

A Data Act kiberbiztonsági kockázatai KKV-k esetében

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/56

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.25	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A Data Act, vagyis az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (a magyar hivatalos szövegben „adatrendelet”, a továbbiakban „Data Act”) 2025. szeptember 12. óta alkalmazandó, és az összekapcsolt termékek, valamint a kapcsolódó szolgáltatások által generált adatokhoz teremt hozzáférési jogot a felhasználók javára.

A KKV-k a rendeletben egyszerre jelennek meg kedvezményezettként és kötelezettként. Felhasználóként a saját gépeik és eszközeik adatait kérhetik ki a gyártótól, és azokat harmadik félnek, például független szerviznek adhatják át. Adatbirtokosként azonban maguk is kötelezetté válhatnak, ha összekapcsolt terméket gyártanak, kapcsolódó szolgáltatást nyújtanak, vagy a kapott adatokat továbbadják.

A mikro- és kisvállalkozások gyártói mentessége nem terjed ki minden esetre, a középvállalkozásokra pedig a rendelet egy év átmenet után teljes egészében vonatkozik.

Kiberbiztonsági szempontból a Data Act nem új védelmi követelményrendszer, hanem új, jogszabályon alapuló adatkiáramlási csatorna, amely az alábbi pontokon sebezhető:

- Az adatbirtokosnál a kötelező hozzáférési felület új támadási felületet nyit, amelyen a jogosult felhasználó és a támadó azonos formájú kérelemmel jelentkezik.
- Az adatot fogadó KKV-nál az üzleti titok, a termékbiztonság és a személyes adat védelme egyszerre válik szerződéses és technikai feladattá.
- A két fél között pedig az ellátási lánc hosszabbodik meg a harmadik felekkel, a felhőszolgáltatókkal és az alvállalkozókkal.

Adatvédelmi szempontból a legnagyobb kockázat a vegyes adatállomány, mert az ipari és a flottaadatok szinte mindig tartalmaznak természetes személyre visszavezethető adatot, a gépkezelő azonosítójától a jármű helyzetéig. A Data Act ilyenkor nem ad önálló jogalapot, a GDPR szabályai változatlanul alkalmazandók, és a személyes adatokat érintő jogsértések miatt a NAIH a GDPR bírságkeretével járhat el.

A javasolt válasz az adatmegosztás beépítése a meglévő NIS2 kockázatmenedzsment keretrendszerbe. A hozzáférési felületet, a kiadott és a fogadott adatköröket, valamint az érintett partnereket a KKV a rendszerbiztonsági tervben, a kockázatelemzésben, a szerződésekben és a naplózásban ugyanúgy kezeli, mint bármely más külső kapcsolatot. A 7/2024. (VI. 24.) MK rendelet 2. mellékletének védelmi intézkedései erre közvetlenül alkalmazhatók, ezért a megfelelés nem új rendszer bevezetését, hanem a meglévő kontrollok hatókörének kiterjesztését jelenti.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy magyarországi kis- vagy középvállalkozás (a továbbiakban „Szervezet”) összekapcsolt termékeket, például ipari gépeket, járműflottát, energetikai vagy épületgépészeti eszközöket üzemeltet, és a NIS2 irányelvet átültető, Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban „Kiberbiztonsági tv.”) hatálya alá tartozik vagy tartozhat.¹ A Szervezet

¹ 2024. évi LXIX. törvény, hatályos 2025. január 1-től, 1. § (1) bekezdés d) és e) pont, valamint 2. és 3. melléklet

vezetése arra keres választ, hogy a Data Act milyen új jogokat és kötelezettségeket teremt számára, és az ezekből fakadó adatmegosztás milyen kiberbiztonsági és adatvédelmi kockázatot hordoz.

Az állásfoglalás a Data Act lényegét és alkalmazási mérföldköveit, a KKV-k adatigénylési lehetőségeit és adatszolgáltatási kötelezettségeit, az adatszolgáltatás kiberbiztonsági és adatvédelmi kockázatait, a javasolt kockázatcsökkentő intézkedéseket, valamint a kockázatokat lefedő NIS2 kontrollokat vizsgálja.

Nem tárgya az állásfoglalásnak a felhőszolgáltató-váltás részletes szabályozása, az intelligens szerződések, az ágazati adatmegosztási jogszabályok és a kiberrezilienciáról szóló rendelet (CRA) részletes ismertetése.

3. GYAKORLATI JAVASLATOK

3.1 Ha a Szervezet adatot igényel

Az adatigénylés a Szervezet számára lehetőség, a kapott adat azonban azonnal védendő vagyonelemmé válik. A javasolt szabályok a következők.

- a) Az igénylés előtt a Szervezet rögzíti, milyen célra, milyen adatkört és milyen gyakorisággal kér, és a célt a harmadik féllel kötött szerződésben is megjeleníti, mert a harmadik fél csak a megállapodott célra kezelheti az adatot.
- b) A kapott adatot a Szervezet a rendszerelem-leltárban rögzített, biztonsági osztályba sorolt rendszerben tárolja, és a hozzáférést a szükséges ismeret elvén korlátozza.
- c) A szervezet a kapott adattal kiegészíti az adatvagyon felmérés és üzleti hatáselemzés (BIA) táblázatát
- d) A gyártó által üzleti titokként megjelölt adatokra a Szervezet titoktartási és technikai védelmi intézkedéseket vállal, és ezeket be is vezeti, mert a vállalt intézkedések elmulasztása a hozzáférés felfüggesztéséhez, súlyosabb esetben törlési és kártérítési igényhez vezet.
- e) Harmadik fél (szerviz, elemző cég, platform) bevonásakor a Szervezet ellenőrzi, hogy a partner nem kapuőr, nem adja tovább az adatot, nem használja profilalkotásra és a termék biztonságát hátrányosan érintő módon.
- f) A Szervezet nem használja ki a gyártó hozzáférési felületének gyengeségeit akkor sem, ha a gyártó a kérelmet késve vagy hiányosan teljesíti. Ilyenkor a jogorvoslat a hatósági panasz vagy a vitarendezési testület.

3.2 Ha a Szervezet adatot szolgáltat

Ha a Szervezet gyártóként, kapcsolódó szolgáltatás nyújtójaként vagy a kapott adatok továbbadójaként adatbirtokos, az adatszolgáltatást önálló, biztonsági szempontból megtervezett folyamatként kezelje.

- a) A Szervezet azonosítja, hogy adatbirtokos-e, és ha mikro- vagy kisvállalkozás, ellenőrzi, hogy a mentesség feltételei (nincs nem KKV partner- vagy kapcsolt vállalkozás, nincs alvállalkozói megbízás) ténylegesen fennállnak-e.

- b) A hozzáférési felület (programozási felület, letöltési portál, eszközön való hozzáférés) önálló rendszerelemként kerül a rendszerbiztonsági tervbe, hálózatilag elkülönítve, naplózva és hitelesítéshez kötve.
- c) A kérelmező azonosítása arányos, de megbízható. A Szervezet nem kér a szükségesnél több adatot, de a jogosultság ellenőrzése nélkül nem ad ki adatot, a visszaélés gyanús kérélmeket pedig biztonsági eseményként kezeli.
- d) Az üzleti titkokat a Szervezet előre azonosítja, a metaadatokban is megjelöli, és a titoktartási megállapodás, valamint a technikai intézkedések megkötése előtt nem adja ki. A megtagadás vagy felfüggesztés csak írásban indokolt döntéssel és az illetékes hatóság értesítésével lehetséges.
- e) A személyes adatokat tartalmazó adatköröket a Szervezet elkülöníti, a kiadás előtt GDPR-jogalapot vizsgál, és ahol lehet, anonimizál vagy álnevesít. Közsférabeli adatigénylésnél az anonimizálás a főszabály.
- f) A közsférabeli szükséghelyzeti adatigénylést a Szervezet a kérelem kötelező tartalmi elemei és az adatkoordinátor nyilvántartása alapján ellenőrzi, mert az ilyen kérelem a társadalmi mérnökség eszköze is lehet.

3.3 A javasolt eljárás

A fenti szabályok bevezetését az alábbi lépésekben javasoljuk.

- a) Érintettség-vizsgálat, a Szervezet szerepének (felhasználó, adatbirtokos, harmadik fél) meghatározása termékenként, a KKV-mentesség feltételeinek dokumentálásával.
- b) Adatleltár, a rendelet hatálya alá tartozó adatok, azon belül a személyes adatok és az üzleti titkok azonosítása és megjelölése a metaadatokban is.
- c) Kockázatelemzés, az adatmegosztási folyamat felvétele a NIS2 kockázatelemzésbe, szükség esetén adatvédelmi hatásvizsgálattal.
- d) Szerződések, a gépbeszerzési és szolgáltatási szerződések, a titoktartási megállapodások és a harmadik felekkel kötött adatmegosztási szerződések felülvizsgálata a Bizottság ajánlott minta-szerződési feltételei alapján.²
- e) Technikai kialakítás, a hozzáférési felület elkülönítése, a hitelesítés, a naplózás, a titkosított adattovábbítás és a kiadott adatok mennyiségének korlátozása.
- f) Eljárásrend, az adatigénylések fogadására, ellenőrzésére, teljesítésére és megtagadására vonatkozó belső eljárás, beleértve a hatósági értesítést és az incidensbejelentést.
- g) Felülvizsgálat, a kiadott adatkörök, a partnerek és a hozzáférési naplók legalább évenkénti ellenőrzése, a kockázatelemzés frissítésével.

² Európai Bizottság, C(2025) 7750 final, ajánlás az adatrendelet szerinti minta-szerződési feltételekről és a felhőszolgáltatási szerződések általános szerződési feltételeiről (2025. november 19.)

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A Data Act rövid bemutatása és alkalmazási mérföldkövei

A Data Act az uniós adatstratégia második pillére az adatkormányzási rendelet mellett.³ Célja, hogy az összekapcsolt termékek használata során keletkező adatok értéke ne kizárólag a gyártónál maradjon. A rendelet tárgya az 1. cikk szerint a termékadatok és a kapcsolódószolgáltatás-adatok rendelkezésre bocsátása a felhasználó, az adatátvevők és rendkívüli igény esetén a közsférabeli szervezetek számára, a felhőszolgáltató-váltás megkönnyítése, a nem személyes adatokhoz való jogellenes hozzáférés elleni biztosítékok és az interoperabilitási szabványok. A rendelet a személyes és a nem személyes adatokra egyaránt kiterjed, a személyes adatok védelmére vonatkozó jogot azonban nem írja felül, ütközés esetén a GDPR az irányadó.

Az összekapcsolt termék olyan tárgy, amely a használatára vagy a környezetére vonatkozó adatot gyűjt, és azt hírközlési szolgáltatáson, fizikai kapcsolaton vagy eszközön való hozzáféréseken keresztül közölni képes. A másik két meghatározó fogalom a felhasználó és az adatbirtokos.

12. „felhasználó”: olyan természetes vagy jogi személy, aki vagy amely egy összekapcsolt termék tulajdonosa, vagy akire vagy amelyre szerződésben ideiglenes jogokat ruháztak át az adott összekapcsolt termék használatára vonatkozóan, vagy aki vagy amely kapcsolódó szolgáltatást vesz igénybe;

13. „adatbirtokos”: olyan természetes vagy jogi személy, akinek vagy amelynek – e rendelettel, az alkalmazandó uniós joggal vagy az uniós joggal összhangban elfogadott nemzeti jogszabályokkal összhangban – joga vagy kötelezettsége olyan adatokat – többek között, amennyiben arról szerződésben megállapodtak, termékadatokat vagy kapcsolódószolgáltatás-adatokat – használni és rendelkezésre bocsátani, amelyeket valamely kapcsolódó szolgáltatás nyújtása során visszanyert vagy generált; [Data Act 2. cikk 12. és 13. pont]

A rendelet 2024. január 11-én lépett hatályba, és 2025. szeptember 12-től alkalmazandó, az egyes kötelezettségek azonban lépcsőzetesen élesednek. Az alkalmazás mérföldkövei a következők.

- a) 2025. szeptember 12. óta a felhasználó kérheti az adatokhoz való hozzáférést és azok megosztását, a tisztességtelen szerződési feltételek tilalma az ettől a naptól kötött szerződésekre vonatkozik, és a felhőszolgáltató-váltás szabályai alkalmazandók.
- b) A 2026. szeptember 12. után forgalomba hozott összekapcsolt termékeket és a hozzájuk kapcsolódó szolgáltatásokat már úgy kell megtervezni, hogy az adatok alapértelmezés szerint közvetlenül hozzáférhetőek legyenek a felhasználó számára.
- c) 2027. január 12-től az adatkezelési szolgáltatók szolgáltatóváltási díjat nem számíthatnak fel.

³ Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (adatkormányzási rendelet, DGA), alkalmazandó 2023. szeptember 24-től

- d) 2027. szeptember 12-től a tisztességtelen szerződési feltételek tilalma a korábban kötött, határozatlan idejű vagy legalább 2034. január 11-ig tartó szerződésekre is kiterjed.

A rendelet végrehajtásához tagállami hatóság kijelölése szükséges. Az Energiaügyi Minisztérium 2025 novemberében bocsátotta társadalmi egyeztetésre a végrehajtási törvény tervezetét, amely a Központi Statisztikai Hivatalt jelöli illetékes hatósággént és adatkoordinátorként, a felhőszolgáltató-váltás felügyeletét pedig a Nemzeti Média- és Hírközlési Hatósághoz telepíti.⁴ Az állásfoglalás lezárásakor a törvény kihirdetett szövegét nem sikerült azonosítani, ezért a hatásköröket a Szervezet a mindenkor hatályos magyar jogszabály alapján ellenőrizze. A személyes adatokat érintő rendelkezések felügyelete ettől függetlenül, közvetlenül a rendelet alapján a NAIH feladata.

4.2 A KKV-k adatigénylési lehetőségei

A felhasználó, tehát az összekapcsolt termék tulajdonosa, bérlője vagy lízingbe vevője, a rendelet legfontosabb kedvezményezettje. Ha az adatok a termékből közvetlenül nem érhetők el, kérelemre az adatbirtokos köteles azokat rendelkezésre bocsátani.

(1) Amennyiben a felhasználó nem tud az összekapcsolt termékből vagy a kapcsolódó szolgáltatásból közvetlenül hozzáférni az adatokhoz, az adatbirtokosoknak indokolatlan késedelem nélkül – az adatbirtokos rendelkezésére állóval megegyező minőségben – könnyen elérhető adatokat, valamint az említett adatok értelmezéséhez és felhasználásához szükséges releváns metaadatokat kell hozzáférhetővé tennie a felhasználó számára, könnyen, biztonságosan, díjmentesen, egy átfogó, strukturált, széles körben használt és géppel olvasható formátumban, és – amennyiben releváns és technikailag kivitelezhető – folyamatosan és valós időben. Ezt egyszerű kérelem alapján, elektronikus úton kell megtenni, amennyiben technikailag kivitelezhető. [Data Act 4. cikk (1) bekezdés]

A felhasználó a kapott adatot bármely jogszerű célra használhatja, például prediktív karbantartásra vagy független szerviz igénybevétele. A rendelet ugyanezt a jogot a harmadik fél javára is biztosítja, a felhasználó kérelmére az adatbirtokos köteles az adatokat a felhasználó által megjelölt harmadik fél rendelkezésére bocsátani, a felhasználó számára díjmentesen. A harmadik féltől az adatbirtokos észszerű kompenzációt kérhet, de ha az adatátvevő KKV, a kompenzáció nem haladhatja meg az adatok rendelkezésre bocsátásának költségeit.

Az igénylési jognak korlátai is vannak. A kapott adat nem használható fel a forrástermékkel versengő összekapcsolt termék fejlesztésére, és nem szolgálhat a gyártó gazdasági helyzetének, eszközeinek és termelési módszereinek megismerésére. A kapuőrnek minősített nagy platformok nem lehetnek jogosult harmadik felek, a Szervezet tehát a kapott adatot nem adhatja át nekik, felhőinfrastruktúrájukat azonban igénybe veheti. A felhasználó nem élhet kényszerítő

⁴ Energiaügyi Minisztérium, törvényjavaslat az adatrendelet végrehajtásáról, társadalmi egyeztetés 2025. november 5. és 10. között, a tervezet 2. § (1) és (2) bekezdése, valamint 3. §-a (kormany.hu)

eszközökkel, és nem használhatja ki az adatbirtokos adatvédelmi célból kialakított technikai infrastruktúrájának hiányosságait.

A KKV-kat a rendelet a szerződéses egyensúlytalansággal szemben is védi. Az egyoldalúan megállapított, tisztességtelen adathozzáférési feltétel nem köti a másik vállalkozást, a tisztességtelenség védelme pedig kiterjed többek között arra a feltételre, amely megakadályozza, hogy a fél az általa generált adatokat felhasználja vagy azokról másolatot kapjon. A közsférabeli szervezetek nem szükséghelyzeti adatigénylése alól a mikro- és kisvállalkozások mentesülnek.

4.3 A KKV-k lehetséges adatszolgáltatási kötelezettségei

A KKV négy úton válhat kötelezetté. Először, ha összekapcsolt terméket gyárt vagy kapcsolódó szolgáltatást nyújt, adatbirtokosként köteles az adatokat a felhasználó és a harmadik fél rendelkezésére bocsátani. Másodszor, ha a felhasználóként kapott adatot továbbadja, a (34) preambulumbekkezdés szerint maga is adatbirtokossá válhat.⁵ Harmadszor, harmadik félként az 5. cikk alapján kapott adatokra a 6. cikk kötelezettségei vonatkoznak rá. Negyedszer, jogi személyiséggel rendelkező adatbirtokosként a közsférabeli szervezetek rendkívüli igény alapján benyújtott kérelmeit is teljesítenie kell.

A mikro- és kisvállalkozások gyártói mentessége szűkebb, mint amit a köznyelv sugall.

(1) Az e fejezetben foglalt kötelezettségek nem alkalmazandók a mikrovállalkozások vagy a kisvállalkozások által előállított vagy tervezett összekapcsolt termékek vagy az általuk nyújtott kapcsolódó szolgáltatások használata révén generált adatokra, feltéve, hogy az említett vállalkozások nem rendelkeznek a 2003/361/EK ajánlás mellékletének 3. cikke értelmében vett olyan partnervállalkozásokkal vagy kapcsolt vállalkozásokkal, amelyek nem minősülnek mikrovállalkozásnak vagy kisvállalkozásnak, továbbá amennyiben a mikrovállalkozás vagy kisvállalkozás nem kapott alvállalkozói megbízást valamely összekapcsolt termék előállítására vagy tervezésére, vagy valamely kapcsolódó szolgáltatás nyújtására vonatkozóan. [Data Act 7. cikk (1) bekezdés]

A mentesség tehát nem illeti meg azt a kisvállalkozást, amely nagyvállalati csoport tagja, vagy amely alvállalkozóként gyárt egy nagyobb vállalkozás számára. A középvállalkozás csak egy évig mentesül. A (41) preambulumbekkezdés szerint a mentesség a gyártói minőségre vonatkozik, más minőségben a mikro- és kisvállalkozást is terhelhetik adatbirtokosi kötelezettségek. A felhasználói jogokat kizáró vagy korlátozó szerződési feltétel nem köti a felhasználót.

A harmadik fél kötelezettségei az adatot fogadó KKV-t is terhelik. A kapott adatot csak a felhasználóval megállapodott célra kezelheti, és törli, ha a célhoz már nem szükséges. Nem használhatja fel az adatot a termék vagy a kapcsolódó szolgáltatás biztonságára hátrányos módon, és nem hagyhatja figyelmen kívül az üzleti titok védelmére az adatbirtokossal megállapodott intézkedéseket.

⁵ Európai Bizottság, Frequently Asked Questions on the Data Act ([digital-strategy.ec.europa.eu](https://digital-strategy.ec.europa.eu/en/frequently-asked-questions/data-act)), az adatbirtokos fogalmáról szóló válaszok

4.4 A Data Act adatszolgáltatásból adódó kiberbiztonsági kockázatok

A rendelet a (42) preambulumbekkezdésben maga is elismeri, hogy az összekapcsolt termékek különböző szintű adat- és kiberbiztonsági kockázatot jelentenek. A kockázatokat az adatáramlás szereplői szerint érdemes megszerezni.

4.4.1 A kötelező hozzáférési felület mint támadási felület

A 3. cikk (1) bekezdése szerint az adatoknak könnyen, biztonságosan és díjmentesen hozzáférhetőnek kell lenniük, a 4. cikk (1) bekezdése szerint pedig elektronikus úton, adott esetben folyamatosan és valós időben. Ez a gyakorlatban folyamatosan elérhető programozási felületet vagy adatportált jelent, amely a gyártó hálózatának eddig zárt részét nyitja meg, és a programozási felületek jellemző sérülékenységeit hordozza, például a hibás jogosultságkezelést vagy a hozzáférési kulcsok kiszivárgását. A rendelet nem határoz meg biztonsági szabványt, a „biztonságosan” fordulat tartalmát a NIS2 és a digitális elemeket tartalmazó termékekre vonatkozó CRA követelményei töltik ki.⁶

A kérelmező azonosítása külön kockázat. A rendelet a (29) preambulumbekkezdésben megengedi a megfelelő felhasználóazonosítást, a 4. cikk (5) bekezdése azonban korlátozza, milyen információ kérhető és őrizhető meg.

(5) Annak ellenőrzése céljából, hogy egy természetes vagy jogi személy az (1) bekezdés alkalmazásában felhasználónak minősül-e, az adatbirtokos nem követelheti meg az említett személytől, hogy a szükséges meghaladó információkat adjon meg. Az adatbirtokosok nem őrizhetnek meg semmilyen, a felhasználónak a kért adatokhoz való hozzáférésére vonatkozó, azt meghaladó információt – különösen naplódokumentumokat –, amely a felhasználó hozzáférési kérelmének megfelelő teljesítéséhez, valamint az adatinfrastruktúra biztonságához és fenntartásához szükséges. [Data Act 4. cikk (5) bekezdés]

A biztonsági célú naplózás tehát megengedett, de a célját és a megőrzési idejét dokumentálni kell. A visszaélés tipikus formája a jogosult felhasználó vagy meghatalmazott harmadik fél nevében benyújtott hamis kérelem, amellyel a támadó gépadatot, helyadatot vagy üzemi paramétereket szerez. A kényszerítő eszközök és az infrastruktúra hiányosságainak kihasználását a rendelet a harmadik fél számára is tiltja.

4.4.2 Az üzleti titok és a termékbiztonság kiszivárgása

Az adatbirtokos a kérelmet nem tagadhatja meg pusztán azért, mert az adat üzleti titok, az adatok kiadását azonban technikai és szervezési intézkedésekhez kötheti. Az üzleti titokként védett adatokat a metaadatokban is azonosítani kell, és meg kell állapodnia a felhasználóval az arányos védelmi intézkedésekről, például titoktartási megállapodásról, szigorú hozzáférési protokollról vagy technikai szabványok alkalmazásáról. Ha a megállapodás nem jön létre, vagy a felhasználó a vállalt intézkedéseket nem hajtja végre, az adatbirtokos az üzleti titokként azonosított adatok

⁶ Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (kiberrezilienciáról szóló rendelet, CRA), a gyártók jelentéstételi kötelezettségei 2026. szeptember 11-től, a termékkövetelmények 2027. december 11-től alkalmazandók

megosztását írásban indokolt döntéssel visszatárhathatja vagy felfüggesztheti, és az illetékes hatóságot értesíti. Rendkívüli körülmények között, ha a felfedés nagy valószínűséggel súlyos gazdasági kárt okozna, a kérelem eseti alapon, objektív elemekkel alátámasztva elutasítható. A (31) preambulumbekkezdés szerint ilyenkor a kiberbiztonságra gyakorolt negatív hatás is figyelembe vehető, a KKV-gyártó tehát akkor hivatkozhat eredményesen kiberbiztonsági kockázatra, ha azt a kockázatelemzésében előre, konkrét adatkörre dokumentálta.

A termékbiztonság önálló korlát. A felek szerződésben korlátozhatják az adathozzáférést, ha az alááshatná a termékre vonatkozó jogszabályi biztonsági követelményeket, és ez súlyosan hátrányos hatással járhat a természetes személyek egészségére vagy biztonságára, a megtagadásról pedig az illetékes hatóságot értesíteni kell. Ipari vezérlőrendszereknél ez különösen fontos, mert a kiadott telemetria a vezérlési logika visszafejtését is lehetővé teheti.

4.4.3 A meghosszabbodó ellátási lánc

Az adatot fogadó KKV a gyártó ellátási láncának új tagjává válik, a KKV által bevont harmadik felek pedig a KKV láncának tagjai. A rendelet a harmadik félnek tiltja a kapott adatok továbbadását a felhasználóval kötött szerződés hiányában, a kapuőrnek való átadást pedig feltétel nélkül. A kockázat abban áll, hogy a harmadik fél gyengébb védelmi szintje a lánc leggyengébb pontjává válik. Ha a harmadik fél a kapott adatot jogosulatlanul használja, az adatbirtokos követelheti az adatok törlését, a jogsértő termékek megsemmisítését és kártérítést, és ugyanezt követelheti a felhasználótól is, ha az az adatbirtokos technikai védelmi intézkedéseit módosítja vagy eltávolítja. Az adatbirtokos ilyen intézkedésként titkosítást és intelligens szerződést is alkalmazhat, ezeket a felhasználó és a harmadik fél megállapodás nélkül nem módosíthatja.

4.4.4 A közsférabeli adatigénylés és a felhő

A szükséghelyzet fogalma a jelentős kiberbiztonsági eseményt is magában foglalja, az ilyen adatigénylés pedig rövid határidőt szab, ezért társadalmi mérnökségre alkalmas. A kérelemnek írásban kell érkeznie, meg kell jelölnie a rendkívüli igény fennállását, a célt, a törlés várható idejét és a feladatot előíró jogi rendelkezést, a közsférabeli szervezet kérelmét pedig az adatkoordinátor online elérhetővé teszi. Ezek alapján ellenőrizhető a kérelem valódisága az adat kiadása előtt. Az elutasításra vagy a módosítás kérésére szükséghelyzetben öt, egyéb rendkívüli igény esetén harminc munkanap áll rendelkezésre.

A felhőben tárolt nem személyes adatok tekintetében az adatkezelési szolgáltatóknak meg kell akadályozniuk az uniós joggal ütköző harmadik országbeli kormányzati hozzáférést, és a kérelem teljesítése előtt tájékoztatniuk kell az ügyfelet. A felhőszerződésekben ezért a Data Act és a NIS2 közreműködői követelményeit együtt kell érvényesíteni.

4.5 A Data Act adatszolgáltatásból adódó adatvédelmi kockázatok

A rendelet a személyes adatokra is kiterjed, de nem teremt önálló jogalapot. A (34) preambulumbekkezdés szerint ha a felhasználó vállalkozás, a termék használata során generált személyes adatok tekintetében adatkezelőnek minősül, és a GDPR 6. cikke szerinti jogalappal

kell rendelkeznie.⁷ A gépkezelő, a sofőr vagy az ügyfél adatai így a Szervezet adatkezelésévé válnak, amint az adatot kikéri.

*(12) Ha a felhasználó nem az az érintett, akinek a személyes adatait kéri, az összekapcsolt termék vagy a kapcsolódó szolgáltatás használata által generált személyes adatokat az adatbirtokos csak akkor bocsáthatja a felhasználó rendelkezésére, amennyiben az (EU) 2016/679 rendelet 6. cikke szerint érvényes adatkezelési jogalap áll fenn, valamint amennyiben – adott esetben – teljesülnek az említett rendelet 9. cikkében és a 2002/58/EK irányelv 5. cikkének (3) bekezdésében foglalt feltételek.
[Data Act 4. cikk (12) bekezdés]*

Az adatbirtokos oldalán ugyanez a kötelezettség áll fenn a harmadik félnek történő átadásnál. A gyakorlatban három kockázat jellemző. Az első a vegyes adatállomány, amelyben a személyes és a nem személyes adatok elválaszthatatlanul összekapcsolódnak, ilyenkor a (34) preambulumbekkezdés szerint a teljes állományra a GDPR vonatkozik. A második a jogalap hiánya, mert a hozzájárulás a munkaviszonyban nem mindig állja meg a helyét, a jogos érdek pedig dokumentált érdekmérlegelést kíván. A harmadik a szerepek tisztázatlansága, mert az adatbirtokos és a felhasználó közös adatkezelőnek minősülhet, ekkor a GDPR 26. cikke szerinti megállapodás szükséges.

A harmadik fél a kapott adatot profilalkotásra csak akkor használhatja, ha az a felhasználó által kért szolgáltatás nyújtásához szükséges. A közsférabeli adatigénylésnél a személyes adatokat az adatbirtokosnak anonimíznia kell, és csak ha a kérelem teljesítéséhez személyes adat közlése szükséges, álnevesítheti azokat. Az adattakarékosság elve a Data Act saját szabályaként is megjelenik, a (38) preambulumbekkezdés szerint a harmadik fél csak a kért szolgáltatás nyújtásához szükséges információhoz férhet hozzá, a kikért adatkörre pedig a GDPR célhoz kötöttségi és adattakarékossági elve közvetlenül alkalmazandó.

A rendelet II., III. és V. fejezetének megsértése esetén a GDPR szerinti felügyeleti hatóság, Magyarországon a NAIH, a GDPR 83. cikk (5) bekezdése szerinti összeghatárig, legfeljebb 20 millió euróig vagy a világpiaci éves forgalom 4 százalékáig bírságozhat. Adatvédelmi hatásvizsgálat akkor szükséges, ha az adatmegosztás az érintettek valószínűsíthetően magas kockázattal jár, például munkavállalók rendszeres megfigyelését vagy helymeghatározását teszi lehetővé.

4.6 A releváns NIS2 kontrollok

A Kiberbiztonsági tv. a hatálya alá tartozó szervezet vezetőjének kötelezettségévé teszi a kockázatmenedzsment keretrendszer működtetését és a kockázatokkal arányos védelmi intézkedések meghatározását, a közreműködők szerződéses kötelezését a kiberbiztonsági követelmények betartására, valamint a rendszer eseményeinek nyomon követhetőségét. A védelmi intézkedéseket a 7/2024. (VI. 24.) MK rendelet 2. melléklete tartalmazza, az alábbi pontok erre a mellékletre hivatkoznak, és a releváns intézkedéseket a fenti kockázatokhoz

⁷ EDPB-EDPS 2/2022. számú közös vélemény az adatrendelet javaslatáról (2022. május 4.), a vegyes adatállományokról és a jogalapról szóló pontok

rendezik. A szögletes zárójel azt a biztonsági osztályt jelöli, amelyben az intézkedés kötelező (Alap, Jelentős, Magas).

4.6.1 Kockázatelemzés és adatleltár

- a) 15.4. [A, J, M] a rendszerszintű kockázatelemzés, amely a hozzáférési felületre és a kiadott adatkörökre is kiterjed, ideértve 15.4.1.3. [A, J, M] a személyes adatok kezeléséből eredő hatások vizsgálatát
- b) 15.5. [A, J, M] a kockázatelemzés rendszeres frissítése, különösen új adatátvevő vagy harmadik fél belépésekor, és 15.9. [A, J, M] a sérülékenységek rendszeres ellenőrzése a hozzáférési felületen
- c) 6.36. [A, J, M] a rendszerelem-leltár, amelyben a hozzáférési felület és az adatmegosztásban részt vevő komponensek szerepelnek, valamint 6.15. [A, J, M] a biztonsági hatásvizsgálat az adatkiadási felületet érintő változtatások előtt

4.6.2 Szerződéses és ellátási lánc kontrollok

- a) 16.7. [A, J, M] a szerződésekben rögzített biztonsági követelmények, ezen belül 16.7.4. [A, J, M] az érintett rendszer biztonsági osztálya és védelmi intézkedései, valamint 16.7.8. [A, J, M] a felelősség megosztása
- b) 16.49. [A, J, M] a külső rendszerszolgáltatások megfelelőségének ellenőrzése, amely a harmadik félre és a felhőszolgáltatóra egyaránt vonatkozik
- c) 19.2. [A, J, M] az ellátási lánc kockázatkezelése a beszerzéstől a kivezetésig, 19.7. [A, J, M] a követelmények érvényesítése az alvállalkozókra, 19.13. [A, J, M] a beszerzési és szerződéses eszközök hozzáigazítása, 19.16. [J, M] a beszállítók rendszeres felülvizsgálata és 19.19. [A, J, M] a közreműködők biztonsági kötelezése
- d) 5.7. [A, J, M] az információcsere-megállapodások jóváhagyása, amely a Data Act szerinti adatmegosztási megállapodásokra közvetlenül alkalmazható

4.6.3 Hozzáférés, hitelesítés és határvédelem

- a) 2.2. [A, J, M] a felhasználói jogosultságok rendszeres felülvizsgálata és 2.2.5. [A, J, M] a külsős felhasználók hozzáféréseinek jóváhagyása, valamint 14.11. [A, J, M] a külső személyek hozzáféréseire vonatkozó szabályok
- b) 17.17. [A, J, M] a hálózati szegmentáció, amellyel a hozzáférési felület az üzemi és a vezérlő hálózattól elválasztható, és 17.20. [J, M] az alapértelmezett tiltás elve a hálózati forgalomra
- c) 6.26.2. [A, J, M] a tiltott portok, protokollok és szolgáltatások meghatározása, valamint 16.13. [J, M] a használt portok és protokollok dokumentálása
- d) 10.11. [A, J, M] a távoli karbantartás engedélyezése és naplózása, ha a gyártó távolról fér hozzá a termékhez, és 11.14.1. [A, J, M] a külső adathordozók használatának korlátozása

4.6.4 Naplózás, monitorozás és sértetlenség

- a) 4.2. [A, J, M] a naplózandó események meghatározása, 4.3. [A, J, M] a naplóbejegyzés kötelező tartalma és 4.13. [A, J, M] a naplók rendszeres elemzése, amelyek az adatkiadási kérelmek nyomon követhetőségét biztosítják

- b) 18.13. [A, J, M] a rendszer figyelése, 18.37. [A, J, M] a biztonsági riasztások kezelése és 5.15. [A, J, M] a folyamatos felügyelet
- c) 18.8.1. [A, J, M] a kártékony kód elleni védelem a belépési és kilépési pontokon, 18.42. [J, M] a sértetlenség-ellenőrzés és 18.59. [J, M] a bemeneti adatok ellenőrzése a fogadott adatállományok feldolgozásánál
- d) 18.2. [A, J, M] a hibajavítás és 18.2.3. [A, J, M] a biztonsági frissítések meghatározott időn belüli telepítése a hozzáférési felületet kiszolgáló rendszerelemeken

4.6.5 Eseménykezelés és üzletmenet-folytonosság

- a) 9.9. [A, J, M] a biztonsági események kivizsgálása, ideértve a jogosulatlan adatkiadást és a visszaélés gyanús kérelmet, valamint 9.25. [A, J, M] az események éves értékelése
- b) 7.35. [A, J, M] a mentések és 7.43. [A, J, M] a visszaállítás tesztelése, amelyek a kiadott adatok forrásának megőrzését szolgálják
- c) A Kiberbiztonsági tv. 66. § (2) bekezdése szerinti incidensbejelentés a 418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdésében meghatározott határidővel, ha az adatkiadási felület kompromittálódása jelentős incidenst okoz.⁸

A felsorolt kontrollok többsége már az Alap biztonsági osztályban kötelező, a Data Act-megfelelés ezért a NIS2-kötelezett KKV számára a meglévő intézkedések hatókörének kiterjesztése az adatmegosztási folyamatra. Ahol a Szervezet a kiadott vagy fogadott adatok között üzleti titkot vagy nagy mennyiségű személyes adatot azonosít, a biztonsági osztályba sorolást felül kell vizsgálni, mert a 7/2024. (VI. 24.) MK rendelet 1. melléklete a nagy mennyiségű személyes adat sérülését a Jelentős, a nagy értékű üzleti titkot kezelő rendszer sérülését a Magas osztály szempontjai között nevesíti.⁹ A NIS2-kötelezettség hiányában is érdemes ezt a keretrendszert követni, mert a Data Act üzleti titokra vonatkozó szabályai és a GDPR biztonsági követelményei ugyanezeket az intézkedéseket várják el.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (Data Act, adatrendelet); az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR); az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS2); az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (CRA); az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (DMA); az Európai Parlament és a Tanács (EU) 2022/868 rendelete (DGA)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról; 418/2024. (XII. 23.) Korm. rendelet; 7/2024. (VI. 24.) MK rendelet; az Energiaügyi Minisztérium törvényjavaslata az adatrendelet végrehajtásáról (társadalmi egyeztetés, 2025. november)

⁸ 418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1., 3. és 5. pont, a korai figyelmeztetés 24 órán, a bejelentés 72 órán belül, a zárójelentés egy hónapon belül esedékes

⁹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 2.2.3.1. és 2.2.4.5. pont, a Jelentős osztályhoz a nagy mennyiségű személyes adat, a Magas osztályhoz a nagy értékű üzleti titkot kezelő rendszer sérülése tartozik

- Európai Bizottság, C(2025) 7750 final ajánlás a minta-szerződési feltételekről és az általános szerződési feltételekről (2025. november 19.); Európai Bizottság, Frequently Asked Questions on the Data Act; EDPB-EDPS 2/2022. számú közös vélemény
- VFP2 KiberVéd jogi állásfoglalások a naplózásról, a nem támogatott operációs rendszerekről, az IBIR szerepköreiről, az MI-komponenst tartalmazó célszoftvekről és a szerverbeszerzésről (nis2.mkik.hu)