és engedély kell.** A felhő-, adatközpont- és irányított szolgáltatókra közvetlenül alkalmazandó (EU) 2024/2690 végrehajtási rendelet ezt kifejezetten előírja, a többi Szervezetnél pedig ez a megoldás igazolható a legkönnyebben.
- **Csak a Szervezet saját, nyilvántartott, személyhez rendelt eszköze csatlakoztatható.** Az azonosítható tulajdonos nélküli, például talált eszközt a rendelet minden osztályban tiltja, a magáneszközök kizárásáról pedig a Szervezetnek kell döntenie.
- **Adat csak titkosítva kerülhet külső adathordozóra.** Jelentős és magas osztályban a rendelet a tárolt adatok kriptográfiai védelmét írja elő, alap osztályban a GDPR és az incidenskockázat teszi szükségessé. A megfelelően titkosított eszköz elvesztését jellemzően nem kell a NAIH-nak bejelenteni, a titkosítatlanét általában igen.
- **Az adminisztratív és a technológiai kontrollok csak együtt igazolhatók.** A szabályzat, a nyilvántartás, a felhasználói nyilatkozat, a képzés és a bejelentési rend mellé engedélyezőlistás eszközvezérlés, kártevő-ellenőrzés, kényszerített titkosítás, naplózás és tanúsított törlés kell.

2. A VIZSGÁLANDÓ KÉRDÉS

A vizsgálandó kérdés az, hogy a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban mint „Kiberbiztonsági tv.”) és a 7/2024. (VI. 24.) MK rendelet (a továbbiakban mint „Rendelet”) alapján milyen feltételekkel használhatók ezek az eszközök, milyen adminisztratív és technológiai kontrollok szükségesek, és milyen szoftverek és technológiák segítik a megfelelést.

Külső adathordozón a pendrive-ot, a memóriakártyát, a külső SSD-t és a külső merevlemezt értjük, a mobiltelefonok és a felhőtárhelyek nem tárgyai az állásfoglalásnak.

3. GYAKORLATI JAVASLATOK

3.1 A használat hat feltétele

Álláspontunk szerint külső adathordozó egy NIS2-kötelezett Szervezetnél akkor használható, ha az alábbi hat feltétel együttesen teljesül.

- a) Szervezeti indok és engedély. A használathoz dokumentált üzleti ok és a felhasználóra vagy a szerepkörre szóló engedély tartozik, minden más esetben a csatlakoztatást technikai eszköz akadályozza meg.
- b) Szervezeti eszköz. Csak a Szervezet által beszerezett, nyilvántartott és név szerint kiadott eszköz csatlakoztatható, [magán-](#), talált vagy ajándékba kapott eszköz nem.
- c) Titkosítás. Az eszközre csak titkosítva kerülhet adat, lehetőleg hardveresen titkosított eszközre, a helyreállítási kulcsok központi megőrzésével.
- d) Ellenőrzött csatlakoztatás. Az eszközről nem indulhat automatikusan program, tartalmát a kártevővédelem megnyitás előtt átvizsgálja, ipari hálózatba pedig csak ellenőrző állomáson átvizsgált eszköz kerülhet.
- e) Adattakarékosság. Az eszközre csak a feladathoz szükséges adat kerül, és csak a szükséges ideig marad rajta.
- f) Elszámoltathatóság. A kiadás, a szállítás, a visszavétel és a megsemmisítés nyomon követhető, a csatlakoztatásokat és a másolásokat a rendszer naplózza.

3.2 Adminisztratív kontrollok

Az adminisztratív kontrollok közül a következőket tartjuk nélkülözhetetlennek.

- a) Szabályzat és esetleg eljárásrend az engedélyezett eszközökről és rendszerekről, az engedélyezés, a titkosítás és a törlés rendjéről, a felelős kijelölésével.
- b) Felhasználói nyilatkozat a szabályok megismeréséről, a hozzáférés megadása előtt.
- c) Eszköznyilvántartás a sorozatszámmal, a birtokossal, a kiadás, a visszavétel és a megsemmisítés adataival.
- d) Képzés a talált eszközök és a megtévesztésen alapuló támadások veszélyeiről.
- e) Bejelentési kötelezettség az elvesztésre, a lopásra és a talált eszközre.
- f) Szállítási, tárolási és törlési szabályok, a törlésről jegyzőkönyvvel vagy tanúsítvánnyal.
- g) Szerződéses kikötések a közreműködők saját eszközeiről.

3.3 Technológiai kontrollok

A technológiai kontrollok célja, hogy a szabályzat betartása ne a felhasználók fegyelmén múljon.

- a) Eszközvezérlés (device control), amely alapértelmezetten tiltja a tárolóeszközöket, és csak az engedélyezőlistán szereplő eszközt engedi sorozatszám alapján, szükség esetén csak olvasásra, kritikus rendszeren fizikai portzárral kiegészítve.
- b) Az automatikus futtatás tiltása és az adathordozóról induló, nem megbízható programok blokkolása.
- c) Valós idejű kártevő-ellenőrzés, ipari környezetben ellenőrző állomással (kioszk).
- d) Kényszerített titkosítás, vagyis írás csak titkosított eszközre.
- e) Naplózás és riasztás a központi naplógyűjtőben, a bizalmas fájlok másolásánál adatszivárgás-megelőzéssel (DLP).
- f) Védelem a billentyűzetnek álcázott eszközök (BadUSB) ellen az eszköztelepítés korlátozásával.

Bevezetéskor érdemes az eszközvezérlést néhány hétig naplózó üzemmódban futtatni, és csak a tényleges használat felmérése, a szabályzat elfogadása és a titkosított eszközök kiosztása után tiltó üzemmódra állítani.

3.4 Konkrét szoftverek és technológiák

Az alábbi táblázat funkciók szerint mutat példákat. Érdemes a Szervezet meglévő végpontvédelmi és identitáskezelési környezetéből kiindulni, mert az eszközvezérlés, a titkosítás és az adatszivárgás-megelőzés gyakran egy már megvásárolt licenc része. A felsorolás nem teljes körű, és nem termékajánlás (lásd az 5. pontot).

Funkció	Példák	Mire figyeljünk
Eszközvezérlés	Windows csoportházirend („Removable Storage Access”, „Device Installation Restrictions”); Microsoft Defender for Endpoint Device control (Intune); az ESET PROTECT, a Sophos Central, a Bitdefender GravityZone, a CrowdStrike Falcon, a SentinelOne Singularity, a Trellix és az Ivanti eszközvezérlő modulja; macOS-en Jamf Protect, Linuxon USBGuard	Az engedélyezés sorozatszám szintjén történjen. A támogatott platformokat, különösen a kiszolgáltatókat, a bevezetés előtt ellenőrizni kell.
Futtatásvédelem és kártevőgátlás	A végpontvédelem valós idejű ellenőrzése; a Microsoft Defender „Block untrusted and unsigned processes that run from USB” szabálya; alkalmazás-engedélyezőlista (App Control for Business, AppLocker)	Az automatikus lejártszám tiltását házirendben kell rögzíteni.
Ellenőrző állomás (kioszk)	OPSWAT MetaDefender Kiosk és Media Firewall; Honeywell Secure Media Exchange (SMX); tartalomhatástanító (CDR) megoldások, például OPSWAT Deep CDR vagy Glasswall	Ipari és elkülönített hálózaton indokolt. A 2020 óta nem fejlesztett CIRCLean nem javasolt.
Szoftveres titkosítás	BitLocker To Go, csoportházirenddel kényszerítve („Deny write access to removable drives not protected by BitLocker”); macOS-en titkosított APFS-kötet; Check Point Harmony Endpoint Media Encryption; Netwrix Endpoint Protector EasyLock; VeraCrypt	A helyreállítási kulcsok megőrzését külön meg kell tervezni és tesztelni. A VeraCrypt központi kulcskezelést nem nyújt.
Hardveresen titkosított eszköz	FIPS 140-3 szerinti 3. szintű tanúsítvánnyal például Kingston IronKey D500S és Keypad 200, Apricorn Aegis Secure Key 3.0, iStorage datAshur PRO+C, DataLocker Sentry K350, külső meghajtóként DataLocker DL4 FE; központi felügyelet DataLocker SafeConsole	A NIST 2026 szeptemberében a FIPS 140-2 tanúsítványokat a történeti listára helyezte, új beszerzésnél FIPS 140-3 tanúsítványt érdemes elvárni.
Adatszivárgás-megelőzés (DLP)	Microsoft Purview Endpoint DLP; Forcepoint DLP; Fortra DLP (korábban Digital Guardian); Trellix DLP Endpoint; Netwrix Endpoint Protector; Safetica	A tartalomvizsgálat személyes adatot érinthet, adatvédelmi hatásvizsgálat lehet szükséges.
Naplózás	Windows naplózás (6416-os és 4663-as esemény); a Defender for Endpoint USB-eseményei (PnpDeviceConnected, UsbDriveMounted, RemovableStoragePolicyTriggered); SIEM-rendszer	A naplózandó eseményeket a naplózási szabályzatban rögzíteni kell.
Törlés és megsemmisítés	Blancco Drive Eraser, Stellar BitRaser; kriptográfiai törlés titkosított eszközön; fizikai megsemmisítés az ISO/IEC 21964 (DIN 66399) szerint	Pendrive-on és SSD-n a felülírásos törlés nem megbízható.

A termékválasztás az ellátási lánc kockázatkezelésének is része, ezért a gyártó eredetét, tulajdonosi hátterét és az esetleges hatósági figyelmeztetéseket is mérlegelni kell.¹

¹ A német szövetségi informatikai biztonsági hivatal (BSI) 2022. március 15-én például figyelmeztetést adott ki, és a Kaspersky vírusvédelmi termékeinek lecserélését javasolta.

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) pontja alá tartozik, és kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el.² A válasz lényege a többi szervezettípusra is irányadó, a közszféra eltéréseit a 4.6. pont foglalja össze.

A törvény az általános alapelvek között a védelem tárgyaként az adathordozókat is megnevezi.

(2) Az elektronikus információs rendszer védelme keretében az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezet, az adatkezelő vagy az adatfeldolgozó által, adott cél érdekében

a) az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat

b) az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint

c) az a) és b) pontban foglaltakat kezelő személyek

együttesének védelmét is biztosítani szükséges. [2024. évi LXIX. tv. 5. §

(2) bekezdés]

Álláspontunk szerint a csatlakoztatott külső adathordozó az elektronikus információs rendszer része, a rajta tárolt adat pedig a rendszer adata.³ A Szervezet vezetőjének ezért az információbiztonsági szabályzatban az adathordozókról is rendelkeznie kell, és gondoskodnia kell a védelmi intézkedések teljesüléséről.⁴

A részletes követelményeket a Rendelet 2. mellékletének 11. követelménycsoportja (Adathordozók védelme) tartalmazza, amelyet a 2., 6., 17. és 18. követelménycsoport több pontja egészít ki. A Nemzeti Kiberbiztonsági Intézet alkalmazási útmutatója az adathordozók között kifejezetten említi a külső és cserélhető merevlemezt és a flash meghajtót.⁵ Az érintett követelményeket a Rendelet szerinti pontszámukkal és biztonsági osztályonként az 1. melléklet foglalja össze.

4.2 A használat feltételeinek jogi alapja

A Rendelet nem tiltja a külső adathordozókat, hanem döntést és annak kikényszerítését várja el. A 11.14. pont (A, J, M) két kötelezettséget ír elő.

11.14.1. Korlátozza vagy tiltja a szervezet által meghatározott típusú adathordozók használatát a szervezet által meghatározott EIR-eken vagy rendszerelemeken, a szervezet által meghatározott irányítási mechanizmusok alkalmazásával.

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

³ 2024. évi LXIX. tv. 4. § 24. pont b) és c) alpont

⁴ 2024. évi LXIX. tv. 6. § (3) bekezdés 7. és 8. pont

⁵ NBSZ Nemzeti Kiberbiztonsági Intézet, Alkalmazási Útmutató, 11. Adathordozók védelme, V.1.2 (2026). Elérhető az NKI honlapján.

*11.14.2. Megtiltja a hordozható adattároló eszközök használatát a szervezeti EIR-ekben, ha azoknak nincs azonosítható tulajdonosa.
[7/2024. (VI. 24.) MK rendelet 2. melléklet 11.14. pont] (A, J, M)*

A 11.14.1. pont (A, J, M) alapján a Szervezetnek meg kell határoznia, mely eszköztípusok használhatók, mely rendszereken, és milyen mechanizmus érvényesíti a szabályt. A pusztai írásbeli tilalom ezt álláspontunk szerint nem teljesíti. Ha az auditor mintavételkor egy nem engedélyezett pendrive-ot csatlakoztat, és az működik, a követelmény nem teljesül.

A 11.14.2. pont (A, J, M) a talált vagy ismeretlen eredetű eszközt zárja ki. A magáneszközt a Rendelet kifejezetten nem tiltja, hiszen annak van tulajdonosa. Kizárásáról a Szervezet a 11.14.1. pont (A, J, M) alapján dönt, és álláspontunk szerint ezt minden osztályban meg kell tennie, mert a magáneszköz előéletéről és védelméről nincs információja. Ezt a megoldást írja le példaként a Nemzeti Kiberbiztonsági Intézet útmutatója, és ezt javasolja a német szövetségi informatikai biztonsági hivatal (BSI) is.⁶

Az elvet a legvilágosabban az (EU) 2024/2690 bizottsági végrehajtási rendelet fogalmazza meg, amely többek között a felhő-, adatközpont-, DNS- és irányított szolgáltatókra, valamint a bizalmi szolgáltatókra közvetlenül alkalmazandó.⁷ Az eltávolítható adathordozókra vonatkozó szabályzatnak a rendelet szerint a következőket kell tartalmaznia.

- a) rendelkeznie kell az eltávolítható adathordozók csatlakoztatásának technikai tilalmáról, kivéve, ha használatuknak szervezeti oka van;*
- b) rendelkeznie kell az ilyen adathordozókról történő automatikus végrehajtás megakadályozásáról, valamint azoknak a rosszindulatú kódok tekintetében történő átvizsgálásáról az érintett szervezetek rendszereiben való felhasználást megelőzően;*
- c) intézkedéseket kell előírnia az adatokat tartalmazó hordozható tárolóeszközök ellenőrzésére és védelmére az adatátvitel és a tárolás során;*
- d) ha indokolt, intézkedéseket kell előírnia kriptográfiai technikák alkalmazására az eltávolítható adathordozókon tárolt adatok védelme érdekében. [(EU) 2024/2690 bizottsági végrehajtási rendelet melléklet 12.3.2. pont]*

A többi Szervezetre a végrehajtási rendelet közvetlenül nem vonatkozik, a négy elem azonban megfeleltethető a Rendelet 11.14. (A, J, M), 18.8. (A, J, M), 11.6. (J, M) és 17.82. (J, M) pontjának, valamint az adathordozók ellenőrzött tárolására vonatkozó követelménynek.⁸ A technikai tiltás és az indokolt kivétel rendszere ezért minden NIS2-kötelezett Szervezetnél a legkönnyebben igazolható megoldás.

⁶ NKI alkalmazási útmutató, a 11.14. ponthoz (A, J, M) fűzött magyarázat; BSI IT-Grundschutz-Kompendium, SYS.4.5.A4 (Edition 2023)

⁷ (EU) 2024/2690 végrehajtási rendelet 1. cikk; 2024. évi LXIX. tv. 6. § (2) bekezdés

⁸ Jó mérce az ENISA Technical implementation guidance on cybersecurity risk management measures, 1.0 verzió (2025. június), 12.3. pont.

Jelentős és magas osztályban a Szervezet eszközének külső rendszerben, például egy partner vagy a munkatárs otthoni számítógépén történő használatát korlátozni kell, a visszahozott eszközt pedig újra ellenőrizni. Magas osztályban a hordozható tárolóeszközt a Szervezet által meghatározott esetekben csatlakoztatás előtt roncsolásmentes technikával törölni is kell, ami a gyakorlatban az új vagy kívülről érkező eszköz első használat előtti törlését jelenti.

4.3 Az adminisztratív kontrollok jogi alapja

Az adminisztratív kontrollok gerince az adathordozók védelmére vonatkozó írásos szabályzat és eljárásrend, amelyet a Rendelet minden osztályban előír, a felelős kijelölésével és rendszeres felülvizsgálattal együtt. Szintén minden osztályban kötelező, hogy a felhasználó a hozzáférés engedélyezése előtt dokumentált nyilatkozatban igazolja, hogy a rá vonatkozó szabályokat megismerte és betartja. A biztonságtudatossági képzés minden osztályban, a pszichológiai manipuláció felismerését célzó képzés jelentős és magas osztályban kötelező. Egy egyetemi kísérletben az elhagyott pendrive-ok 98 százalékát elvitték, és legalább 45 százalékukon a fájlokat is megnyitották.⁹

A nyilvántartás az adathordozókhoz való hozzáférés minden osztályban kötelező korlátozásának és a 11.14. pont (A, J, M) teljesítésének is feltétele, hiszen a hozzáférést csak az tudja korlátozni, aki tudja, melyik eszköz kié. A kiadott eszközöket célszerű a minden osztályban kötelező rendszerelem-leltárban is szerepeltetni, a jogviszony megszűnésekor pedig vissza kell venni őket. Jelentős és magas osztályban az adathordozókat meg kell jelölni és ellenőrzött helyen kell tárolni, szállításukra pedig részletes szabályok vonatkoznak.

11.6.1. A szervezet által meghatározott védelmi intézkedéssel védi és ellenőrzi az adathordozókat az ellenőrzött területen kívülre történő szállítás alatt.

11.6.2. Biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás alatt.

11.6.3. Dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket.

11.6.4. A jogosult személyekre korlátozza az adathordozók szállításával kapcsolatos tevékenységeket. [7/2024. (VI. 24.) MK rendelet 2. melléklet 11.6. pont] (J, M)

A mentést tartalmazó merevlemez telephelyen kívüli őrzőhelyre vitele is ilyen szállítás. A Szervezet által meghatározott típusú rendszerelemek be- és kiszállításának engedélyezése és nyilvántartása minden osztályban kötelező.

A biztonságos törlés minden osztályban kötelező a selejtezés, a Szervezet ellenőrzési körén kívülre kerülés és az újrafelhasználás előtt, az adatok besorolásával arányos módszerrel. Magas osztályban a törlést jóvá kell hagyni, dokumentálni és ellenőrizni, a törlőberendezéseket és a törlési eljárásokat pedig tesztelni kell. Pendrive-on és SSD-n a felülírással történő törlés nem megbízható, ezért ezeknél a kriptográfiai törlés vagy a fizikai megsemmisítés a biztos módszer.¹⁰

⁹ Tischer, M. et al., Users Really Do Plug in USB Drives They Find, IEEE Symposium on Security and Privacy, 2016

¹⁰ NIST SP 800-88 Rev. 2 (2025); IEEE 2883-2022. A fizikai megsemmisítésre az ISO/IEC 21964 szabványsorozat irányadó, a pendrive és az SSD az E, a mágneses merevlemez a H kategóriába tartozik.

A személyzetet minden osztályban kötelezni kell a biztonsági esemény gyanújának jelentésére, ide tartozik az eszköz elvesztése és a talált eszköz is. A közreműködők eszközhasználatát szerződésben kell rendezni,¹¹ jelentős és magas osztályban pedig a karbantartók diagnosztikai adathordozóit használat előtt kártékony kódra kell ellenőrizni.

4.4 A technológiai kontrollok jogi alapja

A Szervezet minden osztályban meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat. Jelentős és magas osztályban a szükségtelen portokat ki kell kapcsolni, meg kell akadályozni a szabályzattal ellentétes programfuttatást, és engedélyezőlistával kell biztosítani, hogy csak az engedélyezett szoftverek fussanak. Magas osztályban a jogosulatlan hardvert automatizáltan észlelni kell. A nem engedélyezett hardver kifejezett tilalma és a portok letiltása egyik osztályban sem kötelező, az eszközvezérlő szoftver azonban a kötelező követelmények teljesítése során ezeket is megvalósítja.

A kártevők elleni védelem minden osztályban kötelező, és kifejezetten a rendszer belépési pontjaira vonatkozik.

18.8.1. Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat. [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.8. pont] (A, J, M)

A külső adathordozó tipikus belépési pont, a 18.8. pont (A, J, M) pedig a külső forrásból származó fájlok valós idejű ellenőrzését is előírja megnyitáskor vagy futtatáskor.

Jelentős és magas osztályban a Rendelet a tárolt adatok védelmét általánosan is előírja, a titkosítást pedig a 17.82. pont (J, M) teszi kifejezetté.

17.82. A szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmaz a szervezet által meghatározott tárolt vagy archivált adatok jogosulatlan felfedésének és módosításának megelőzésére. [7/2024. (VI. 24.) MK rendelet 2. melléklet 17.82. pont] (J, M)

A titkosítandó adathordozók körét a Szervezet határozza meg, a külső eszközök azonban álláspontunk szerint ebből ésszerűen nem hagyhatók ki, mert náluk a legnagyobb az elvesztés kockázata. Alap osztályban is kötelező a kriptográfia felhasználási területeinek meghatározása, és ha személyes adat vagy üzleti titok külső eszközön is tárolható, a titkosítás mellőzése itt is nehezen indokolható. A kriptográfiai kulcsokat minden osztályban meghatározott követelmények szerint kell előállítani és kezelni, magas osztályban pedig a kulcsok elvesztése esetén is biztosítani kell az adatok rendelkezésre állását. Ezt a helyreállítási kulcsok központi megőrzése biztosítja, amely a többi osztályban is javasolt.

¹¹ 2024. évi LXIX. tv. 6. § (5) bekezdés d) pont

A naplózandó eseményeket minden osztályban a Szervezet határozza meg, a vezető pedig gondoskodik az események nyomkövethetőségéről.¹² Ide célszerű felvenni a csatlakoztatást, a blokkolt csatlakoztatási kísérletet és a fájlmásolást.

4.5 Adatvédelmi és munkajogi összefüggések

A személyes adatot tartalmazó adathordozó elvesztése adatvédelmi incidens. A GDPR a titkosítást a megfelelő biztonsági intézkedések között nevesíti, és ha az adat az illetéktelen személy számára értelmezhetetlen, az érintettek tájékoztatása alól is mentesít.¹³ Az Európai Adatvédelmi Testület példái szerint a titkosított, mentéssel rendelkező eszköz ellopását nem kell bejelenteni, csak nyilvántartásba venni, a titkosítatlanét viszont a hatóságnak és az érintetteknek is.¹⁴ A NAIH 5 millió forint bírsággal sújtott egy rendőri szervet, amelynek mintegy 1700 munkatárs adatait tartalmazó, jelszó és titkosítás nélküli pendrive-ja elveszett, és az incidenst késve jelentette be.¹⁵

A naplózás, különösen a fájlok tartalmát is vizsgáló adatszivárgás-megelőzés, [a munkavállalók ellenőrzésének minősül](#). A munkavállalót erről előzetesen írásban tájékoztatni kell, és az ellenőrzésnek az adatvédelmi alapelveknek is meg kell felelnie. [A munkáltató által biztosított eszköz](#) eltérő megállapodás hiányában csak a munkaviszony teljesítése érdekében használható, ez a magáncélú adathordozó-használat korlátozásának munkajogi alapja.¹⁶

4.6 A közszférába tartozó szervezetek

A 418/2024. (XII. 23.) Korm. rendelet az adathordozókra külön szabályt nem tartalmaz, a fentiek ezért a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetekre is irányadók. Az eltérés a bejelentendő események körében van. E szervezetek az incidenseken túl az incidensközeli helyzeteket és a fenyegetéseket is haladéktalanul bejelentik, az üzleti szféra szervezetei viszont csak a súlyos zavart, vagyoni hátrányt vagy jelentős kárt okozó eseményeket.¹⁷ Az első bejelentés határideje mindkét körben 24 óra.¹⁸ Egy elveszett vagy fertőzött adathordozó ezért a közszférában szinte mindig bejelentendő. Az adathordozó-szabályzat betartásának ellenőrzése az elektronikus információs rendszer biztonságáért felelős személy feladatai közé is tartozik.¹⁹

¹² 2024. évi LXIX. tv. 6. § (5) bekezdés c) pont

¹³ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet, GDPR) 32. cikk (1) bekezdés a) pont és 34. cikk (3) bekezdés a) pont

¹⁴ Európai Adatvédelmi Testület, 01/2021. számú iránymutatás az adatvédelmi incidensek bejelentésével kapcsolatos példákról, 2.0 verzió (2021. december 14.), 10. és 11. eset

¹⁵ NAIH/2019/2471/6. számú határozat (2019. június 25.)

¹⁶ 2012. évi I. tv. 11/A. § (1) és (2) bekezdés; a Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről (2016)

¹⁷ 2024. évi LXIX. tv. 66. § (1) és (2) bekezdés

¹⁸ 418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1. pont

¹⁹ 418/2024. (XII. 23.) Korm. rendelet 12. § (2) bekezdés g) és h) pont

5. FELELŐSSÉGGKIZÁRÓ NYILATKOZAT

Az állásfoglalás 3.4. pontjában bemutatott szoftverek, eszközök és technológiák ismertetése nem teljes körű, és nem minősül termékajánlásnak. A bemutatás a 2026. szeptember 30-i állapotot tükrözi a gyártók nyilvános tájékoztatása és a tanúsító szervezetek adatbázisai alapján. A piacon folyamatosan jelennek meg új megoldások, a meglévők funkciói, elnevezése, tanúsítványai és gyártói háttere pedig változhat, ezért beszerzés előtt ezeket minden esetben ellenőrizni kell.

6. FELHASZNÁLT FORRÁSOK

- [Az Európai Parlament és a Tanács \(EU\) 2022/2555 irányelve \(NIS 2 irányelv\)](#)
- [A Bizottság \(EU\) 2024/2690 végrehajtási rendelete \(2024. október 17.\), melléklet 12.3. pont \(az eltávolítható adathordozókra vonatkozó szabályzat\)](#)
- [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](#)
- [2012. évi I. törvény a munka törvénykönyvéről](#)
- [NBSZ Nemzeti Kiberbiztonsági Intézet, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, 11. Adathordozók védelme \(V.1.2, 2026\)](#)
- [ENISA, Technical implementation guidance on cybersecurity risk management measures \(1.0 verzió, 2025. június\)](#)
- [Európai Adatvédelmi Testület, 01/2021. számú iránymutatás az adatvédelmi incidensek bejelentésével kapcsolatos példákról \(2.0 verzió\)](#)
- [Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH/2019/2471/6. számú határozat, valamint a munkahelyi adatkezelések alapvető követelményeiről szóló tájékoztató \(2016\)](#)
- [NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations \(MP-6, MP-7, SC-28, SC-41\)](#)
- [NIST Special Publication 800-88 Revision 2, Guidelines for Media Sanitization \(2025\)](#)
- IEEE 2883-2022, IEEE Standard for Sanitizing Storage; ISO/IEC 21964 szabványsorozat (2018), Destruction of data carriers
- BSI IT-Grundschutz-Kompendium, SYS.4.5 Wechseldatenträger (Edition 2023)
- [Tischer, M. et al., Users Really Do Plug in USB Drives They Find, IEEE Symposium on Security and Privacy \(2016\)](#)

- [Microsoft Threat Intelligence, Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity \(2022\)](#)

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

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

[Az MKIK NIS2-Tudástár nyitóoldala és a workshopok programja is nyilvánosan elérhető.](#)

7. KAPCSOLÓDÓ MKIK-ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- [MKIK-19 Saját tulajdonú eszköz munkahelyi használatának \(BYOD\) biztonsági követelményei](#)
- [MKIK-64 Egy PC vagy notebook leselejtezéséhez és értékesítéséhez milyen információbiztonsági intézkedéseket kell végezni?](#)
- [2026/5 A munkáltató által biztosított IT eszközök magánhasználata](#)
- [2026/2 A munkavállaló IT eszközeinek ellenőrzése](#)

1. MELLÉKLET

A külső adathordozókhoz kapcsolódó követelmények a 7/2024. (VI. 24.) MK rendelet 2. melléklete alapján

A táblázat a külső adathordozók 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 külső adathordozók esetén
Szabályozás, tudatosság és felelősség				
11.1.	Szabályzat és eljárásrendek	A, J, M	4.3.	Adathordozó-kezelési szabályzat és eljárásrend a felelős kijelölésével és rendszeres felülvizsgálattal.
13.3.	Viselkedési szabályok	A, J, M	4.3.	A felhasználó a hozzáférés engedélyezése előtt dokumentált nyilatkozatban vállalja a szabályok betartását.
3.2.	Biztonságtudatossági képzés	A, J, M	4.3.	Képzés a külső adathordozók kockázatairól és használatuk szabályairól.
3.5.	Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés	J, M	4.3.	A talált vagy ajándékba kapott eszközzel történő megtevesztés felismerése.
9.27.	A biztonsági események jelentése	A, J, M	4.3.	Az eszköz elvesztésének, ellopásának és a talált eszköznek a bejelentése.
14.5.	Személyek munkaviszonyának megszűnése	A, J, M	4.3.	A kiadott eszközök visszavétele a jogviszony megszűnésekor.

Pont	Követelmény	Osztály	Állásfoglalás pontja	Teljesítés külső adathordozók esetén
Nyilvántartás, hozzáférés és használat				
11.2.	Hozzáférés az adathordozókhoz	A, J, M	4.3.	A jogosultak körének meghatározása, az eszközök személyhez rendelt kiadása.
11.14.	Adathordozók használata	A, J, M	4.2., 4.3.	Az engedélyezett eszköztípusok és rendszerek meghatározása, a döntés technikai érvényesítése, a tulajdonos nélküli eszköz tilalma.
11.15.	Adathordozók használata – Biztonságos törlésnek ellenálló adathordozók használatának tiltása	O	–	A biztonságosan nem törölhető, például flash alapú eszközök korlátozása.
6.36.	Rendszerelem leltár	A, J, M	4.3.	A kiadott eszközök szerepeltetése a leltárban sorozatszámokkal és birtokossal.
6.39.	Rendszerelem leltár – Jogosulatlan elemek automatikus észlelése	M	4.4.	A nem engedélyezett eszköz csatlakoztatásának automatikus észlelése.
12.42.	Be- és kiszállítás	A, J, M	4.3.	A telephelyről kivitt és oda behozott eszközök engedélyezése és nyilvántartása.
Külső rendszerek				
2.115.	Külső elektronikus információs rendszerek használata	A, J, M	–	A külső rendszerek használati feltételeinek meghatározása.
2.116.	Külső rendszerek használata – Engedélyezett használat korlátozásai	J, M	–	A külső rendszer védelmének ellenőrzése a használat előtt.
2.117.	Külső rendszerek használata – Hordozható adattárolók használatának korlátozása	J, M	4.2.	A Szervezet eszközeinek korlátozott használata partner vagy a munkatárs otthoni számítógépén.
2.118.	Külső rendszerek használata – A nem szervezeti tulajdonban lévő rendszerek használatának korlátozása	O	–	Magáneszközök korlátozása.
2.120.	Külső rendszerek használata – Hordozható adattárolók használatának tiltása	O	–	A Szervezet eszközeinek idegen számítógépen való használatának tilalma.
Jelölés, tárolás és szállítás				
11.3.	Adathordozók címkézése	J, M	4.3.	A minősítés és a kezelési korlátozások jelölése az eszközön.
11.4.	Adathordozók tárolása	J, M	4.2., 4.3.	Zárt, ellenőrzött helyen történő tárolás.
11.5.	Adathordozók tárolása – Automatizált korlátozott hozzáférés	O	–	A tárolóhely automatizált, naplózott hozzáférés-korlátozása.
11.6.	Adathordozók szállítás	J, M	4.2., 4.3.	A szállítás védelme, elszámoltathatósága és dokumentálása, például a mentés telephelyen kívüli őrzőhelyre vitelekor.
11.7.	Adathordozók szállítás – Kijelölt felelős	O	–	Szállítási felelős kijelölése.
Törlés				
11.8.	Adathordozók törlése	A, J, M	4.3.	Törlés selejtezés, a Szervezet ellenőrzési körén kívülre kerülés és újrafelhasználás előtt, pendrive-on és SSD-n kriptográfiai törléssel vagy fizikai megsemmisítéssel.
11.9.	Adathordozók törlése – Felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés	M	4.3.	A törlés jóváhagyása és ellenőrzése, törlési jegyzőkönyv vagy tanúsítvány.
11.10.	Adathordozók törlése – Berendezés tesztelése	M	4.3.	A törlőberendezések és -eljárások rendszeres tesztelése.
11.11.	Adathordozók törlése – Roncsolásmentes technikák	M	4.2.	Az új vagy kívülről érkező eszköz törlése az első csatlakoztatás előtt.

Pont	Követelmény	Osztály	Állásfoglalás pontja	Teljesítés külső adathordozók esetén
11.12.	Adathordozók törlése – Kettős jóváhagyás	O	–	Négy szem elve a törlésnél.
11.13.	Adathordozók törlése – Adatok távoli törlése vagy megsemmisítése	O	–	Távoli törlés képessége.
Eszkövezérlés és futtatásvédelem				
6.26.	Legszűkebb funkcionalitás	A, J, M	4.4.	A tiltott és korlátozott portok, eszközök és funkciók meghatározása.
6.27.	Legszűkebb funkcionalitás – Rendszeres felülvizsgálat	J, M	4.4.	A szükségtelen portok azonosítása és kikapcsolása.
6.28.	Legszűkebb funkcionalitás – Program futtatásának megakadályozása	J, M	4.4.	Az automatikus és a szabállyal ellentétes programfuttatás tiltása az adathordozóról.
6.31.	Legszűkebb funkcionalitás – Engedélyezett szoftverek, kivételes engedélyezés	J, M	4.4.	Alkalmazás-engedélyezőlista, az adathordozóról induló, nem engedélyezett program blokkolása.
6.35.	Legszűkebb funkcionalitás – Nem engedélyezett hardverek használatának tilalma	O	4.4.	Eszköz-engedélyezőlista sorozatszám alapján.
17.116.	Portok, illetve ki- és bemeneti eszközök hozzáférése	O	4.4.	A portok fizikai vagy logikai letiltása, kritikus rendszeren portzár.
Kártevővédelem és naplózás				
18.8.	Kártékony kódok elleni védelem	A, J, M	4.2., 4.4.	Kártevő-ellenőrzés csatlakoztatáskor és megnyitáskor, ipari környezetben ellenőrző állomással.
10.6.	Karbantartási eszközök – Adathordozók vizsgálata	J, M	4.3.	A karbantartók diagnosztikai adathordozóinak ellenőrzése használat előtt.
4.2.	Naplózható események	A, J, M	4.4.	A csatlakoztatás, a blokkolt csatlakoztatási kísérlet és a fájlmásolás naplózása.
Kriptográfia				
17.53.	Kriptográfiai védelem	A, J, M	4.4.	A titkosítás alkalmazási területeinek meghatározása, ideértve a külső adathordozókat.
17.49.	Kriptográfiai kulcs előállítása és kezelése	A, J, M	4.4.	A titkosítási kulcsok előállítása, tárolása és visszavonása.
17.50.	Kriptográfiai kulcs előállítása és kezelése – Rendelkezésre állás	M	4.4.	A helyreállítási kulcsok központi megőrzése.
17.81.	Tárolt (at rest) adatok védelme	J, M	4.4.	A külső eszközön tárolt adatok bizalmasságának és sértetlenségének védelme.
17.82.	Tárolt (at rest) adatok védelme – Kriptográfiai védelem	J, M	4.2., 4.4.	Kényszerített titkosítás, írás csak titkosított eszközre.