A KÖZREMŰKÖDŐVEL KÖTÖTT SZERZŐDÉS TARTALMA

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/10

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.26	Kálmán és Társai Ügyvédi Iroda.	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1 VEZETŐI ÖSSZEFOGLALÓ

Jelen iránymutatás célja annak bemutatása, hogy az érintett szervezetnek közreműködő (szofverfejlesztők, SaaS, IaaS, PaaS szolgáltatók, külsős üzemeltetetők) igénybevétele esetén milyen tartalmi elemeket kell és célszerű a szerződésbe belefoglalni.

Alapvető elvárás, hogy amennyiben az érintett szervezetek közreműködőt vesznek igénybe, akkor a közreműködővel szemben kifejezetten érvényesítsék az ellátási lánc biztonsági követelményeit. Ezeknek a biztonsági követelményeknek szerződéses kötelemként kell teljesülniük.

Általánosan elmondható, hogy a szerződésnek minden egyes esetben kockázatarányosnak, ellenőrizhetőnek, valamint kikényszeríthetőnek kell lennie az ellátási lánc biztonságának biztosítása érdekében.

A Kiberbiztonsági tv. és a 7/2024 (VI.24) MK rendelet meghatároz egyes szerződésbe foglalandó követelményeket. Azonban minden egyes szerződés tartalma egyedileg mérlegelendő a szervezetek és a közreműködőik közötti kapcsolatok biztonságával kapcsolatos szempontok alapján. Ebből kifolyólag nincs egy olyan egységes követelménylista, amely minden egyes szerződésre alkalmazható lenne. Vannak kötelezően beépítendő és ajánlott szerződéses követelmények, melyeket minden egyes esetben a hatályos jogszabályok előírásai és az alkalmazott kockázatelemzés figyelembevétele alapján kell a szerződésben rögzíteni.

2 A VIZSGÁLANDÓ KÉRDÉS

A modern informatikai architektúrák decentralizált, hibrid és felhőalapú természete okán az egyik fő támadási vektorrá az elmúlt időszakban a beszállítói lánc és a bizalmi ökoszisztéma vált. A támadók felismerték, hogy az információbiztonsági tudatossággal és felkészültséggel rendelkező szervezetek közvetlen kompromittálása helyett nagyobb sikerességi rátával kecsegtet a gyengébb, fragmentált védelmi szinttel rendelkező harmadik felek, alvállalkozók és szoftverbeszállítók infrastruktúrájának feltörése.

Ezért fektet kiemelt hangsúlyt a Magyarország kiberbiztonságáról szóló 2024. évi LXIX törvény (Kiberbiztonsági tv.) és a 7/2024 (VI.24) MK rendelet a beszállítói lánc védelmére.

Jelen dokumentum azt vizsgálja, hogy a fenti jogszabályok alapján mit kell tartalmaznia egy NIS2 kötelezett szervezet és a közreműködő partnere között létrejött szerződésnek.

3 FOGALMI BEHATÁROLÁS

A közreműködő fogalma a Magyarország kiberbiztonságáról szóló 2024. évi LXIX törvényből (Kiberbiztonsági tv.) vezethető le. A törvény szerint:

> *„ … 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;" [Kiberbiztonsági tv. 6. § (5) bekezdés d pont]

A Kiberbiztonsági tv. fent idézett szakasza rendkívül tágan határozza meg azon tevékenységek körét, amelyek megalapozzák a közreműködői státuszt. Nem csupán az informatikai infrastruktúrát fizikailag építő vagy karbantartó cégek tartoznak ide, hanem minden olyan entitás, amely az elektronikus információs rendszer logikai, fizikai vagy adatkezelési rétegeihez kapcsolódik.

- A gyakorlatban közreműködőnek minősül:
- A felhőszolgáltató (IaaS, PaaS, SaaS), amely infrastruktúrát vagy szoftvert biztosít a szervezet számára, beleértve a globális szereplőket is.
- A menedzselt informatikai szolgáltató (Managed Service Provider - MSP), amely a szervezet belső hálózatának, végpontjainak vagy szervereinek távoli üzemeltetését végzi.
- Az egyedi szoftvert fejlesztő vállalat, amely az EIR alapját képező vagy abba integrálódó alkalmazást készíti.
- A kiberbiztonsági szolgáltatásokat nyújtó cég (Managed Security Service Provider - MSSP), beleértve a biztonsági műveleti központot (SOC) üzemeltető partnereket.
- Olyan, látszólag nem informatikai profilú szolgáltató is (például bérszámfejtő iroda, marketingügynökség, HR tanácsadó), amely az EIR-rel kapcsolatos adatkezelési vagy adatfeldolgozási tevékenységet lát el.

4 SZERZŐDÉSES KÖVETELMÉNYEK

4.1 Bevezetés

Ha egy szervezet közreműködőt vesz igénybe, elengedhetetlen az ellátási lánc biztonságos kezelése. Az ellátási láncokon keresztül érkező kockázatok azért jelentenek kritikus fenyegetést, mert a támadók gyakran a megrendelő és a közreműködő közötti bizalmi kapcsolatot (például VPN összeköttetések, megosztott hitelesítő adatok, automatizált szoftverfrissítési csatornák) használják fel a behatolásra. Egy rosszul konfigurált beszállítói hozzáférés vagy egy nem megfelelően auditált szoftverkód olyan kaput nyit a szervezet rendszerébe, amelyet a belső védelmi intézkedések nem képesek maradéktalanul megvédeni.

A szervezeteknek fel tehát mérniük és figyelembe kell venniük az általuk igénybe vett közreműködők termékeinek, szolgáltatásainak, az azokba beépített kiberbiztonsági kockázatkezelési intézkedéseknek, valamint kiberbiztonsági gyakorlatainak általános minőségét és rezilienciáját, beleértve a biztonságos fejlesztési eljárásaikat is. Célszerű és részben kötelező, hogy a szervezetek a kiberbiztonsági kockázatkezelési intézkedéseket beépítsék az általuk igénybe vett közreműködőkkel kötött szerződéses megállapodásokba.1

A közreműködővel kötött szerződés speciális tartalmi elemei az alábbi témakörökre oszthatók:

i. A Kiberbiztonsági tv. által előírt általános kiberbiztonsági követelmények meghatározása
   A feleknek meg kell határozniuk a szerződés tárgyát képező EIR-t, annak biztonsági osztályát és a vonatkozó kiberbiztonsági követelményeket, különös tekintettel a

[1] NIS2 irányelv preambulum (85) bekezdés

Kiberbiztonsági tv. 6. § -ában vagy 7/ 2024 (VI.24) MK rendelet 2. számú mellékletében foglalt követelményekre. Konkrétan nevesíteni érdemes a vonatkozó követelményeket és kifejteni, hogy a közreműködő hogyan teljesíti azokat. (Ide nem értve szoftverfejlesztés esetén rendszer funkcionalitásával kapcsolatos biztonsági jellegű követelményeket, azokat a rendszerbiztonsági tervben kell kifejteni.)

ii. Szoftverfejlesztéssel kapcsolatos biztonsági követelmények
A fejlesztésre vonatkozó követelmények a 7/2024 (VI.24) MK rendelet védelmi intézkedéseiből vezethetők le, különösen a fejlesztési életciklus, változáskezelés és tesztelés körében.

iii. Szoftverfejlesztéssel kapcsolatos dokumentációs követelmények
A szerződésben a közreműködőnek vállalnia kell a biztonsággal kapcsolatos dokumentumok elkészítését és be kell tartania az ezen dokumentumok védelmére vonatkozó követelményeket.

iv. Humán kockázati követelmények
A rendelet szerint a szerződésnek tartalmaznia kell a teljesítés során a közreműködőnél foglalkoztatott, az EIR-hez hozzáférő személyek kötelezettségeit és az esetleges egyéb, humán kockázattal kapcsolatos kötelezettségeket, ilyen például az egyedi jogosultságkezelés, információbiztonsági képzés.

v. További közreműködők foglalkoztatásával kapcsolatos követelmények
A közreműködőnek vállalnia kell, hogy a vállalt biztonsági követelményeket tovább érvényesíti az által foglalkoztatott alvállalkozókkal kötött szerződéseiben.

vi. Üzemeltetéssel és szoftvertámogatással kapcsolatos követelmények
Az ilyen szerződésekben tehát rögzíteni kell azt, hogy távoli karbantartás azonos biztonsági szinten történjen. Ezen kívül célszerű rögzíteni a hibajavítással együtt kötelezettségeket is (pl. szolgáltatási szintek, hibajavítás menete és határideje, kötbér, további fejlesztési igényekhez kapcsolódó költségek), valamint a jogszabálykövetéssel és verziófrissítéssel kapcsolatosan felmerülő kérdéseket.

vii. Egyéb követelmények
Célszerű kikötni olyan követelményeket, amelyek segítik a felek együttműködését a kiberbiztonság egyéb területein. Ilyen például az együttműködés az audit során, az incidenskezelés kérdései, a megrendelő auditálási joga, a közreműködő általi rendszeres adatszolgáltatás az éves beszállítói kockázatértékeléshez.

A követelmények egy részének szerződésbe foglalása jogszabályban foglalt kötelezettség. Vannak továbbá olyan követelmények, amelyek szerződésbe foglalása audit- és felelősségi szempontból ajánlott. A közreműködőkkel kötött szerződésbe építendő konkrét követelményeket a Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet tartalmazza.

4.2 Általános követelmények

A 7/2024. (VI. 24.) MK rendelet az alábbiakat rögzíti:

> *16.7.[A], A Szervezet a beszerzési folyamat során - beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is - a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:*
> *16.7.1. A funkcionális biztonsági követelményeket.*
> *16.7.2. A mechanizmusok erősségére vonatkozó követelményeket.*
> *16.7.3. A biztonság garanciális követelményeit.*

16.7.4. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket. (...)
16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.
16.7.9. A teljesítési kritériumokat. [7/2024 MK rendelet 2. melléklet]

A fentiek alapján, a közreműködő köteles vállalni a vonatkozó jogszabályi előírásoknak a maradéktalan betartását, és fejlesztés esetén szavatolni, hogy az általa fejlesztett elektronikus információs rendszer megfelel a jogszabályok által támasztott követelményeknek. A szervezet köteles az elektronikus információs rendszert megfelelő biztonság osztályba sorolni, ezért a közreműködőnek vállalnia kell az erre vonatkozó konkrét biztonsági követelmények teljesítését is. Ezeket a kötelezettségvállalásokat a szerződésben is rögzíteni szükséges.
A szerződésnek tartalmaznia kell azt is, hogy a teljesítés során a közreműködő mely szervezeti szabályzatok és egyéb dokumentumok megismerésére és betartására kötelezett. Ilyenek lehetnek például (a teljesség igénye nélkül):

- Szoftverfejlesztési szabályzat,
- Felhasználói szabályzat,
- Információbiztonsági követelmények,
- Személyi biztonsági követelmények.

Jó gyakorlat, ha a szervezet készít egy kivonatot az általa alkalmazott információbiztonsági szabályozásból, amely a közreműködők által betartandó kötelezettségeket és az egyéb tudnivalókat rögzíti.

19.16.[J], A Szervezet meghatározott gyakorisággal értékeli és felülvizsgálja a beszállítókkal vagy szerződéses partnerekkel, illetve az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat. [7/2024 MK rendelet 2. melléklet]

A Jelentős (J) biztonsági osztálytól kezdődően a szerződésben meg kell határozni a rendszeres (évente történő) felülvizsgálati procedúrát. A közreműködőnek évente be kell számolnia a saját kiberbiztonsági helyzetéről, az általa bevont további alvállalkozókról és az esetlegesen elszenvedett, de a megrendelőt közvetlenül még nem érintő biztonsági incidensekről is.

4.3 Szoftverfejlesztéssel kapcsolatos követelmények

A fejlesztésre (szoftverfejlesztés, rendszerfejlesztés, módosítás, integráció) vonatkozó követelményeket a 7/2024 MK rendelet védelmi intézkedéseiből vezethetők le, különösen a fejlesztési életciklus, változáskezelés és tesztelés körében.

16.9.[J], A Szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője biztosítson tervezési és megvalósítási információkat a védelmi intézkedésekhez. Ezek az információk tartalmazzák a biztonsági szempontból releváns külső rendszerinterfészeket, a magas szintű rendszertervet, az alacsony szintű rendszertervet, a forráskódot vagy a hardversémákat, valamint a szervezet által meghatározott részletes tervezési és megvalósítási információkat.

Ez a követelmény Jelentős (J) biztonsági osztálytól kötelező. A szoftverfejlesztési szerződésekben sok esetben a közreműködő saját szellemi tulajdonának tekinti a forráskódot. Ennek a feszültségnek a feloldására a szerződésben forráskód letéti megállapodást javasolt alkalmazni, vagy szerződéses garanciát kell kérni arra, hogy a megrendelő által megbízott harmadik fél (például egy auditor) biztonsági célból elvégezhesse a kód vizsgálatát anélkül, hogy a közreműködő szellemi alkotáshoz való jogai sérülnének.

16.11.[M], A Szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:
16.11.1.[M], Az EIR, rendszerelem vagy szolgáltatás szállítása a meghatározott biztonsági konfigurációk alkalmazásával történjen.
16.11.2.[M], Minden EIR, rendszerelem vagy szolgáltatás későbbi újratelepítése vagy frissítése során az alapkonfigurációkat használják.

A Magas (M) biztonsági osztályú rendszereknél az alapértelmezett biztonság elve kötelező. A szerződésnek rögzítenie kell, hogy a közreműködő a rendszert keményítési (hardening) eljárásnak veti alá az átadás előtt. Tilos olyan szoftvert átadni, amely megváltoztathatatlan gyári jelszavakat tartalmaz, vagy olyan szolgáltatásokat futtat (pl. Telnet, FTP), amelyek nem biztonságosak.

16.13.[J], A Szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy határozza meg a használatra tervezett funkciókat, portokat, protokollokat és szolgáltatásokat.

A Jelentős (J) biztonsági osztálytól kezdve tilos az informatikai hálózatokban az "any-to-any" (minden forgalmat engedélyező) tűzfalszabályok alkalmazása.

16.16.[A], A Szervezet az általa meghatározott biztonságtervezési elveket alkalmazza és megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és az EIR, valamint a rendszerelemek módosítása során.

Az Alap (A) szinttől kezdődően a "Security by Design" (tervezésbe épített biztonság) koncepció érvényesítése elvárt. A közreműködői szerződésben hivatkozni kell a szervezet belső információbiztonsági szabályzatára (IBSZ), és kötelezni kell a fejlesztőt, hogy a szoftverfejlesztési életciklus minden fázisában (a specifikációtól a tesztelésig) alkalmazza a védelmi kontrollokat

16.49.2.[A], Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban.
16.49.3.[A], külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek.

Amikor a szervezet egy SaaS (Software as a Service) megoldást vásárol, az adatok a közreműködő infrastruktúrájába kerülnek. Ezen Alap (A) szintű követelmény alapján a szerződésnek biztosítania kell a megrendelő jogát a külső rendszer ellenőrzésére. Ha a helyszíni audit (On-site Audit) nem lehetséges (például multinacionális felhőszolgáltatók esetében), a szerződésben ki kell kötni a független harmadik fél által kiállított megfelelőségi jelentések (például SOC 2 Type II, ISO/IEC 27001) meglétét.

16.76.1.[J], A Szervezet:
16.76.2.[J], Megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen.
16.76.2.1.[J], Kiemelten kezelje a biztonsági követelményeket.
16.76.2.2.[J], Határozza meg a fejlesztés során alkalmazott szabványokat és eszközöket.
16.76.2.3.[J], Dokumentálja a fejlesztés során alkalmazott speciális eszköz konfigurációkat és opciókat.
16.76.2.4.[J], Tartsa nyilván a változtatásokat, és biztosítsa ezek jogosulatlan változtatás elleni védelmét; továbbá
16.76.3.[J], Előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat

A Jelentős (J) biztonsági osztálytól a fejlesztő nem dolgozhat ad-hoc módszerekkel. A szerződésben rögzíteni kell a biztonságos szoftverfejlesztési életciklus (SSDLC) alkalmazását, a forráskód-verziókövető rendszerek (például Git) használatát, valamint azt, hogy a fejlesztési és az éles környezetek szigorúan el legyenek választva egymástól.

> *16.79.[J], [M], A Szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezzen kritikussági elemzést:*
> *16.79.1.[J], [M], A rendszerfejlesztési életciklus alatt, a szervezet által meghatározott döntési pontokon.*
> *16.79.2.[J], [M], A szervezet által meghatározott szigorúsággal.*

A fejlesztőnek az architektúra tervezésekor modelleznie kell a fenyegetéseket és azonosítania kell a rendszer legkritikusabb elemeit, amelyek meghibásodása vagy kompromittálódása a legnagyobb kárt okozhatná a megrendelő számára.

> *16.86.[M], A szervezet kötelezi a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztőknek a megvalósított biztonsági funkciók, szabályozások és mechanizmusok helyes használatáról és működéséről.*

A Magas (M) biztonsági osztályú rendszereket fejlesztő vagy üzemeltető közreműködőkre vonatkozó szerződéses klauzulák a legszigorúbbak, a beszállítónak nyilatkoznia kell arról, hogy munkatársai rendelkeznek a szükséges kiberbiztonsági ismeretekkel és ezt oktatási naplókkal vagy tanúsítványokkal igazolnia is kell.

> *16.87.[M], A Szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan tervezési specifikációt és biztonsági architektúrát hozzon létre, amely:*
> *16.87.1.[M], Illeszkedik a szervezet biztonsági architektúrájához és támogatja azt.*
> *16.87.2.[M], Leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között.*
> *16.87.3.[M], Bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.*

A rendszerátadás feltétele egy részletes Biztonsági Architektúra Leírás elkészítése és a megrendelő általi jóváhagyása.

Ez a gyakorlatban azt jelenti, hogy a fejlesztési folyamatnak formálisan szabályozott, dokumentált, biztonsági kontrollokkal ellátott folyamatnak kell lennie. A közreműködőnek pedig ezen dokumentált, szabályozott fejlesztési életciklus szerint kell eljárnia. Ennek meg kell jelennie a szerződésben is.
Ezen kívül a szerződésnek az alábbiakra is érdemes kitérnie fejlesztés esetén:

- forráskód- és konfigurációkezelés,
- külső komponensek és nyílt forráskód,
- tesztelési és biztonsági vizsgálati kötelezettség,
- változáskezelés.

4.4 Dokumentációs követelmények

A 7/2024 (VI.24) MK rendelet alapján a szerződésben a közreműködőnek vállalnia kell a biztonsággal kapcsolatos dokumentumok elkészítését és be kell tartania az ezen dokumentumok védelmére vonatkozó követelményeket.
A rendelet az alábbi előírásokat tartalmazza ennek kapcsán:

16.8.[A], A Szervezet megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását.
16.15.1.[A], Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:
16.15.1.1.[A], az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;
16.15.1.2.[A], a biztonsági funkciók hatékony használatát és karbantartását; valamint
16.15.1.3.[A], az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.
16.15.2.[A], Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:
16.15.2.1.[A], a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;
16.15.2.2.[A], a felhasználói interakció biztonságos módját;
16.15.2.3.[A], a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.
16.15.3.[A], Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy A Szervezet dokumentálja az EIR, rendszerelem vagy rend-szerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket; és
16.15.4.[A], a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek. [7/2024 MK rendelet 2. melléklet]

Javasoljuk továbbá, hogy a szoftverfejlesztés esetén a szerződés rendelkezzen arról, hogy a rendszerbiztonság terv mely részeit készíti el a fejlesztő és mely részeit a megrendelő. Mindkét fél érdeke, hogy tisztázzák a feladatok terjedelmét.

Javasoljuk a Nemzeti Kiberbiztonsági Intézet által készített sablon használatát.

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/a-7-2024-mk-rendelet-alapjan-aktualizalt-rendszerbiztonsagi-terv-sablonok/

4.5 Humán kockázati követelmények

A rendelet szerint a szerződésnek tartalmaznia kell a teljesítés során a közreműködő és annak a teljesítésben közreműködő, az elektronikus információs rendszerhez hozzáférő munkatársai (az általa munkavégzésre irányuló jogviszony alapján vagy alvállalkozói minőségben foglalkoztatott személyek) titoktartási kötelezettségeit és az esetleges egyéb, személyi biztonsággal, humán kockázattal kapcsolatos kötelezettségeket, amelyek az alábbiak:

14.11.1.[A], [J], [M] "A szervezet:
Személyi biztonsági követelményeket állít fel a külső szolgáltatókkal szemben, amelyek magukba foglalják a szükséges biztonsági szerepköröket és felelősségeket."
14.11.2.[A], [J], [M] Megköveteli a külső szolgáltatóktól, hogy tartsák be a szervezet által meghatározott személyi biztonsági szabályokat.
14.11.3.[A], [J], [M] Dokumentálja a személyi biztonsági követelményeket.
14.11.4.[A], [J], [M] Megköveteli a külső szolgáltatóktól, hogy a meghatározott időn belül értesítsék a meghatározott személyeket vagy szerepköröket minden olyan külső személy áthelyezéséről vagy kilépéséről, akik szervezeti hitelesítő eszközzel, belépőkártyával vagy rendszerjogosultsággal rendelkeztek.

14.11.5.[A], [J], [M] Ellenőrzi, hogy a szolgáltató megfelel-e a személyi biztonsági követelményeknek.
16.98.1.[M] "A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:
rendelkezzen a hivatalos feladatok alapján meghatározott megfelelő hozzáférési jogosultságokkal; és"
16.98.2.[M] teljesítse a szervezet által meghatározott további átvilágítási kritériumokat.

A fentiek alapján tehát ezen kötelezettségek így különösen a következőket jelentik:

- a jogszabályok és a szervezet által meghatározott személyi biztonsági szabályok betartása és azok betartásának ellenőrzése (pl. a közreműködő tevékenységének szervezet általi logolása),
- a szervezet haladéktalan értesítése, amennyiben a közreműködő szervezeti hitelesítő eszközzel, belépőkártyával vagy rendszerjogosultsággal rendelkező munkatársai áthelyezésre kerülnek vagy munkaviszonyuk megszűnik,
- csak egyedileg használható, névre szóló jogosultság biztosítása a teljesítésben közreműködő munkatársak részére,
- a hozzáférési jogosultságoknak kizárólag a kapcsolódó feladatok ellátására való használata,
- a szervezet haladéktalan értesítése, ha a hozzáférési jogosultság biztosítása már nem szükséges az adott feladat ellátáshoz.

4.6 További közreműködő igénybevételével kapcsolatos követelmények

Amennyiben az elektronikus információs rendszer létrehozásában, üzemeltetésében, karbantartásában vagy javításában további közreműködő (alvállalkozó) igénybevételére kerül sor, akkor a rendelet az alábbiakat várja el:

19.7.[A], [J], [M] A Szervezet gondoskodik arról, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.
16.49.[A], [J], [M] A Szervezet:
16.49.1.[A], [J], [M] Szerződéses kötelezettségként 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.
19.19.[A], [J], [M] A Szervezet megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel. [7/2024 MK rendelet 2. melléklet]

Ez azt jelenti, hogy a közreműködővel kötött eredeti szerződésben foglalt követelményeknek tehát a további közreműködő(k) esetében is teljesülniük kell, amelyért a közreműködő tartozik felelősséggel. Ezért a közreműködő és az általa igénybe vett alvállalkozó közötti szerződésnek ezeket az elemeket tartalmaznia kell.
Az eredeti közreműködői szerződésnek továbbá rendelkeznie kell arról is, hogy a közreműködő kap-e általános felhatalmazást további közreműködő igénybevételére, vagy egyedileg kell erre engedélyt kérnie a szervezettől.

4.7 Üzemeltetési-támogatási szerződésekre vonatkozó követelmények

Az üzemeltetési-támogatási szerződések kapcsán a rendelet az alábbi előírást tartalmazza:

10.13.[M] A szervezet: 10.13.1. megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan EIR-ből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a karbantartott rendszer biztonsági képességeivel, vagy amennyiben ez nem biztosított,
10.13.2. megköveteli, hogy a karbantartandó elemet az EIR-ből eltávolítsák, a karbantartást megelőzően minden szervezeti információt biztonságosan töröljenek az érintett rendszerelemről. A karbantartási folyamat végrehajtását követően az érintett elemet átvizsgálják a potenciálisan kártékony szoftverek észlelése érdekében, mielőtt az EIR-hez csatlakoztatnák.

Az ilyen szerződésekben tehát rögzíteni kell azt, hogy távoli karbantartás azonos biztonsági szinten történjen és amennyiben ez pedig nem biztosított, akkor megvalósuljon az adattörlés.
Ezen kívül célszerű a szerződésben rögzíteni a hibajavítással együtt járó dolgokat is (pl. szolgáltatási szintek, hibajavítás menete és határideje, kötbér, további fejlesztési igényekhez kapcsolódó költségek), valamint a jogszabálykövetéssel és verziófrissítéssel kapcsolatosan felmerülő kérdéseket.

4.8 Egyéb követelmények

A rendelet a fentieken kívül az alábbi előírásokat is tartalmazza:

16.7.[A],A Szervezet a beszerzési folyamat során - beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is - a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:
16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.

Mivel a közreműködő a szervezet ellátási láncának a része, ezért a szerződésnek a fentiekből kifolyólag tartalmaznia kell rendelkezéseket:

- a közreműködő általi adatszolgáltatásra (a Kiberbiztonsági tv.ben foglalt kötelezettségeik teljesítéséről, információbiztonsági kockázatokról),
- incidensbejelentésre, valamint
- a kiberbiztonsági audit lefolytatása kapcsán, a felek közötti együttműködésre vonatkozóan is.

Ezen kívül ajánlott a szerződésben rögzíteni a biztonságtudatossági és szerepkör szerinti képzés szükségességét is.

5 FELHASZNÁLT FORRÁSOK

- 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 hatályon kívül helyezéséről (NIS 2 irányelv)
- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.)
- Kormányrendelet Magyarország kiberbiztonságáról szóló törvény 2024. évi LXIX. törvény végrehajtásáról szóló 418/2024. (XII.23.) Korm. rendelet
- A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet