

Virtuális magánszerver-szolgáltatás (VPS) NIS2-kompatibilis használata

VFP3 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/61

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 virtuális magánszerver (VPS) NIS2-kötelezett szervezetnél is használható.** A Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet nem tiltja a felhőszolgáltatást, és a törvény 1. § (1) bekezdés d) pontja alá tartozó szervezeteknek adatlokalizációt sem ír elő. A VPS felhőszolgáltatás, a szolgáltató közreműködő, a rajta futó rendszerre pedig a biztonsági osztály követelményei vonatkoznak.
- **A feladat megoszlik, a felelősség nem száll át.** Az adatközpont, a fizikai szerver és a virtualizáció védelme a szolgáltatóé, ezt a Szervezet szerződéssel és tanúsítványokkal igazolja. A vendég operációs rendszertől felfelé minden a Szervezet feladata.
- **A szerződés a legerősebb kontroll.** A rendelet minden osztályban megköveteli a szerződéses megfelelést, a felelőségek dokumentálását és a szolgáltató ellenőrzését. Rendezni kell az órákban mért incidensértesítést, az alvállalkozókat, az adatok helyét, az ellenőrzési jogot és a kilépést.
- **Adatvédelmi szempontból a szolgáltató adatfeldolgozó.** Kell a GDPR 28. cikke szerinti szerződés és a további adatfeldolgozók listája. Európai adatközpont mellett is vizsgálni kell a harmadik országbeli joghatóság kockázatát, amelyet az uniós szolgáltató és a saját kulcsú titkosítás érdemben csökkent.
- **Az adathordozó itt a virtuális lemez, a pillanatkép és a mentés.** Titkosításuk jelentős és magas osztályban kötelező, VPS-nél osztálytól függetlenül saját kulccsal javasolt, a mentést pedig a szolgáltatótól függetlenül is tárolni kell. A szolgáltatás végén a kulcsok megsemmisítése és a törlés szolgáltatói igazolása zárja le az életciklust.
- **A kilépést az első naptól tervezni kell.** A magánszférában erősen ajánlott, a 418/2024. Korm. rendelet hatálya alá tartozó szervezeteknél a kilépési terv kötelező, és az adatosztályozástól függően egyes adatok nyilvános felhőben futó VPS-en nem is kezelhetők.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) a honlapját, az ügyfélportálját és belső alkalmazásait külső szolgáltatótól bérelt virtuális magánszervereken (Virtual Private Server, VPS) kívánja üzemeltetni. A fizikai szervert, a virtualizációt, a tárolót és a hálózatot a szolgáltató adja, a vendég operációs rendszert és az alkalmazásokat a Szervezet kezeli.

A vizsgálandó kérdés az, hogy milyen feltételekkel használható VPS-szolgáltatás NIS2-kötelezett szervezetnél, milyen adminisztratív kontrollok szükségesek, milyen adatvédelmi előírásokat kell figyelembe venni, milyen technológiai kontrollokkal kell védeni az adathordozókat, és milyen szoftveres és technológiai megoldások állnak ehhez rendelkezésre. 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) 2018/1792 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

platform- és szoftverszolgáltatások (PaaS, SaaS) és a kolokáció sajátos kérdései nem tárgyai az állásfoglalásnak.

3. GYAKORLATI JAVASLATOK

3.1 A VPS igénybevételének feltételei

A Szervezet akkor tudja a VPS használatának megfelelőségét az auditon is igazolni, ha a következő feltételek együtt teljesülnek.

- a) Nyilvántartás és besorolás, a rendszer szerepel az elektronikus információs rendszerek (EIR) nyilvántartásában, biztonsági osztályba van sorolva, a rendszerbiztonsági terv megnevezi a szolgáltatónál működő elemeket és az adatok helyét.
- b) Kockázatelemzés, amely kiterjed a szolgáltatóra, a szolgáltatás kiesésére, a joghatósági kitettségre és a megosztott infrastruktúrára.
- c) Felelősségmegosztás, a feladatok követelményenként dokumentáltak, ennek kiindulópontja lehet az 1. melléklet.
- d) Szerződés és garanciák, a szerződés rögzíti a biztonsági követelményeket, az incidensértesítést, az adatok helyét, az ellenőrzési jogot, a kilépést és az adatfeldolgozói kikötéseket, a tanúsítványok pedig az igénybe vett szolgáltatásra is kiterjednek.
- e) Saját kontrollok, a Szervezet a saját rétegeiben teljesíti a biztonsági osztály követelményeit.
- f) Folytonosság és kilépés, független mentés, kipróbált visszaállítás és átköltözési terv.
- g) Vezetői döntés, a vezető a fenti dokumentumok alapján, jegyzőkönyvben dönt a használatbavételről.

3.2 Adminisztratív kontrollok

VPS-nél a megfelelés terhét nagyrészt az adminisztratív kontrollok viselik, mert a szolgáltató rétegébe a Szervezet nem lát bele.

Felelősségi mátrix. Követelménycsoportonként rögzíti, mit teljesít a Szervezet, mit a szolgáltató, és mi közös. A fizikai védelem, a hipervizor, a megosztott erőforrások elkülönítése és a fizikai adathordozók selejtezése jellemzően a szolgáltatóé. Felügyelt (managed) VPS-nél az operációs rendszer üzemeltetése is hozzá kerül, a Szervezet ellenőrzési kötelezettsége viszont nem csökken.

Szerződés. Az általános szerződési feltételek ritkán fedik le a rendelet elvárásait. Ellenőrizni kell, hogy a feltételek, az adatfeldolgozói szerződés és a biztonsági melléklet együtt kitérnek-e a következőkre.

- a biztonsági osztályra és a szolgáltató által teljesítendő védelmi intézkedésekre,
- az incidensek órákban meghatározott bejelentési határidejére,
- az alvállalkozókra, a követelmények továbbhárítására és az adatok helyére (ország, adatközpont),

- a Szervezet, az EIR biztonságaért felelős személy és az auditor tájékoztatási és ellenőrzési jogára, a szolgáltatói hozzáférések naplózására,
- a megszűnéskor az adatok kiadására és a tárolók igazolt törlésére.

Ahol a feltételek nem tárgyalhatók, a hiányt dokumentáltan, saját kontrollal kell ellensúlyozni.

Beszállítói értékelés és szabályzatok. A szolgáltatót szerződéskötés előtt, majd rendszeresen, javaslatunk szerint évente értékelni kell a tanúsítványok hatóköre és érvényessége, a NIS2-státusz, a tulajdonosi háttér és a joghatóság, az adatközpontok helye és a további adatfeldolgozók alapján. Szerencsés, ha az információbiztonsági szabályzat rögzíti a felhőszolgáltatások igénybevételének rendjét, eljárásrend pedig szabályozza a távoli adminisztrációt, a mentést és a közös incidenskezelést.

3.3 Technológiai kontrollok és az adathordozók védelme

VPS-nél a Szervezet adathordozói a virtuális lemezek és kötetek, a pillanatképek (snapshot), a rendszerképek (image), a mentések és az objektumtárolóban tárolt állományok.

Titkosítás saját kulccsal. Az adatköteteket az operációs rendszer szintjén kell titkosítani, a kulcsot a szolgáltatótól elkülönítve kezelni. A szolgáltatói tárolótitkosítás csak kiegészítés, mert ott a kulcs a szolgáltatónál van, és a gyakorlat is eltérő.

Független mentés. A pillanatkép nem mentés, mert ugyanannál a szolgáltatónál tárolódik. A mentést kliensoldali titkosítással, független helyre, módosíthatatlan (WORM) tárolással kell készíteni, a visszaállítást pedig rendszeresen ki kell próbálni.

Kriptográfiai törlés. A kötet életciklusát a kulcsok megsemmisítése, majd a kötet, a pillanatképek és a mentések törlése zárja le, amelyről a szolgáltató igazolását kell kérni.

Hozzáférés és üzemeltetés. A szolgáltatói kezelőfelületen többtényezős hitelesítés kell, a szerverre pedig kulcsalapú SSH-val, root belépés nélkül, VPN-en keresztül érdemes belépni. Emellett tiltó alapú tűzfalszabályok, keményített (hardened) konfiguráció, automatikus frissítés és a szerveren kívüli naplógyűjtés javasolt.

3.4 Szoftveres és technológiai megoldások

A felsorolás a szükséges megoldástípusokat írja le, konkrét termékeket nem nevez meg. A választás a környezettől, a támogatási igényektől és a licencfeltételektől függ. Szolgáltatói példákat a 2. melléklet tartalmaz.

Hozzáférés és hálózat. Távoli adminisztrációra olyan SSH-implementáció javasolt, amely támogatja a FIDO2 hardverkulcshoz kötött kulcsokat és a hibrid poszt-kvantum kulcscserét. Az adminisztrációs hozzáféréshez korszerű, kernelszintű VPN-protokoll, több szerver esetén központilag menedzsel, pont-pont kapcsolatú (mesh) VPN-hálózat jöhet szóba. Ez utóbbi saját üzemeltetésben és szolgáltatásként is elérhető, szolgáltatásként igénybe véve a vezérlő infrastruktúra üzemeltetőjének joghatóságát is értékelni kell. A privilegizált munkamenetek rögzítésére hozzáférés-kezelő (PAM) eszköz alkalmas. Egyes termékek ingyenes kiadása csak meghatározott létszám vagy árbevétel alatti szervezetnek használható, ezért a licencfeltételeket előre ellenőrizni kell. Tűzfalként az operációs rendszer beépített csomagszűrője, a jelszópróbálgatásos támadások ellen pedig a naplók alapján automatikusan tiltó eszköz alkalmazható, amely közösségi fenyegetésinformációval is kiegészíthető.

Titkosítás, kulcsok és mentés. Kötetttitkosításra az operációs rendszer szabványos, beépített lemeztitkosítása szolgál. Újraindítás után a kötet hálózati kulcskiszolgálóhoz kötött automatikus feloldással vagy a rendszerindítás korai szakaszában SSH-n keresztül megadott jelszóval nyitható meg. A titkokat dedikált titokkezelő rendszerben, a konfigurációs állományokban tárolt titkokat állományszintű titkosítással érdemes védeni. A titokkezelő kiválasztásánál a licencfeltételeket és a fejlesztő tulajdonosi hátterét is mérlegelni kell. Mentésre kliensoldalon titkosító, deduplikáló mentőszoftver, virtuális gépek teljes mentésére dedikált mentőkiszolgáló alkalmas. Módosíthatatlan tárolást az objektumtárolók zárolási (object lock) funkciója biztosít, amelyet több uniós objektumtároló támogat.

Keményítés, naplózás és észlelés. Kiindulási alapként nemzetközileg elismert, platformonként kiadott keményítési ajánlások szolgálnak. A megfelelés automatizált konfigurációellenőrző és auditeszközökkel ellenőrizhető, a konfiguráció kódként kezelésére konfigurációkezelő és infrastruktúra-leíró (infrastructure as code) eszközök valók. Naplóelemzésre és behatolásérzékelésre biztonsági eseménykezelő (SIEM) platform, naplógyűjtésre központi naplókezelő, fájlintegritás-figyelésre integritásellenőrző eszköz, sérülékenységvizsgálatra hálózati sérülékenységszkenner, konténerképekhez képellenőrző eszköz használható. Mindegyik kategóriában van nyílt forráskódú és kereskedelmi megoldás. 2026 tavaszán egy széles körben használt, nyílt forráskódú konténerkép-ellenőrző eszköz kiadási csatornáját feltörték, és a CERT-EU szerint ezen keresztül az Európai Bizottság egyik felhőfiókját is kompromittálták.² A biztonsági eszköz is az ellátási lánc része, rögzített verzióval és ellenőrzött aláírással kell használni.

Webes szolgáltatások. Javasolt a webalkalmazás-tűzfal elismert szabálykészlettel, valamint a TLS-tanúsítványok automatikus megújítása (például ACME-protokollal), mert érvényességük 2029-ig 47 napra rövidül.

3.5 A javasolt eljárás

- a) Felmérés, a rendszerek és adatok azonosítása, a biztonsági osztály és az adatvédelmi hatásvizsgálat szükségességének meghatározása.
- b) Kiválasztás, legalább két szolgáltató összevetése a tanúsítás, a helyszín, a joghatóság és a kilépés szerint.
- c) Szerződés, a szerződések kiegészítése és a felelősségi mátrix elkészítése.
- d) Kialakítás, keményítés, titkosítás, hozzáférés-kezelés, naplózás és független mentés.
- e) Használatbavétel, a védelmi intézkedések értékelése és a vezető jegyzőkönyvezett döntése.
- f) Felügyelet, sérülékenységvizsgálat, visszaállítási próba, éves beszállítói felülvizsgálat és kilépési próba.

² A CERT-EU tájékoztatója az Európai Bizottság felhőfiókját érintő, egy nyílt forráskódú konténerkép-ellenőrző eszköz ellátási láncán keresztül elkövetett incidensről (2026. április 2., cert.europa.eu)

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 Az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek eltéréseit a 4.9. pont foglalja össze. A VPS a törvény fogalmai szerint felhőszolgáltatás, mert önkiszolgáló módon, hálózaton keresztül ad hozzáférést igény szerint méretezhető, megosztott virtuális erőforrásokhoz.⁴ Az ilyen szervezetek számára a kiberbiztonsági jogszabályok a felhőszolgáltatást nem tiltják, és földrajzi korlátozást sem írnak elő. A rendelet a feldolgozás helyének korlátozását, a kizárólag magyarországi helyszínt is beleértve, csak kiegészítő, egyik osztályban sem kötelező intézkedésként ismeri.⁵

4.2 A rendelkezési jog határa és a felelősség megosztása

A szervezet rendelkezésében lévő rendszer a szervezet EIR-jének minősül,⁶ így a VPS-en futó rendszer akkor is a Szervezeté, ha a szolgáltató hardverén fut. A rendelet számol a megosztott rendelkezési joggal.

(3) Ha a szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni. [7/2024. (VI. 24.) MK rendelet 2. § (3) bekezdés]

A Szervezet a saját rétegeiben közvetlenül teljesíti a követelményeket, a szolgáltatói réteg (adatközpont, fizikai szerver, hipervizor, tároló) intézkedéseit pedig a szolgáltató valósítja meg. Mivel a létesítményi intézkedések csak az EIR-t közvetlenül védő vagy támogató létesítményekre, a technológiai intézkedések pedig az érintett komponensekre vonatkoznak, [az adatközponti követelmények a Szervezet irodájára nem hárulnak át](#). Ezt az eltérést dokumentálni és jóváhagyni kell.⁷ Ez nem mentesítés, hanem áthelyezés. A szolgáltatói réteg követelményei a szerződésben és a szolgáltató bizonyítékaiban jelennek meg, a felelősség pedig a vezetőnél marad akkor is, ha felügyelt VPS-nél a szolgáltató kihelyezett (irányított) szolgáltatást nyújt.⁸

4.3 A közreműködő és a szerződéses követelmények

A VPS-szolgáltató közreműködő, mert részt vesz az EIR üzemeltetésében, és tárolja az adatokat.

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

⁴ 2024. évi LXIX. tv. 4. § 30. pont

⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.54. és 16.57. pont (O), valamint 20.4. pont

⁶ 2024. évi LXIX. tv. 6. § (1) bekezdés

⁷ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.2.1. és 3.2.4.2. pont, a dokumentálásról és a jóváhagyásról 3.1.2. és 3.1.3. pont

⁸ 2024. évi LXIX. tv. 6. § (6) bekezdés és 4. § 53. pont

(5) A szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében

[...]

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 minden osztályban három elemre bontja.

16.49. A szervezet:

16.49.1. Szerződéses kötelezettséggként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.

16.49.2. Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban.

16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont] (A, J, M)

Az első elem a szerződés, a második a felelősségi mátrix, a harmadik az ellenőrzés. A szerződésben rögzíteni kell a biztonsági osztályt, a védelmi intézkedéseket és a felelősség megosztását, a követelményeket az alvállalkozókra és a szolgáltató személyzetére is ki kell terjeszteni, jelentős és magas osztályban pedig a szolgáltatónak a szükséges portokat és protokollokat is meg kell adnia.⁹ Az EIR biztonságáért felelős személy a közreműködőtől tájékoztatást kérhet, és megismerheti a megfelelést alátámasztó dokumentumokat.¹⁰

A súlyos zavart vagy jelentős kárt okozó incidensről a Szervezetnek a tudomásszerzéstől számított 24 órán belül első bejelentést kell tennie a nemzeti kiberbiztonsági incidenskezelő központnak.¹¹ Ha a szolgáltató napok múlva értesít, ez nem tartható, ezért a kötelező értesítési megállapodásban órákban kell meghatározni a határidőt és rendezni az incidensinformációk megosztását.¹²

⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7., 19.7. és 14.11. pont (A, J, M), 16.51. pont (J, M)

¹⁰ 2024. évi LXIX. tv. 11. § (9) bekezdés

¹¹ 2024. évi LXIX. tv. 66. § (2) bekezdés; 418/2024. (XII. 23.) Korm. rendelet 1. § (6) bekezdés a) pont és 77. § (1) bekezdés 1. pont

¹² 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.19. pont (A, J, M) és 9.30. pont (J, M)

4.4 Az ellátási lánc és a szolgáltató értékelése

A NIS 2 irányelv a közvetlen szolgáltatók kiberbiztonsági gyakorlatának figyelembevételét is elvárja. A rendelet minden osztályban megköveteli az ellátási lánc kockázatainak felmérését, a kritikus beszállítók azonosítását és rangsorolását, jelentős és magas osztályban pedig azok rendszeres felülvizsgálatát.¹³ Számít, hogy a szolgáltató maga NIS2-kötelezett-e. A Kiberbiztonsági tv. a felhőszolgáltatóra főszabály szerint akkor alkalmazandó, ha üzleti tevékenységének fő helye Magyarországon van, és legalább közép vállalkozás.¹⁴ Egy kisvállalkozásnak minősülő hazai szolgáltató tehát csak akkor tartozik a hatálya alá, ha a hatóság azonosítja. Az uniós felhőszolgáltatókra az Unión belüli fő tevékenységi helyük szerinti tagállam felügyelete és a Bizottság végrehajtási rendelete vonatkozik, amelynek teljesítéséről bizonyíték kérhető.¹⁵

A megfelelés tanúsított IKT-szolgáltatással is igazolható, az uniós felhőtanúsítási rendszert (EUCS) azonban még nem fogadták el. A gyakorlatban ezért az ISO/IEC 27001 (a hatókör ellenőrzésével), az ISO/IEC 27017 és 27018, a BSI C5 és a CISPE adatvédelmi magatartási kódexe szolgál bizonyítékként.¹⁶

4.5 Az adathordozók és a tárolt adatok védelme

A törvény a védelem tárgyaként megnevezi az adathordozókat.¹⁷ A virtuális lemez, a pillanatkép és a mentés funkcionálisan adathordozó, amely a szolgáltatás végén kikerül a Szervezet ellenőrzési köréből, így rá a törlési követelmény közvetlenül alkalmazható.

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. [7/2024. (VI. 24.) MK rendelet 2. melléklet 11.8. pont] (A, J, M)

Mivel a szolgáltató a felszabadított tárterületet más ügyfélnek adja ki, a megfelelő technika a kriptográfiai törlés, amelyet az IEEE 2883 szabvány elfogadott módszerként kezel.¹⁸ A fizikai lemezek selejtezése a szolgáltató feladata, ezt a szerződésnek és a tanúsításnak le kell fednie.¹⁹ Jelentős és magas osztályban a tárolt adatok titkosítása kötelező.

¹³ (EU) 2022/2555 irányelv 21. cikk (2) bekezdés d) pont és (3) bekezdés; 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.5. és 1.22. pont (A, J, M), 19.16. pont (J, M)

¹⁴ 2024. évi LXIX. tv. 2. § (1) bekezdés c) pont, 1. § (1) bekezdés c) és d) pont, 2. melléklet 17. sor

¹⁵ (EU) 2022/2555 irányelv 26. cikk (1) bekezdés b) pont; a Bizottság (EU) 2024/2690 végrehajtási rendelete, különösen a melléklet 5. pontja (az ellátási lánc biztonsága)

¹⁶ 2024. évi LXIX. tv. 6. § (8) bekezdés; ISO/IEC 27017 (2026) és ISO/IEC 27018 (2025); a CISPE magatartási kódexről az EDPB 17/2021. számú véleménye (2021. május 19.)

¹⁷ 2024. évi LXIX. tv. 5. § (2) bekezdés a) pont

¹⁸ IEEE 2883-2022, Standard for Sanitizing Storage; a törlési program kialakításához lásd a NIST SP 800-88 Rev. 2 útmutatót (2025. szeptember)

¹⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.27. pont (A, J, M)

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)

Alap osztályban a titkosítás nem kötelező, a kriptográfia felhasználási területeit azonban ott is meg kell határozni,²⁰ és nyilvános felhőben nehéz a mellőzését indokolni. Ha a kulcsot a szolgáltató kezeli, a titkosítás az ellopott lemez ellen véd, a hatósági megkeresés vagy a szolgáltatói fiók kompromittálása ellen viszont nem. Ezért VPS-nél osztálytól függetlenül javasoljuk a következő kiegészítő intézkedést.

16.55. A szervezet kizárólagos ellenőrzést gyakorol a külső rendszerekben tárolt, vagy külső rendszerekbe továbbított titkos adatokhoz tartozó kriptográfiai kulcsok felett. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.55. pont] (O)

A mentést minden osztályban védeni kell, jelentős és magas osztályban kriptográfiailag és az elsődlegestől elkülönített helyszínen.²¹

4.6 Hozzáférés, üzemeltetés és naplózás

A privilegizált hozzáférés többtényezős hitelesítése már alap osztályban is kötelező.

8.3. A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez. [7/2024. (VI. 24.) MK rendelet 2. melléklet 8.3. pont] (A, J, M)

Privilegizált a szolgáltatói kezelőfelület fiókja is, mert onnan a szerver törölhető és konzolon elérhető. A távoli hozzáférést engedélyezni és dokumentálni kell, jelentős és magas osztályban titkosítással, menedzselt hozzáférési ponttal és a privilegizált műveletek naplózásával. A szolgáltató konzolon keresztüli beavatkozása távoli karbantartás, amelyet jóvá kell hagyni és nyilvántartásba kell venni.²² Minden osztályban kötelező a hibajavítás, a sérülékenységek ellenőrzése, a támogatás nélküli elemek cseréje vagy alternatív támogatása és a naplók védelme, magas osztályban a naplókat fizikailag elkülönült rendszeren is tárolni kell.²³

4.7 Adatvédelmi követelmények

Ha a VPS személyes adatot tárol, a szolgáltató adatfeldolgozó, mert a tárolás is adatkezelési művelet. Csak megfelelő garanciákat nyújtó adatfeldolgozó vehető igénybe, a jogviszonyt a GDPR 28. cikk (3) bekezdése szerinti szerződésben kell rögzíteni, további adatfeldolgozó pedig csak engedéllyel vonható be.²⁴ Az EDPB szerint az adatkezelőnek a teljes adatfeldolgozói láncot

²⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 17.53. pont (A, J, M)

²¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 7.35. pont (A, J, M), 7.19., 7.20. és 7.42. pont (J, M)

²² 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.100. és 10.11. pont (A, J, M), 2.102.-2.104. pont (J, M)

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.2., 15.9., 16.99. és 4.25. pont (A, J, M), 4.27. pont (M)

²⁴ (EU) 2016/679 rendelet (GDPR) 4. cikk 2. és 8. pont, 28. cikk (1)-(4) bekezdés; EDPB 07/2020. számú iránymutatás az adatkezelő és az adatfeldolgozó fogalmáról (2.0 verzió, 2021. július 7.)

bármikor ismernie kell.²⁵ A szerződés rendezi az adatok törlését vagy visszaadását és az adatvédelmi incidensről szóló késedelem nélküli értesítést.²⁶

Az EGT-n belüli adatközpont mellett is adattovábbítás valósulhat meg, ha a szolgáltató EGT-n kívüli személyzete távolról hozzáfér az adatokhoz.²⁷ Ha a szolgáltató vagy anyavállalata harmadik ország joghatósága alá tartozik, az ottani hatóság az adatok kiadását is kérheti, ami a GDPR 48. cikke szerint csak nemzetközi megállapodás alapján ismerhető el.²⁸ Az EU-USA adatvédelmi keretrendszer hatályos, a Törvényszék 2025-ben elutasította az ellene indított keresetet. A fellebbezés azonban folyamatban van, és az EDPB 2026 júliusában egy amerikai bírósági döntés miatt újabb vizsgálatot kért a Bizottságtól.²⁹ Amerikai háttérű szolgáltatónál ezért kiegészítő intézkedésekkel, elsősorban saját kulcsú titkosítással kell számolni,³⁰ a legegyszerűbb megoldás pedig az uniós tulajdonú szolgáltató EGT-n belüli adatközpontja.

4.8 A folytonosság és a kilépés

Minden osztályban kötelező az üzletmenet-folytonossági terv és a helyreállítás a meghatározott időn belül, jelentős és magas osztályban alternatív feldolgozási helyszín is kell.³¹ VPS-nél ez lehet egy második szolgáltató vagy régió. A váltást a Data Act jogként biztosítja. A szerződésnek a váltás kezdeményezésére legfeljebb két hónapos értesítési időt, legfeljebb 30 napos átállási időszakot, legalább 30 napos adatlekérési időt és teljes törlést kell tartalmaznia, 2027. január 12-től pedig váltási díj sem számítható fel.³²

4.9 A közszférába tartozó szervezetek

A Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) pontja, valamint honvédelmi célú rendszereik tekintetében az f) pontja alá tartozó szervezeteknél a nyilvános felhőben futó VPS nem privát felhőszolgáltatás,³³ amelynek külön feltételei vannak.

(4) Az 1. § (1) bekezdés a)–c) és a honvédelmi célú elektronikus információs rendszerei tekintetében az f) pontja szerinti szervezet kizárólag az adatosztályozás alapján, annak eredményére figyelemmel vehet igénybe nem privát felhőszolgáltatást, vagy kezelhet külföldön adatot, amennyiben más jogszabály a felhőszolgáltatás igénybevételét, vagy a külföldi adatkezelést nem tiltja vagy korlátozza. [2024. évi LXIX. tv. 9. § (4) bekezdés]

²⁵ EDPB 22/2024. számú vélemény az adatfeldolgozók és további adatfeldolgozók igénybevételéből eredő egyes kötelezettségekről (2024. október 7.)

²⁶ GDPR 28. cikk (3) bekezdés g) pont és 33. cikk (2) bekezdés

²⁷ EDPB 05/2021. számú iránymutatás a 3. cikk és az V. fejezet nemzetközi adattovábbításra vonatkozó rendelkezéseinek kölcsönhatásáról (2.0 verzió, 2023. február 14.)

²⁸ EDPB 02/2024. számú iránymutatás a GDPR 48. cikkéről (2.0 verzió, 2025. június 4.)

²⁹ (EU) 2023/1795 bizottsági végrehajtási határozat; T-553/23. sz. Latombe-ügy (2025. szeptember 3.) és C-703/25. P. sz. fellebbezés; az EDPB 2026. július 31-i levele. Magyar nyelvű tájékoztató a NAIH honlapján (naih.hu).

³⁰ EDPB 01/2020. számú ajánlás az adattovábbítási eszközöket kiegészítő intézkedésekről (2.0 verzió, 2021. június 18.)

³¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 7.2. és 7.43. pont (A, J, M), 7.23. pont (J, M)

³² (EU) 2023/2854 rendelet 23., 25. és 29. cikk

³³ 2024. évi LXIX. tv. 4. § 75. pont

Az a) pont szerinti szervezet csak költség-haszon elemzés és kilépési terv alapján, igazolt előny esetén dönthet a nem privát felhőszolgáltatás igénybevétele mellett. A b) és c) pont szerinti, valamint honvédelmi célú rendszereinél az f) pont szerinti szervezet legalább kilépési tervet készít.³⁴ A B2 szintű adatot technológiailag lehetséges esetben, a B3 és B4 szintűt mindig titkosítani kell. A kritikus sértetlenségű vagy rendelkezésre állású (SR2) adat csak EGT-tagállamban tárolható, és külföldi tárolásnál Magyarországon is rendelkezésre kell állnia. Nem privát felhőben az F2 adat az EGT-n belül tanúsítás nélkül is, az F3 adat az EGT-n belül csak a hatóság honlapján közzétett lista szerint tanúsított szolgáltatásban, egyébként csak Magyarországon kezelhető, az F4 adathoz pedig nyilvános VPS nem vehető igénybe.³⁵

A nemzeti kiberbiztonsági hatóság az adatosztályozást a biztonsági osztályba sorolás vizsgálatakor értékeli, és ha a nem privát felhő nem megengedett, a rendszer használatát nem hagyja jóvá.³⁶ Az 1. § (1) bekezdés d) pontja alá tartozó szervezeteknek ez a módszertan nem kötelező, de a helyszín kiválasztásához jó mérce.

5. FELHASZNÁLT FORRÁSOK

- [Az Európai Parlament és a Tanács \(EU\) 2022/2555 irányelve \(NIS 2 irányelv\)](#)
- [Az Európai Parlament és a Tanács \(EU\) 2016/679 rendelete \(általános adatvédelmi rendelet, GDPR\)](#)
- [Az Európai Parlament és a Tanács \(EU\) 2023/2854 rendelete \(Data Act\)](#)
- [A Bizottság \(EU\) 2024/2690 végrehajtási rendelete a NIS 2 irányelv szerinti kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeiről](#)
- [A Bizottság \(EU\) 2023/1795 végrehajtási határozata az EU-USA adatvédelmi keretrendszer szerinti megfelelő védelmi szintről](#)
- [2024. évi LXIX. törvény Magyarország kiberbiztonságáról \(Kiberbiztonsági tv.\)](#)
- [7/2024. \(VI. 24.\) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről](#)
- [418/2024. \(XII. 23.\) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról](#)
- [EDPB 07/2020. számú iránymutatás az adatkezelő és az adatfeldolgozó fogalmáról a GDPR-ban \(2.0 verzió, 2021\)](#)
- [EDPB 22/2024. számú vélemény az adatfeldolgozók és további adatfeldolgozók igénybevételeiből eredő egyes kötelezettségekről \(2024\)](#)
- [EDPB 01/2020. számú ajánlás az adattovábbítási eszközöket kiegészítő intézkedésekről \(2.0 verzió, 2021\)](#)
- [EDPB 05/2021. számú iránymutatás a 3. cikk és az V. fejezet kölcsönhatásáról \(2.0 verzió, 2023\)](#)

³⁴ 418/2024. (XII. 23.) Korm. rendelet 3. § (2)-(4) bekezdés

³⁵ 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 4.1., 4.2.1. és 4.2.2. pont

³⁶ 418/2024. (XII. 23.) Korm. rendelet 29. § (1) és (4) bekezdés; 2024. évi LXIX. tv. 24. § (1) bekezdés 17. pont

- [EDPB 02/2024. számú iránymutatás a GDPR 48. cikkéről \(2.0 verzió, 2025\)](#)
- [EDPB 17/2021. számú vélemény a CISPE adatvédelmi magatartási kódexéről \(2021\)](#)
- [NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations \(5.2.0 kiadás, 2025\)](#)
- [NIST Special Publication 800-88 Revision 2, Guidelines for Media Sanitization \(2025\)](#)
- [IEEE 2883-2022, Standard for Sanitizing Storage](#)
- ISO szabványok: [ISO/IEC 27001 \(2022\)](#), [ISO/IEC 27017 \(2026\)](#) és [ISO/IEC 27018 \(2025\)](#) szabványok
- [CERT-EU tájékoztató egy biztonsági eszköz ellátási láncát érintő incidensről \(2026\)](#)
- [CA/Browser Forum SC-081v3 szavazás a TLS-tanúsítványok érvényességi idejéről \(2025\)](#)
- A 2. mellékletben szereplő szolgáltatók honlapjai és közzétett dokumentumai (2026. szeptember 30.)

MKIK NIS2 Tudásközpont kiadványai és iránymutatásai: [MKIK Jogi állásfoglalások](#) és [MKIK Iránymutatások](#)

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

6. KAPCSOLÓDÓ MKIK-ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- MKIK-29 [Egy középvállalkozás méretet el nem érő felhő szolgáltató a Kiberbiztonsági tv. hatálya alá tartozik –e?](#)
- 2026/10 [A KÖZREMŰKÖDŐVEL KÖTÖTT SZERZŐDÉS TARTALMA](#)
- MKIK-18 [Hogyan ellenőrizheti egy NIS2 kötelezett cég az általa megbízott közreműködő kiberbiztonsági megfelelését?](#)
- MKIK-50 [Elhagyható-e a szerverszoba NIS2 kötelezett szervezet esetén?](#)
- MKIK-56 [Mikro- és kisvállalkozások számára ajánlott mentési stratégia és mentőeszközök](#)

1. MELLÉKLET

A VPS-szolgáltatáshoz kapcsolódó követelmények a 7/2024. (VI. 24.) MK rendelet 2. melléklete alapján

A táblázat a VPS-szolgáltatás igénybevételénél leggyakrabban 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. A felelős oszlop a tipikus, nem felügyelt VPS-szolgáltatást feltételezi. A Szolgáltató jelölés azt jelenti, hogy a követelmény a szolgáltatónál teljesül, a Szervezet pedig a szerződéssel és a szolgáltató bizonyítékaival igazolja. A táblázat nem helyettesíti a rendszerre vonatkozó teljes követelménykatalógus alkalmazását.

Pont	Követelmény	Osztály	Felelős	Teljesítés VPS-környezetben
Irányítás, nyilvántartás és tervezés				
1.5.	Elektronikus információs rendszerek nyilvántartása	A, J, M	Szervezet	A VPS-en futó EIR felvétele a nyilvántartásba, a szolgáltató és a helyszín megjelölésével.
1.21.	Ellátási lánc kockázatmenedzsment stratégiája	A, J, M	Szervezet	A felhőszolgáltatások igénybevételének szempontjai az ellátási lánc kockázatmenedzsment stratégiájában.
1.22.	Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói	A, J, M	Szervezet	A VPS-szolgáltató kritikus beszállítóként történő azonosítása és rangsorolása.
13.2.	Rendszerbiztonsági terv	A, J, M	Szervezet	A rendszerbiztonsági terv rögzíti a szolgáltatónál működő elemeket, a működési környezetet és a függőségeket.

Pont	Követelmény	Osztály	Felelős	Teljesítés VPS-környezetben
6.52.	Információ helyének azonosítása és dokumentálása	J, M	Szervezet	Az adatok és a feldolgozó rendszerelemek helyének (ország, adatközpont, régió) dokumentálása, a változások követése.
15.4.	Kockázatelemzés	A, J, M	Szervezet	A kockázatelemzés kiterjed a megosztott infrastruktúrára, a szolgáltató kiesésére és a joghatósági kiterjedtségre.
15.5.	Kockázatelemzés – Ellátási lánc	A, J, M	Szervezet	Ellátásilánc-kockázatelemzés a szolgáltatóra, jelentős változásokkor frissítve.
Beszerezés, szerződés és ellátási lánc				
16.7.	Beszerezések	A, J, M	Közös	A szerződés rögzíti a biztonsági osztályt, a védelmi intézkedéseket és a felelősség megosztását.
16.49.	Külső elektronikus információs rendszerek szolgáltatásai	A, J, M	Közös	Szerződéses megfelelés, felelősségi mátrix, a szolgáltató ellenőrzése tanúsítványok és auditjelentések alapján.
16.51.	Külső információs rendszerek szolgáltatásai – Funkciók, portok, protokollok és szolgáltatások azonosítása	J, M	Szolgáltató	A szolgáltatáshoz szükséges funkciók, portok és protokollok megadása.
16.54.	Külső információs rendszerek szolgáltatásai – Feldolgozás, tárolás és szolgáltatási helyszín	O	Közös	Az adatközpont és a régió szerződéses rögzítése, javasolt kiegészítő intézkedés.
16.55.	Külső információs rendszerek szolgáltatásai – Felügyelt kriptográfiai kulcsok	O	Szervezet	Saját kezelésű titkosítási kulcsok, VPS-nél osztálytól függetlenül javasolt.
16.57.	Külső információs rendszerek szolgáltatásai – Feldolgozási és tárolási helyszín – Magyarország joghatósága	O	Közös	Kizárólag magyarországi helyszín, ha a kockázatelemzés vagy más jogszabály indokolja.
19.2.	Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	A, J, M	Szervezet	Az ellátási lánc kockázatmenedzsment szabályzata kiterjed a felhőszolgáltatókra.
19.4.	Ellátási láncra vonatkozó követelmények és folyamatok	A, J, M	Szervezet	Az ellátási láncra vonatkozó kontrollok dokumentálása a szabályzatokban.
19.7.	Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók	A, J, M	Szolgáltató	A követelmények továbbhárítása az alvállalkozókra és a további adatfeldolgozókra.
19.13.	Beszerezési stratégiák, eszközök és módszerek	A, J, M	Szervezet	Olyan beszerzési módszer, amely a tanúsítást, a helyszínt és a kilépést is értékeli.
19.16.	Beszállítók értékelése és felülvizsgálata	J, M	Szervezet	Rendszeres, javasoltan éves beszállítói felülvizsgálat, a tanúsítványok érvényességének ellenőrzése.
19.19.	Értesítési megállapodások	A, J, M	Közös	Értesítési megállapodás az incidensekről, a sérülékenységekről és a szolgáltatás változásairól.
14.11.	Külső személyekhez kapcsolódó biztonsági követelmények	A, J, M	Szolgáltató	A szolgáltatói személyzetre vonatkozó biztonsági követelmények és azok ellenőrzése.
5.7.	Információcsere	A, J, M	Közös	A VPS és a Szervezet más rendszerei közötti kapcsolatok engedélyezése és dokumentálása.

Pont	Követelmény	Osztály	Felelős	Teljesítés VPS-környezetben
Hozzáférés és hitelesítés				
2.2.	Fiókkezelés	A, J, M	Szervezet	A szerver és a szolgáltatói kezelőfelület fiókjainak kezelése, közös fiókok nélkül.
2.60.	Legkisebb jogosultság elve	J, M	Szervezet	Legkisebb jogosultság a szerveren és a kezelőfelületen, szerepkörök szerint.
2.65.	Legkisebb jogosultság elve – Privilegizált fiókok	J, M	Szervezet	A root és a kezelőfelületi adminisztrátori jogosultság kijelölt személyekre korlátozva.
2.100.	Távoli hozzáférés	A, J, M	Szervezet	A távoli hozzáférés módjai (SSH, VPN, konzol) engedélyezve és dokumentálva.
2.102.	Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által	J, M	Szervezet	Titkosított adminisztrációs csatorna (SSH, VPN, TLS).
2.103.	Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok	J, M	Szervezet	Belépés VPN-en vagy ugrószerveren keresztül, nyílt adminisztrációs port nélkül.
2.104.	Távoli hozzáférés – Privilegizált parancsok és hozzáférés	J, M	Szervezet	A privilegizált műveletek naplózása, a távoli hozzáférés indoklása a rendszerbiztonsági tervben.
8.2.	Azonosítás és hitelesítés	A, J, M	Szervezet	Egyedi fiókok, a tevékenységek személyhez köthetők.
8.3.	Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése	A, J, M	Szervezet	Többtényezős hitelesítés a rendszergazdai és a kezelőfelületi fiókokon.
8.4.	Azonosítás és hitelesítés (felhasználók) – Nem-privilegizált fiókok többtényezős hitelesítése	J, M	Szervezet	Többtényezős hitelesítés a nem privilegizált hozzáféréseknél is.
8.21.	A hitelesítésre szolgáló eszközök kezelése	A, J, M	Szervezet	Az SSH-kulcsok, API-tokenek és tanúsítványok kiadása, cseréje és visszavonása.
10.11.	Távoli karbantartás	A, J, M	Közös	A szolgáltatói konzol- és mentőrendszer-hozzáférés jóváhagyása és nyilvántartása.
Konfiguráció, sérülékenység és sértetlenség				
6.2.	Alapkonfiguráció	A, J, M	Szervezet	Dokumentált, verziókezelte alapkonfiguráció, például kódként kezelt infrastruktúra.
6.23.	Konfigurációs beállítások	A, J, M	Szervezet	Keményítés elismert, platformspecifikus ajánlás szerint, az eltérések dokumentálásával.
6.26.	Legszűkebb funkcionalitás	A, J, M	Szervezet	Csak a szükséges szolgáltatások és portok, a többi letiltva.
6.36.	Rendszerelem leltár	A, J, M	Szervezet	Leltár a VPS-példányokról, kötetekről, pillanatképekről és hálózati elemekről.
15.9.	Sérülékenységek ellenőrzése	A, J, M	Szervezet	Rendszeres sérülékenységvizsgálat és határidőhöz kötött javítás.
18.2.	Hibajavítás	A, J, M	Szervezet	Automatikus biztonsági frissítés, a kritikus javítások meghatározott időn belül.

Pont	Követelmény	Osztály	Felelős	Teljesítés VPS-környezetben
18.8.	Kártékony kódok elleni védelem	A, J, M	Szervezet	Kártékony kód elleni védelem a be- és kilépési pontokon, például fájlfeltöltésnél.
18.13.	Az EIR monitorozása	A, J, M	Szervezet	Rendszerfelügyelet, a támadások és a jogosulatlan kapcsolatok észlelése.
16.99.	Támogatással nem rendelkező rendszerelemek	A, J, M	Szervezet	A gyártói támogatás nélküli operációsrendszer-képek cseréje vagy alternatív támogatása.
Naplózás				
4.2.	Naplózható események	A, J, M	Szervezet	A szerver és a kezelőfelület naplózandó eseményeinek meghatározása.
4.13.	Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel	A, J, M	Szervezet	A naplók rendszeres elemzése és riasztás.
4.24.	Időbélyegek	A, J, M	Szervezet	Szinkronizált időbélyeg a koordinált világidő feltüntetésével.
4.25.	Naplóinformációk védelme	A, J, M	Szervezet	A naplók védelme, gyűjtés a szerveren kívül.
4.27.	A naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemek	M	Szervezet	Tárolás fizikailag elkülönült rendszeren, például másik szolgáltatónál.
4.38.	A naplóbejegyzések megőrzése	A, J, M	Szervezet	Megőrzés a meghatározott ideig.
Hálózat és kriptográfia				
17.10.	Információk az osztott használatú rendszererőforrásokban	J, M	Szolgáltató	A virtuális gépek elkülönítése a hipervízor szintjén.
17.12.	Szolgáltatásmegtagadással járó támadások elleni védelem	A, J, M	Közös	Szolgáltatói DDoS-védelem, a Szervezet oldalán terheléskorlátozás.
17.17.	A határok védelme	A, J, M	Közös	Szolgáltatói és helyi tűzfal, a nyilvános szolgáltatások elkülönítése.
17.20.	A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés	J, M	Szervezet	Alapértelmezetten tiltó szabályrendszer mindkét tűzfalon.
17.41.	Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem	J, M	Szervezet	TLS és titkosított adminisztrációs csatornák.
17.49.	Kriptográfiai kulcs előállítása és kezelése	A, J, M	Szervezet	A titkosítási és SSH-kulcsok előállítása, tárolása és megsemmisítése.
17.53.	Kriptográfiai védelem	A, J, M	Szervezet	A kriptográfia felhasználási területeinek meghatározása.
17.81.	Tárolt (at rest) adatok védelme	J, M	Szervezet	A tárolt adatok bizalmasságának és sértetlenségének védelme.
17.82.	Tárolt (at rest) adatok védelme – Kriptográfiai védelem	J, M	Szervezet	Operációsrendszer-szintű kötetitkosítás saját kezelésű kulccsal.
Adathordozók				
11.2.	Hozzáférés az adathordozókhoz	A, J, M	Szervezet	A kötetekhez, pillanatképekhez és mentésekhez való hozzáférés korlátozása.
11.8.	Adathordozók törlése	A, J, M	Közös	Kriptográfiai törlés a Szervezetnél, a fizikai adathordozók törlése a szolgáltatónál.

Pont	Követelmény	Osztály	Felelős	Teljesítés VPS-környezetben
11.9.	Adathordozók törlése – Felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés	M	Közös	A törlés dokumentálása és a szolgáltatói igazolás megőrzése.
11.13.	Adathordozók törlése – Adatok távoli törlése vagy megsemmisítése	O	Szervezet	Távoli törlés képessége, például a kulcsok megsemmisítésével.
19.27.	Rendszerelem selejtezése, megsemmisítése	A, J, M	Szolgáltató	A fizikai adathordozók selejtezése elismert módszertan szerint.
Mentés, folytonosság és incidenskezelés				
7.2.	Üzletmenet-folytonossági terv	A, J, M	Szervezet	Üzletmenet-folytonossági terv a szolgáltató kiesésére is.
7.8.	Üzletmenet-folytonossági terv – Együttműködés külső szolgáltatókkal	O	Közös	A szolgáltató folytonossági tervével való összehangolás.
7.19.	Biztonsági tárolási helyszín	J, M	Szervezet	Biztonsági tárolási helyszín a szolgáltatótól függetlenül.
7.20.	Biztonsági tárolási helyszín – Elkülönítés az elsődleges tárolási helyszíntől	J, M	Szervezet	A mentések eltérő szolgáltatónál vagy régióban.
7.23.	Alternatív feldolgozási helyszín	J, M	Szervezet	Alternatív feldolgozási helyszín, második szolgáltató vagy régió.
7.35.	Az elektronikus információs rendszer mentései	A, J, M	Szervezet	Rendszeres, kliensoldalon titkosított mentés.
7.36.	Az elektronikus információs rendszer mentései – Megbízhatóság és sértetlenség tesztelése	J, M	Szervezet	A mentések rendszeres visszaállítási próbája.
7.42.	Az elektronikus információs rendszer mentései – Kriptográfiai védelem	J, M	Szervezet	A mentések kriptográfiai védelme.
7.43.	Az elektronikus információs rendszer helyreállítása és újraindítása	A, J, M	Szervezet	Helyreállítás a meghatározott helyreállítási időn belül.
9.27.	A biztonsági események jelentése	A, J, M	Szervezet	Bejelentés a nemzeti kiberbiztonsági incidenskezelő központnak (24 óra, 72 óra, egy hónap).
9.19.	Biztonsági események kezelése – Ellátási lánc koordinációja	O	Közös	Az incidenskezelés összehangolása a szolgáltatóval.
9.30.	A biztonsági események jelentése – Ellátási lánc koordinációja	J, M	Közös	Az incidensekkel kapcsolatos információk megosztása a szolgáltatóval.
Fizikai és környezeti védelem				
12.1.	Szabályzat és eljárásrendek	A, J, M	Szervezet	Saját fizikai védelmi szabályzat, amely a szolgáltatónál működő elemekre a szerződéses garanciákra utal.
12.43.	Munkavégzésre kijelölt alternatív helyszín	J, M	Szervezet	A távoli adminisztráció munkahelyeinek meghatározása és védelme.
12.	Fizikai és környezeti védelem (az adatközpontra vonatkozó követelmények)	eltérő	Szolgáltató	A 2. § (3) bekezdés alapján a Szervezet saját kötelezettsége nem terjed ki az adatközpontra, a szolgáltatói teljesítést a 16.49. pont szerint szerződéssel, tanúsítvánnyal és auditjelentéssel kell biztosítani és ellenőrizni.

2. MELLÉKLET

Szolgáltatói példák

A táblázat hazai VPS-szolgáltatók nyilvánosan elérhető adatait foglalja össze, a távközlési háttérű és a tárhely- és szerverszolgáltatókat külön csoportban. A vizsgált szolgáltatók magyarországi székhelyűek, és jellemzően magyarországi, főként budapesti adatközpontokból szolgáltatnak, tanúsítottságuk és szerződéses dokumentációjuk azonban vegyes. ISO/IEC 27001 tanúsításra a szolgáltatók valamivel több mint fele hivatkozik, és a tanúsítvány hatóköre nem mindig terjed ki az adatközpontra. Közzétett adatfeldolgozói szerződés csak néhány szolgáltatónál érhető el, a többinél egyedileg kell kérni. A hazai székhely nem jelent feltétlenül hazai tulajdont, és van olyan szolgáltató, amely külföldi helyszínt is kínál. A tulajdonosi háttérrel ezért a beszállítói értékelésben ellenőrizni, a helyszínt pedig a szerződésben és a szerver létrehozásakor is rögzíteni kell. A tanúsítások a szolgáltatók saját közlésein alapulnak, a tanúsítvány hatókörét, érvényességét és az alkalmazhatósági nyilatkozatot a szerződéskötés előtt minden esetben ellenőrizni kell.

Szolgáltató	VPS-szolgáltatás és helyszín	Tanúsítások és vállalások	Adatfeldolgozói szerződés, megjegyzés
Távközlési háttérű szolgáltatók			
Magyar Telekom Nyrt. és Telekom Rendszerintegráció Zrt. (Budapest)	Virtuális szerverek, virtuális szerverbérlet. Saját adatközpontok Budapesten, Budaörsön és Szegeden.	ISO/IEC 27001 (a Magyar Telekom tanúsítványa 2026. december 3-ig érvényes), ISO 22301 az adatközponti szolgáltatásokra, 2025. évi kiberbiztonsági auditigazolás.	Nyilvános adatfeldolgozói szerződés nem ellenőrzött, egyedileg kérendő.
One Magyarország Zrt. (Budapest)	One Flex Cloud (önkiszolgáló IaaS), virtuális szerverinfrastruktúra és dedikált virtuális környezet. A honlap szerint az infrastruktúra Magyarországon, két földrajzilag elkülönült helyszínen működik, a városokat nem nevezi meg. Az Invitech ICT Services Kft. 2025. október 1-jén olvadt be a társaságba.	ISO-tanúsítvány a honlapon nem található. Az Uptime Institute nyilvántartása szerint a korábbi Invitech DC10-III budapesti adatközpont Tier III tervezési és létesítési minősítéssel rendelkezik.	Nyilvános adatfeldolgozói szerződés nem található, egyedileg kérendő. Tulajdonosa a 4iG Távközlési Holding Zrt. (a 4iG Nyrt. és a Corvinus Nemzetközi Befektetési Zrt. közös tulajdona). A felhőplatform technológiai háttérét a honlap nem nevezi meg, ellátásilánc-szempontról érdemes rákérdezni.
ACE Telecom Kft. (Budapest)	Virtuális szerver (VPS), távoli elérés titkosított VPN-csatornán. Két budapesti adatközpont (Váci út 188. és a Victor Hugo utcai BIX-épület), georedundáns kialakítással.	ISO/IEC 27001:2022 (MSZT), hatóköre kiterjed a szerverhosting- és felhőalapú adatközponti szolgáltatásra és mindkét adatközpontra, 2028. április 10-ig érvényes. A honlapon NIS2-jelölés látható, tartalmát a honlap nem részletezi.	A közzétett általános szerződési feltételek a VPS-szolgáltatásra nem terjednek ki, adatfeldolgozói szerződés nem található, mindkettő egyedileg kérendő. Saját közlése szerint 100%-ban magyar tulajdonú.

Szolgáltató	VPS-szolgáltatás és helyszín	Tanúsítások és vállalások	Adatfeldolgozói szerződés, megjegyzés
Tárhely- és szerverszolgáltatók			
RackForest Zrt. (Budapest)	Linux és Windows SSD VPS, Prémium AMD VPS. Három budapesti adatközponti helyszín, a honlap nem jelöli, melyik szolgálja ki a VPS-t.	ISO/IEC 27001 (2022), a honlapon közzétett tanúsítvány 2025. februári keltezésű.	Adatkezelési szabályzata szerint a VPS- és felhőszolgáltatásnál adatfeldolgozó. Külön adatfeldolgozói szerződésminta a honlapon nem található, egyedileg kérendő.
DotRoll Kft. (Budapest)	KVM VPS és Prémium VPS. A honlap budapesti adatközpontokat nevez meg.	ISO 27001 (a honlap jelzése szerint). Saját közlése szerint 2026 áprilisában a Kiberbiztonsági tv. szerinti kiberbiztonsági auditon megfelelt.	Letölthető GDPR adatfeldolgozói megállapodás.
Tárhely.Eu Szolgáltató Kft. (Budapest)	KVM, NVMe felhő és VMware VPS. Három budapesti adatközpont.	ISO-tanúsítvány a honlapon nem található.	Adatfeldolgozói rendelkezések az általános szerződési feltételekben.
ServerAstra Kft. (Budapest)	Felhőszerver és KVM VPS. Budapest (Dataplex), emellett New York-i helyszín is, ezért a helyszínt szerződésben kell rögzíteni.	Az adatközpont tanúsításaira hivatkozik, saját ISO-tanúsítvány nem található.	Adatkezelési rendelkezések az általános szerződési feltételekben, külön dokumentum a technikai intézkedésekről.
Rackhost Zrt. (Szeged)	Önmenedzselt virtuális szerver, külön díjas szerverüzemeltetési szolgáltatással. Saját adatközpontok Szegeden és Budapesten (BIX-épület), külföldi helyszín nincs.	Saját közlése szerint ISO/IEC 27001 és ISO 9001 (2023), a tanúsítványok hatóköre és érvényessége a honlapon nem szerepel.	Közzétett, a GDPR 28. cikk (3) bekezdése szerinti adatfeldolgozói megállapodás (2026. szeptember 1-jétől hatályos): elsődlegesen EGT-n belüli feldolgozás, további adatfeldolgozó nincs, incidensértesítés 48 órán belül. A tárolt adatok titkosítása a vállalt intézkedések között nem szerepel. Saját közlése szerint 100%-ban magyar tulajdonú.
Nethely Kft. (Budapest)	Prémium tárhely: ügyfelenként dedikált, VPS-alapú, felügyelt szerver SSH-hozzáféréssel, klasszikus VPS-t nem kínál. Két budapesti, bérelt adatközponti helyszín.	ISO/IEC 27001 (e.com-CERT, 2027. július 9-ig érvényes), hatóköre a webtárhely-szolgáltatásra és a domainregisztrációra terjed ki, az adatközpontokat nem tartalmazza. ISO 9001.	Adatfeldolgozói szerződés az általános szerződési feltételekben és a honlapon nem található, egyedileg kérendő. Napi mentés, elkülönített fizikai helyszínen.
INTEGRITY Kft. (Székesfehérvár)	Xen-alapú VPS és VMware-alapú virtuális adatközpont, csak üzleti ügyfeleknek. A VPS-oldal az adatközpont helyét nem nevezi meg, a cég budapesti telephelye a Victor Hugo utcai BIX-épületben van.	ISO-tanúsításra vagy NIS2-megfelelésre vonatkozó közlés a honlapon nem található.	Adatfeldolgozói rendelkezés az általános szerződési feltételekben nem szerepel, egyedileg kérendő. Választható napi mentés, rendszerüzemeltetés is igénybe vehető.

Szolgáltató	VPS-szolgáltatás és helyszín	Tanúsítások és vállalások	Adatfeldolgozói szerződés, megjegyzés
NewPush Europe Kft. (MikroVPS, Vác)	KVM-alapú VPS, önmenedzselt vagy felügyelt változatban. A honlap magyarországi helyszínt jelöl, az adatközpontot nem nevezi meg.	ISO-tanúsítvány a honlapon nem található.	Az adatfeldolgozói függelék az általános szerződési feltételek része. Általános felhatalmazást ad további adatfeldolgozókra, köztük amerikai szolgáltatókra, az adatok helyére nem tartalmaz kikötést. A társaság egy egyesült államokbeli cégcsoporthoz tartozik, ezért a harmadik országbeli joghatóságot vizsgálni kell.

A táblázat a szolgáltatók honlapjain és közzétett dokumentumaiban 2026. szeptember 30-án elérhető információkon alapul. A felsorolás nem teljes körű, a sorrend nem jelent rangsort, és a megnevezés nem minősül ajánlásnak.

FELELŐSSÉGGKIZÁRÓ NYILATKOZAT

Az állásfoglalás a 2026. szeptember 30-án hatályos jogszabályok és a nyilvánosan elérhető információk alapján készült, és nem minősül egyedi ügyben adott jogi tanácsnak.

A 2. mellékletben szereplő szolgáltatók, valamint a szoftveres és technológiai megoldások bemutatása nem teljes körű, példálózó jellegű, és nem minősül ajánlásnak vagy termékminősítésnek. A szolgáltatókra vonatkozó adatok a szolgáltatók által 2026. szeptember 30-án közzétett információkat tükrözik. A piacon folyamatosan jelennek meg új megoldások, a meglévők funkciói, licencfeltételei, tanúsításai és tulajdonosi viszonyai pedig változhatnak, ezért a kiválasztás előtt az aktuális állapotot minden esetben ellenőrizni kell. A megnevezett termék- és cégnevek jogosultjaik tulajdonát képezik.