

Egy PC vagy notebook leselejtezéséhez és értékesítéséhez milyen információbiztonsági intézkedéseket kell végezni?

VFP3 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/63

Kiadja a Magyar Kereskedelmi és Iparkamara. Szerző: Kálmán és Társa Ügyvédi Iroda.
Közzétéve: 2026. szeptember 26. [Az állásfoglalás](#) elérhető a [NIS2-Tudástárban](#), a témához kapcsolódó díjmentes workshopok a [Workshopok oldalon](#) találhatók.

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.26	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A NIS2-kötelezett szervezetek PC-inek és notebookjainak selejtezésére és értékesítésére a 7/2024. (VI. 24.) MK rendelet nem tartalmaz „sejtezési eljárás” című, önálló követelményt, az eszközök kivezetésére mégis több, minden biztonsági osztályban kötelező előírás vonatkozik. A rendelet a rendszerelemek leltárát, az adathordozók törlését a lesejtezés és a szervezet ellenőrzési körén kívülre kerülés előtt, a kiszállítás engedélyezését és nyilvántartását, valamint a selejtezés meghatározott módszerekkel történő végrehajtását írja elő. A négy követelmény együtt zárt folyamatot alkot, amelynek a végén a szervezet igazolni tudja, melyik eszköz mikor és milyen adattartalommal hagyta el a szervezetet.

Az információbiztonsági feladat nem merül ki a merevlemez törlésében. A törlés előtt fel kell mérni az eszközben lévő adathordozókat és a kezelt adatok besorolását, meg kell őrizni a még szükséges adatokat, vissza kell vonni az eszközhöz kötött hitelesítőket és fiókokat, és ki kell léptetni az eszközt a központi felügyeleti rendszerekből. A törlés után a leltárt, a licenccnyilvántartást és a számviteli nyilvántartást le kell zárni.

A kivezetés nem csak információbiztonsági kérdés. A számviteli törvény a tárgyi eszköz kivezetését terven felüli értékcsökkenés elszámolásához és bizonylathoz köti, az értékesítésnél az áfa és a személyi jövedelemadó szabályai a szokásos piaci értékhez igazodnak, a hulladékká vált eszköz csak arra jogosult hulladékkezelőnek adható át, és ha az eszköz személyes adatot tartalmazott, a törlés elmaradása adatvédelmi incidens. Kis- és középvállalkozásoknak egy egyoldalas kivezetési ellenőrzőlistát javasunk, amely a rendszerelem-leltárt, a törlési jegyzőkönyvet és a számviteli bizonylatot összeköti.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) az elavult vagy feleslegessé vált asztali számítógépeit és notebookjait rendszeresen kivezeti a használatból. Az eszközök egy részét megsemmisíti vagy hulladékként adja át, más részét használaton értékesíti, gyakran a saját munkavállalóinak vagy egy erre szakosodott felvásárlónak. A vizsgálandó kérdés az, hogy a 7/2024. (VI. 24.) MK rendelet milyen eljárást ír elő erre az esetre, milyen további, a kiberbiztonsági szabályozáson kívüli követelményekre kell figyelni, és mely szabványok segítik a rendelet tömör követelményeinek értelmezését.

Az állásfoglalás a végfelhasználói eszközökre vonatkozik, a szerverekre az elvek azonosak, az eltérő kockázatokat azonban külön kell értékelni. A biztonságos törlés és a fizikai megsemmisítés módszerei, a törlés ellenőrzése és a törlési tanúsítvány tartalma nem tárgya ennek az állásfoglalásnak, ezekről az MKIK [2026/14. számú, Biztonságos törlési megoldások című iránymutatása](#) ad eligazítást. A minősített adatot kezelő rendszerek nem tartoznak a

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv)

Kiberbiztonsági tv. hatálya alá,² az ilyen eszközök kivezetésére a minősített adat védelméről szóló jogszabályok irányadók.

3. GYAKORLATI JAVASLATOK

3.1 A PC-k és notebookok javasolt kivezetési eljárása

A PC-k és notebookok kivezetését célszerű egységes, minden eszköznél azonos módon lefolytatott eljárásként szabályozni, amely a következő lépésekből áll.

- a) Döntés és jóváhagyás. A kivezetést az eszközért felelős vezető kezdeményezi, az informatikai vezető vagy az elektronikus információs rendszer biztonságáért felelős személy jóváhagyja. A döntés rögzíti az eszköz azonosítóját, a kivezetés okát és a tervezett sorsát.
- b) Felmérés. A Szervezet a rendszerelem-leltár és a fizikai átvizsgálás alapján megállapítja, hogy az eszközben milyen adathordozók vannak, milyen biztonsági osztályú rendszerhez tartozott, és milyen besorolású adatot kezelt.
- c) Adatok megőrzése. A helyben tárolt, még szükséges adatokat a Szervezet a megőrzési szabályai szerint átmozgatja a központi tárhelyre vagy archiválja. A törlés után ez a lépés már nem pótolható.
- d) Logikai leválasztás. A Szervezet visszavonja az eszközhöz kötött hitelesítőket és tanúsítványokat, letiltja az eszköz fiókját a címtárban, kilépteti az eszközt a mobileszköz-felügyeleti, végpontvédelmi és távoli telepítési rendszerekből, feloldja a gyártói aktiválási zárat, és visszaveszi a szoftverlicencket.
- e) Biztonságos törlés vagy megsemmisítés. A Szervezet az adathordozókat az adat besorolásához igazodó módszerrel törli vagy megsemmisíti, az eredményt ellenőrzi és jegyzőkönyvezi. Titkosított eszköznél a helyreállítási kulcs törlése önmagában nem elegendő.
- f) Fizikai előkészítés. A Szervezet eltávolítja a szervezetre, a rendszerre, a biztonsági osztályra vagy a felhasználóra utaló címkeket, és törli a BIOS- vagy firmware-jelszót.
- g) Kiszállítás. Az eszköz kiszállítását a Szervezet által kijelölt személy engedélyezi, az átadás-átvételt a Szervezet dokumentálja, a szállítás alatt az eszköz elszámoltathatóságát biztosítja.
- h) Nyilvántartások lezárása. A Szervezet a rendszerelem-leltárban rögzíti a kivezetést, a számviteli nyilvántartásban bizonylatolja a selejtezést vagy az értékesítést, és frissíti a licenc- és a [hitelesítőeszköz-nyilvántartást](#). A kivezetési jegyzőkönyv eszközönként tartalmazza az azonosítókat, a biztonsági osztályt, az adathordozókat, a jóváhagyót, a törlés módszerét, időpontját és végrehajtóját, az átvevőt és a számviteli bizonylat számát.
- i) Külső szolgáltató. Ha a törlést, a megsemmisítést vagy az értékesítést külső szolgáltató végzi, a Szervezet szerződésben rögzíti a kiberbiztonsági és adatvédelmi követelményeket, és eszközönként törlési vagy megsemmisítési tanúsítványt kér.

² 2024. évi LXIX. tv. 3. § (1) bekezdés a) pont

- j) Ellenőrzés. A Szervezet legalább évente ellenőrzi, hogy a kivezetett eszközök a leltárból, a címtárból és a felügyeleti rendszerekből valóban kikerültek-e, és minden kivezetett eszközhöz tartozik-e törlési bizonyíték.

3.2 Jó gyakorlatok és tipikus hibák KKV-k számára

A leggyakoribb hiba nem a törlés elmaradása, hanem a „fiókban maradt” eszköz. A kilépő munkatárs notebookja hónapokig áll egy szekrényben, nem szerepel sem az aktív, sem a kivezetett eszközök között, de továbbra is tartalmazza a Szervezet adatait. A rendszerelemleltárban ezért célszerű a „kivezetés alatt” státuszt bevezetni, és az ilyen eszközöket zárt helyen tárolni a törlésig.

A munkavállalónak történő értékesítés népszerű, de kockázatos, mert a munkavállaló hajlamos „megtartani” a saját gépét a rajta lévő adatokkal együtt. A Szervezet álláspontunk szerint akkor jár el helyesen, ha a törlést az értékesítés előtt maga végzi el, az eszközt tiszta operációs rendszerrel vagy üresen adja át, és a munkavállalóval írásban rögzíti, hogy az eszköz a Szervezet adatait nem tartalmazza. A „vidd haza, majd letöröld” gyakorlat a 11.8. pont sérelmét jelenti, mert az eszköz a törlés előtt kerül a Szervezet ellenőrzési körén kívülre. Az eszközt a gyártói aktiválási zár és az automatikus telepítési szolgáltatás alól is ki kell léptetni, különben a vevő nem tudja használni, a Szervezet felhős környezetéhez pedig továbbra is egy idegen kézben lévő eszköz tartozik.

A külső felvásárló igénybevétele kényelmes, de csak a megfelelő törlési eljárás vagy az adathordozó eltávolítása után szabad átadni az eszközt.

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.³ A válasz lényege a többi szervezettípusra is irányadó.

A PC és a notebook az elektronikus információs rendszer eleme, mert a törvény minden olyan eszközt ide sorol, amely program alapján digitális adatok automatizált kezelését végzi.⁴ A védelmet a törvény a teljes életciklusra írja elő, amely a megszüntetést is magába foglalja.

*26. életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
[2024. évi LXIX. törvény 4. § 26. pont]*

A teljes életciklusban zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet kell biztosítani,⁵ és a védelem kiterjed az adatok kezelésére használt eszközökre, ideértve a hardvert és az adathordozókat is.⁶ A kivezetés tehát az életciklusba tartozó lépés, amelyre ugyanaz a

³ 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

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

⁵ 2024. évi LXIX. tv. 5. § (1) bekezdés

⁶ 2024. évi LXIX. tv. 5. § (2) bekezdés a) pont

védelmi kötelezettség vonatkozik, mint az üzemeltetésre. A rendelet [a rendszer élesüzemből való kivonására vonatkozó tervet](#) is említi.⁷ A kérdés a Szervezet vezetőjének azon törvényi feladataihoz kapcsolódik, hogy nyilvántartásba veszi a rendelkezésében lévő elektronikus információs rendszereket, meghatározza a kockázatokkal arányos védelmi intézkedéseket, és biztosítja azok teljesülését.⁸ A részletes követelményeket a 7/2024. (VI. 24.) MK rendelet 2. mellékletének 6., 10., 11., 12. és 19. követelménycsoportja tartalmazza, ezeket a melléklet táblázata foglalja össze.

4.2 Mit ír elő a 7/2024. (VI. 24.) MK rendelet?

4.2.1 Az adathordozók törlése a kivezetés előtt

A központi követelmény az adathordozók védelme követelménycsoportban található, és minden biztonsági osztályban kötelező.

11.8. A szervezet:

11.8.1. A meghatározott, biztonságos törlési technikákkal és eljárásokkal törli az EIR meghatározott adathordozóit a leselejtezés, a szervezet ellenőrzési körén kívülre kerülés, vagy az újra felhasználásra való kibocsátás előtt.

11.8.2. A törlési mechanizmusokat az információ biztonsági besorolásával és sértetlenségi követelményével arányosan választja ki és alkalmazza. [7/2024. (VI. 24.) MK rendelet 2. melléklet 11.8. pont] (A, J, M)

A követelmény három élethelyzetet nevesít. A leselejtezés a megsemmisítés vagy a hulladékként történő átadás, a szervezet ellenőrzési körén kívülre kerülés az értékesítés, az adományozás, a lízingelt eszköz visszaadása és a garanciális csere, az újra felhasználásra való kibocsátás pedig az eszköz másik munkatársnak történő átadása. A rendelet tehát a belső újrakiosztásnál is törlést vár el, ami a gyakorlatban gyakran elmarad.

A 11.8.2. pont a törlési módszert az információ besorolásához köti. A Szervezetnek tudnia kell, hogy az eszköz milyen osztályú rendszerhez tartozott és milyen besorolású adatot kezelt, mert ettől függ, hogy elegendő-e a szoftveres felülírás, vagy szükséges a kriptográfiai törlés vagy a fizikai megsemmisítés. A módszerekről az MKIK [2026/14. számú iránymutatása](#) szól. A „meghatározott” törlési technikákat és adathordozókat a Szervezetnek magának kell szabályzatban vagy eljárásrendben rögzítenie,⁹ az adathordozók védelmére vonatkozó szabályzat kiadása minden osztályban kötelező.¹⁰

Jelentős és magas osztályban a rendelet a törlésig tartó időszakra is előír védelmet.

11.4. A szervezet:

⁷ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.7.4. pont

⁸ 2024. évi LXIX. tv. 6. § (3) bekezdés 1. pont a) alpont, 6. pont és 8. pont

⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 20.5. pont

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.1. pont (A, J, M)

11.4.1. Fizikailag ellenőrzi és biztonságosan tárolja mind a digitális, mind az analóg adathordozókat az arra engedélyezett vagy kijelölt helyen.

11.4.2. Védi az EIR adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy a rajtuk tárolt adatot biztonságosan nem törlik. [7/2024. (VI. 24.) MK rendelet 2. melléklet 11.4. pont] (J, M)

A kivezetésre váró eszköz tehát nem tárolható nyitott raktárban, és mivel az adathordozókhoz való hozzáférés korlátozása minden osztályban kötelező,¹¹ hozzá is csak a kijelölt személyek férhetnek. Magas osztályban a rendelet a törlési tevékenységek felülvizsgálatát, jóváhagyását, nyomon követését, dokumentálását és ellenőrzését, valamint a törlőeszközök és eljárások rendszeres tesztelését is megköveteli.¹² Álláspontunk szerint a dokumentálás alacsonyabb osztályban is szükséges, mert a 11.8. pont teljesítését az auditon csak dokumentummal lehet igazolni. A távoli törlés képessége opcionális.¹³

4.2.2 A rendszerelem-leltár és a változáskezelés

A kivezetés a leltár oldaláról is kötelezettséget keletkeztet. A rendszerelem-leltár minden osztályban kötelező.

6.36. A szervezet:

6.36.1. Leltárt készít az EIR elemeiről.

6.36.1.1. A leltár pontosan tükrözi az EIR-t.

6.36.1.2. A leltár tartalmazza a rendszeren belül található összes elemet.

[...]

6.36.2. Meghatározott gyakorisággal felülvizsgálja és frissíti a rendszerelemek leltárát. [7/2024. (VI. 24.) MK rendelet 2. melléklet 6.36. pont] (A, J, M)

A leltár csak akkor tükrözi pontosan a rendszert, ha a kivezetett eszköz kikerül belőle, vagy kivezetett státusszal szerepel benne. Jelentős és magas osztályban a frissítés nem várhat a következő felülvizsgálatig, a leltárt minden rendszerelem telepítése, eltávolítása és frissítése alkalmával frissíteni kell.¹⁴ Magas osztályban a leltárból a felelős személyeknek név, munkakör és szerepkör alapján azonosíthatónak kell lenniük,¹⁵ vagyis ki kell derülnie, ki döntött a kivezetésről, és ki végezte a törlést. A rendszerelem eltávolítása egyben konfigurációváltozás is, jelentős és magas osztályban a Szervezet dokumentálja a változtatásokra vonatkozó döntéseket, és a dokumentumokat visszakereshetően megőrzi.¹⁶

4.2.3 Az eszköz kiszállítása és szállítása

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.2. pont (A, J, M)

¹² 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.9. és 11.10. pont (M)

¹³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.13. pont (O)

¹⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.37. pont (J, M)

¹⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.40. pont (M)

¹⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.7. pont (J, M)

A rendelet a fizikai védelem körében külön követelményt fogalmaz meg a rendszerelemek létesítményből történő kiszállítására.

12.42. A szervezet

12.42.1. Engedélyezi és felügyeli a szervezet által meghatározott típusú rendszerelemek létesítménybe történő beszállítását és kiszállítását a létesítményből; és

12.42.2. nyilvántartást vezet ezekről. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.42. pont] (A, J, M)

A kivezetett PC vagy notebook kiszállítása tehát engedélyhez kötött és nyilvántartandó esemény, a végfelhasználói eszközöket álláspontunk szerint minden esetben be kell vonni az engedélyezésbe, mert adathordozót tartalmaznak. Jelentős és magas osztályban a Szervezet a szállítás alatt is védi az adathordozókat, biztosítja az elszámoltathatóságukat és dokumentálja a szállítást.¹⁷ Ha a törlést a külső szolgáltató a saját telephelyén végzi, a plombált konténer és a sorozatszám átadás-átvétel a 11.6. pont teljesítésének eszköze.

4.2.4 A selejtezés mint ellátási lánc kérdés

A rendelet az ellátási lánc kockázatmenedzsment körében kifejezetten nevesíti a selejtezést.

19.27. A szervezet meghatározott technikákkal és módszerekkel selejtezi a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket. [7/2024. (VI. 24.) MK rendelet 2. melléklet 19.27. pont] (A, J, M)

A Szervezetnek tehát előre rögzítenie kell, hogy melyik eszköztípust milyen módon selejtezi. Az ellátási lánc kockázatmenedzsment stratégiájának és szabályzatának minden osztályban ki kell terjednie a selejtezésre,¹⁸ ezért a felvásárló, a megsemmisítést végző szolgáltató és az e-hulladék átvéője beszállítónak minősül, akit a Szervezet az ellátási lánc szabályai szerint értékel. A Kiberbiztonsági tv. a közreműködők igénybevétele esetén [a kiberbiztonsági követelmények szerződéses érvényesítését](#) írja elő,¹⁹ a szerződésnek ezért tartalmaznia kell a törlési módszert, a tanúsítványt, a szállítás alatti védelmet és az ellenőrzés jogát.

4.2.5 A karbantartásra elszállított és a kilépő munkatárstól visszavett eszköz

A garanciális javításra vagy cserére elszállított notebook is adatot tartalmaz, és a rendelet erre az esetre minden osztályban külön követelményt ad. A Szervezet által meghatározott személyek egyedileg jóváhagyják a rendszerelemek elszállítását külső karbantartás, javítás vagy csere céljából, a Szervezet az elszállítás előtt biztonságosan törli a meghatározott besorolású információkat az adathordozókról, és az elszállítást a karbantartási nyilvántartásban rögzíti.²⁰ A garanciális csere gyakorlati csapdája az, hogy a meghibásodott eszközt a gyártó elviszi, és a hibás SSD nem kerül vissza. A Szervezetnek ilyenkor vagy törölnie kell az adathordozót az elszállítás előtt, vagy a szerződésben ki kell kötnie, hogy a hibás adathordozó a Szervezetnél marad.

¹⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.6. pont (J, M)

¹⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.21. pont és 19.2. pont (A, J, M)

¹⁹ 2024. évi LXIX. tv. 6. § (5) bekezdés d) pont

²⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.2.3., 10.2.4. és 10.2.6. pont (A, J, M)

A notebookok jelentős része a munkaviszony megszűnésekor kerül vissza a Szervezethez, amely minden osztályban köteles visszavenni az összes biztonsági szempontból releváns, a szervezeti EIR-hez kapcsolódó biztonsági eszközt.²¹ Ha a visszavett notebookot másik munkatárs kapja, a 11.8.1. pont szerinti törlés kötelező, ha a Szervezet kivezeti, a fenti eljárás indul.

4.2.6 A titkosítás és a szoftverlicenck

Jelentős és magas osztályban a rendelet a mobil eszközökön teljes eszköztitkosítást vagy tárolóalapú titkosítást ír elő.²² A mobil eszköz fogalmát a rendelet nem határozza meg, a notebook ebbe a körbe tartozása a Szervezet saját meghatározásától függ. A tárolt adatok védelmére vonatkozó 17.82. pont²³ azonban a rendszerelemek és adathordozók kriptográfiai védelmét jelentős és magas osztályban általánosan is előírja, és a notebookok teljes lemeztitkosítása ma alapvető elvárás. A titkosítás csökkenti a kockázatot a törlésig, és lehetővé teszi a kriptográfiai törlést, amelyet a NIST SP 800-88 útmutató az arra alkalmas eszközöknél elfogadott módszerként ismer el, feltéve, hogy a helyreállítási kulcsot a Szervezet a központi tárolóból is törli. A titkosítás tehát a törlési módszer megválasztásánál számít, de a 11.8. pont szerinti törlést nem váltja ki.

A Szervezet minden osztályban kizárólag a szerződéses elvárásoknak és a szerzői jogi előírásoknak megfelelő szoftvereket használhat, és nyomon követi a mennyiségi licenc alá eső szoftverek használatát.²⁴ Az értékesített eszközön nem maradhat olyan szoftver, amelynek licence a Szervezethez és nem az eszközhöz kötött. Az eszközzel szállított operációs rendszer gyártói licence jellemzően átruházható, a mennyiségi licenc és a felhasználóhoz rendelt előfizetés nem.

4.3 Mire kell még figyelni? Számviteli, adózási, adatvédelmi és egyéb szempontok

4.3.1 Számviteli követelmények

A PC és a notebook tárgyi eszköz, amelynek kivezetését a számvitelről szóló 2000. évi C. törvény (Sztv.) szabályozza. Ha az eszköz feleslegessé vált vagy rendeltetésének megfelelően nem használható, terven felüli értékcsökkenést kell elszámolni, és az eszközt a tárgyi eszközök közül ki kell vezetni.²⁵ A kivezetés alapja a selejtezési jegyzőkönyv, amely számviteli bizonylat, és amelyet legalább nyolc évig meg kell őrizni.²⁶ A számviteli politika részeként elkészítendő leltárkészítési és leltározási szabályzat²⁷ jellemzően a selejtezés rendjét is tartalmazza, ezt célszerű összehangolni az információbiztonsági kivezetési eljárással.

A számviteli nyilvántartás az eszköz értékét és jogi sorsát követi, a rendszerelem-leltár a rendszerhez tartozását és biztonsági állapotát. Javasoljuk, hogy a kettő ugyanazt az eszközazonosítót használja, és a selejtezési jegyzőkönyv a törlési jegyzőkönyv számára is hivatkozzon, így az eszközmozgás a kiberbiztonsági auditon is bizonyítékként szolgál.

²¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.5.4. pont (A, J, M)

²² 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.114. pont (J, M)

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 17.82. pont (J, M)

²⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.47. pont (A, J, M)

²⁵ 2000. évi C. törvény 53. § (1) bekezdés b) pont és (2) bekezdés

²⁶ 2000. évi C. törvény 169. § (2) bekezdés

²⁷ 2000. évi C. törvény 14. § (5) bekezdés a) pont

4.3.2 Adózási és polgári jogi szempontok az értékesítésnél

A használt eszköz értékesítése adóköteles. Ha a vevő a Szervezet munkavállalója, a felek az általános forgalmi adóról szóló 2007. évi CXXVII. törvény (Áfa tv.) szerint nem független felek,²⁸ és ha az ellenérték aránytalanul alacsony a szokásos piaci árhoz képest, az adó alapja a szokásos piaci ár.²⁹ A szokásos piaci érték és a ténylegesen fizetett ár különbözete a munkavállalónál a személyi jövedelemadóról szóló 1995. évi CXVII. törvény (Szja tv.) szerint jövedelemnek minősülhet.

A munkavállalónak történő értékesítés polgári jogi szempontból jellemzően fogyasztó és vállalkozás közötti szerződés. A Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) szerint a fogyasztó kellékszavatossági igénye két év alatt évül el, használt dolog esetén a felek rövidebb, de egy évnél nem rövidebb határidőben állapodhatnak meg.³⁰ Az adásvételi szerződésben javasoljuk rögzíteni az eszköz azonosítóit és állapotát, a szavatossági határidőt, valamint azt, hogy az adathordozót a Szervezet törölte, és a vevő az adatok helyreállítására nem tesz kísérletet.

4.3.3 Adatvédelmi és hulladékgazdálkodási szempontok

A végfelhasználói eszközök szinte mindig tartalmaznak személyes adatot. Az általános adatvédelmi rendelet (GDPR) az adatkezelőtől a személyes adatok megfelelő biztonságát, ideértve a jogosulatlan hozzáférés elleni védelmet, és a kockázattal arányos technikai és szervezési intézkedéseket várja el.³¹ A törlés nélkül elidegenített eszköz jogosulatlan hozzáférést tesz lehetővé a személyes adatokhoz, ami adatvédelmi incidens, és a felügyeleti hatóság felé bejelentési kötelezettséget keletkeztethet.³² A törlést vagy megsemmisítést végző külső szolgáltató adatfeldolgozónak minősül, akivel a GDPR 28. cikke szerinti szerződést kell kötni.

A hulladékká vált PC és notebook elektronikai hulladék, amelyre a hulladékról szóló 2012. évi CLXXXV. törvény és a 197/2014. (VIII. 1.) Korm. rendelet vonatkozik. A hulladékbirtokos a hulladékot csak az arra jogosult hulladékkezelőnek adhatja át, az átadást dokumentálni kell, a gyártót és a forgalmazót pedig visszavételi kötelezettség terheli. A hulladékként átadott eszköz is a Szervezet ellenőrzési körén kívülre kerül, ezért a 11.8. pont szerinti törlés vagy az adathordozó megsemmisítése ebben az esetben is kötelező, a hulladékkezelő átvételi bizonylata pedig a kiszállítás nyilvántartásának része.

4.4 Szabványok és útmutatók a selejtezéshez (NIST SP 800-88, ISO/IEC 27001)

A rendelet 2. mellékletének védelmi intézkedései a NIST SP 800-53 kontrollkatalógus ötödik kiadására épülnek,³³ ezért a kivezetéshez kapcsolódó követelmények forrása azonosítható. A megfeleltetést a melléklet táblázata tartalmazza, a legfontosabb párok a 11.8. pont és az MP-6

²⁸ 2007. évi CXXVII. törvény 259. § 13. pont

²⁹ 2007. évi CXXVII. törvény 67. § (1) bekezdés

³⁰ 2013. évi V. törvény 6:163. § (2) bekezdés

³¹ GDPR 5. cikk (1) bekezdés f) pont és 32. cikk (1) bekezdés

³² GDPR 4. cikk 12. pont és 33. cikk (1) bekezdés

³³ Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Előkészületek, 1.0 verzió (2024. augusztus). Elérhető az NKI honlapján.

(Media Sanitization), a 6.36. pont és a CM-8 (System Component Inventory), a 12.42. pont és a PE-16 (Delivery and Removal), valamint a 19.27. pont és az SR-12 (Component Disposal).

A törlés részletes módszertanát a NIST SP 800-88 Guidelines for Media Sanitization útmutató adja, amelynek második kiadását a NIST 2025 szeptemberében tette közzé. Az új kiadás a szervezeti törlési program kialakítására helyezi a hangsúlyt, a technikai módszereknél az IEEE 2883-2022 szabványra hivatkozik, és önálló fejezetet szentel a kriptográfiai törlésnek.

Az ISO/IEC 27001 szabvány 2022-es kiadásának A. mellékletében a kivezetést a 7.14. (Secure disposal or re-use of equipment) intézkedés fedi le, amelyhez az ISO/IEC 27002 szabvány útmutatása kapcsolódik. Az útmutató a kivezetés előtt az adathordozó meglétének ellenőrzését, a bizalmas tartalom helyreállíthatatlan törlését vagy az adathordozó megsemmisítését, a sérült eszközök kockázatértékelését, valamint a szervezetre, a besorolásra vagy a rendszerre utaló címkék eltávolítását várja el. Ehhez kapcsolódik az 5.9., az 5.11., a 7.10. és a 8.10. intézkedés, valamint az ISO/IEC 27040 szabvány. A külső szolgáltató kiválasztásához az ITAD szolgáltatók tanúsítási rendszerei (ADISA, R2v3, e-Stewards, NAID AAA) adnak támpontot. A NIS 2 irányelv a kockázatkezelési intézkedések között az eszkozgazdalkodást is nevesíti,³⁴ amelynek a kivezetés az utolsó lépése.

5. FELHASZNÁLT FORRÁSOK

- (EU) 2022/2555 irányelv (NIS 2 irányelv), (EU) 2016/679 rendelet (GDPR)
- 2024. évi LXIX. törvény (Kiberbiztonsági tv.), 7/2024. (VI. 24.) MK rendelet
- 2000. évi C. törvény (Sztv.), 2007. évi CXXVII. törvény (Áfa tv.), 1995. évi CXVII. törvény (Szja tv.), 2013. évi V. törvény (Ptk.), 2012. évi CLXXXV. törvény (Ht.), 197/2014. (VIII. 1.) Korm. rendelet
- [MKIK NIS2 iránymutatás 2026/14, Biztonságos törlési megoldások \(2026. szeptember 29.\)](#)
- NIST SP 800-53 Rev. 5, NIST SP 800-88 Rev. 2 (2025), IEEE 2883-2022, ISO/IEC 27001 (2022), ISO/IEC 27002 (2022), ISO/IEC 27040 (2024)

6. KAPCSOLÓDÓ MKIK-ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- MKIK-63, [Külső adathordozók NIS2-kompatibilis használata](#)
- MKIK-41, [Hogyan kell nyilvántartani a hitelesítő eszközöket?](#)
- MKIK-33, [EIR-ek változásai auditok között, új rendszer bevezetése, rendszerkivezetés](#)
- [2026/10 - A KÖZREMŰKÖDŐVEL KÖTÖTT SZERZŐDÉS TARTALMA](#)
- [2026/14 Biztonságos törlési megoldások](#)

³⁴ NIS 2 irányelv 21. cikk (2) bekezdés i) pont

MELLÉKLET. A KIVEZETÉSHEZ KAPCSOLÓDÓ VÉDELMI INTÉZKEDÉSEK A 7/2024. (VI. 24.) MK RENDELET SZERINT

A táblázat a PC-k és notebookok kivezetéséhez kapcsolódó, az állásfoglalásban hivatkozott védelmi intézkedéseket foglalja össze a 7/2024. (VI. 24.) MK rendelet 2. mellékletének sorrendjében. A biztonsági osztály oszlop a rendelet C, D és E oszlopát követi (A alap, J jelentős, M magas, O egyik osztályban sem kötelező, kiegészítő intézkedés). A NIST oszlop a NIST SP 800-53 ötödik kiadásának megfelelő kontrollját, a lépés oszlop a 3.1. pont szerinti kivezetési eljárás kapcsolódó lépését jelöli. Az elvárás oszlop a követelmény kivezetési szempontból lényeges tartalmát saját megfogalmazásban adja vissza, a szó szerinti szöveg a rendeletben olvasható.

Pont	Követelménycsoport	Elvárás a kivezetés során	Osztály	NIST SP 800-53	Lépés
1.21.	Ellátási lánc kockázatmenedzsment stratégiája	A szervezet egészére kiterjedő stratégia kiterjed a rendszerelemek selejtezésére is.	A, J, M	PM-30	i)
2.114.	Mobil eszközök hozzáférés-ellenőrzése, teljes eszköz vagy konténer-alapú titkosítás	Teljes eszköz- vagy tárolóalapú titkosítás a meghatározott mobil eszközökön, a kriptográfiai törlés alapja.	J, M	AC-19(5)	e)
6.7.	A konfigurációváltozások felügyelete (változáskezelés)	A rendszerelem eltávolítása jóváhagyott, dokumentált és visszakereshetően megőrzött változás.	J, M	CM-3	a), h)
6.36.	Rendszerelem leltár	A leltár pontosan tükrözi a rendszert, a kivezetett eszköz státusza követhető, a leltárt meghatározott gyakorisággal felülvizsgálják.	A, J, M	CM-8	b), h)
6.37.	Rendszerelem leltár, frissítések a telepítés és eltávolítás során	A leltárt minden rendszerelem eltávolításakor frissíteni kell.	J, M	CM-8(1)	h)
6.40.	Rendszerelem leltár, elszámoltathatósággal kapcsolatos információk	A leltárból a rendszerelemért felelős és számonkérhető személy név, munkakör és szerepkör alapján azonosítható.	M	CM-8(4)	a), h)
6.47.	A szoftverhasználat korlátozásai	Az átadott eszközön nem maradhat a szervezethez kötött licenccel szoftver, a mennyiségi licencek használatát nyomon kell követni.	A, J, M	CM-10	d)
10.2.	Szabályozott karbantartás	Külső javításra vagy cserére történő elszállítás előtt egyedi jóváhagyás és biztonságos törlés, az elszállítás rögzítése a karbantartási nyilvántartásban.	A, J, M	MA-2	e), g)
11.1.	Adathordozók védelme, szabályzat és eljárásrendek	A kivezetési eljárás az adathordozók védelmére vonatkozó szabályzat és eljárásrend része, kijelölt felelőssel.	A, J, M	MP-1	a)
11.2.	Hozzáférés az adathordozókhoz	A kivezetés alatt álló eszköz adathordozójához csak a meghatározott személyek vagy szerepkörök férhetnek hozzá.	A, J, M	MP-2	b)
11.4.	Adathordozók tárolása	A kivezetésre váró eszköz kijelölt, ellenőrzött helyen tárolandó a megsemmisítésig vagy a biztonságos törlésig.	J, M	MP-4	b)
11.6.	Adathordozók szállítása	A törlés előtti szállítás védett, az adathordozók elszámoltathatók, a szállítás dokumentált és jogosult személyekre korlátozott.	J, M	MP-5	g)

Pont	Követelménycsoport	Elvárás a kivezetés során	Osztály	NIST SP 800-53	Lépés
11.8.	Adathordozók törlése	Biztonságos törlés a leselejtezés, az ellenőrzési körön kívülre kerülés és az újrafelhasználás előtt, az információ besorolásához igazodó módszerrel.	A, J, M	MP-6	e)
11.9.	Adathordozók törlése, felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés	A törlési és megsemmisítési tevékenységek jóváhagyása, nyomon követése, dokumentálása és ellenőrzése.	M	MP-6(1)	e), j)
11.10.	Adathordozók törlése, berendezés tesztelése	A törléshez használt eszközök és eljárások meghatározott időközönkénti tesztelése.	M	MP-6(2)	j)
11.13.	Adathordozók törlése, adatok távoli törlése vagy megsemmisítése	Távoli törlés vagy felülírás képessége a meghatározott rendszerelemeken, meghatározott feltételek mellett.	O	MP-6(8)	e)
11.14.	Adathordozók használata	Azonosítható tulajdonos nélküli hordozható adattároló nem használható, a kivezetésnél az eltávolítható adathordozókat is fel kell mérni.	A, J, M	MP-7	b)
12.42.	Be- és kiszállítás	A meghatározott típusú rendszerelemek kiszállítása engedélyhez kötött, felügyelt és nyilvántartott.	A, J, M	PE-16	g)
14.5.	Személyek munkaviszonyának megszűnése	A kilépő munkatárs biztonsági szempontból releváns eszközeinek, köztük a notebooknak a visszavétele.	A, J, M	PS-4	b)
17.82.	Tárolt (at rest) adatok védelme, kriptográfiai védelem	Kriptográfiai védelem a meghatározott rendszerelemeken és adathordozókon tárolt adatokra.	J, M	SC-28(1)	e)
19.2.	Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	A szabályzat kiterjed a kivezetés és a selejtezés során felmerülő ellátási lánc kockázatokra.	A, J, M	SR-2	i)
19.27.	Rendszerelem selejtezése, megsemmisítése	Adatok, dokumentációk, eszközök és rendszerelemek selejtezése meghatározott technikákkal és módszerekkel.	A, J, M	SR-12	e), i)

A rendelet 1. mellékletének 1.1.7.4. pontja a kockázatmenedzsment keretrendszer részeként minden szervezettől elvárja, hogy a rendszer élesüzemből való kivonására vonatkozó terv tartalmazza a felmerülő kockázatok kezeléséhez tartozó intézkedéseket. A 3. melléklet fenyegetéskatalógusából a kivezetés kockázatelemzéséhez a 17. (eszközök, adathordozók, dokumentumok eltulajdonítása), a 18. (eszközök, adathordozók, dokumentumok elvesztése) és a 20. (védett információ nyilvánosságra kerülése) pont hivatkozható.