Tartalom

1 Bevezetés

A Társaság gyakran külső szolgáltatóktól vesz igénybe szolgáltatásokat, vagy felhasználja azok termékeit, amelyek esetenként érzékeny vagy védett információkat, rendszerelemeket tartalmazhatnak. A külső szolgáltatói megállapodások kidolgozásakor figyelembe kell venni, hogy a szállított termékeikkel és szolgáltatásaikkal a beszállítók a Társaság belső működésével, rendszereivel, eszközeivel illetve berendezéseivel és/vagy munkatársaival kapcsolatos információkhoz juthatnak, amelyek a Társaság számára bizalmas, illetve titkos információk, és így üzleti titkot képeznek.

Ezek a bizalmas, illetve üzleti titkot képező információk többféle módon kerülhetnek a beszállító (külső szolgáltató) birtokába. Akár úgy is, hogy az együttműködés érdekében, a beszállító általi termék vagy szolgáltatás teljesítése céljából a Társaság átadja ezeket az adatokat vagy biztosítja ezen adatokhoz való hozzáférést, de az is lehetséges, hogy ezeket az adatokat maga a szolgáltató állítja elő a Társaság számára, amelyek utána a Társaság számára belső bizalmas vagy titkos információkká válnak.

Ez minden információ esetén fontos, azonban a személyes adatok tekintetében, a Társaság ügyfelei adataival, illetve a Társaság informatikai rendszereivel kapcsolatos adatok tekintetében ennek külön jogszabályok kiemelt jelentőséget és jogkövetkezményt adnak.

Ezeknek az adatoknak az adatérzékenységi szerinti biztonsági osztályba sorolása, és az ennek megfelelő védelem biztosítása a Társaság számára kiemelten fontos. A védelemnek egyenszilárdságúan kell működni az adatok teljes életciklusában (a keletkezéstől kezdve a felhasználáson, tároláson, feldolgozáson át a visszaszolgáltatásig, illetve a megsemmisítésig), beleértve minden résztvevő szervezetet és személyt, akik ebben a folyamatban részt vesznek. Ilyen módon – az adatok biztonsága zártságának garantálása érdekében – ennek ki kell terjedni az érintett beszállítókra, külső szolgáltatókra is.

Ehhez kapcsolódóan szükséges, hogy a Társaság olyan információbiztonsági (és kiberbiztonsági) intézkedési, felmérési és értékelési folyamatokat alakítson ki, működtessen és dokumentálja azok eredményét, amik eredményeként csökken a szerződéses partnerek, beszállítók, szolgáltatók és alvállalkozók által közvetített, a Társaság adatai és rendszerei ellen irányuló rosszindulatú és véletlen károkozások kockázata.

Jelen dokumentum ezen követelmények megvalósításához határozza meg a szükséges alapelveket és megvalósítási útmutatókat a tipikus, különböző jellegű beszállítói, külső szolgáltatói esetekre.

Az általános, különböző tárgyú, működéshez illetve egyéb működéstámogatáshoz szükséges alvállalkozói, külső szolgáltatói együttműködésre vonatkozó követelményeket a 2. fejezet tartalmazza, míg – kiemelt, különleges esetnek tekintve – az infokommunikációs szolgáltatásokat nyújtó alvállalkozókra vonatkozó konkrét elvárásokat részletesen a 3. fejezet gyűjti össze.

2 Információbiztonsági követelmények alapelvei a beszerzés során

A Társaság alvállalkozói, külső szolgáltatói együttműködések információbiztonsági kockázatai határozzák meg, hogy az egyes szerződések során milyen szigorú – milyen tartalmú – titoktartási és információbiztonsági követelményeket szükséges előírni és megvalósulásukat felügyelni.

Ennek megvalósításához szükséges, hogy a Társaság beszerzési illetve alvállakozó-kezelési eljárásrendje keretében szabályozottan valósuljanak meg – a beszerzési folyamat egyes szakaszaiba beágyazva, – a következő lépések:

a) Előkészítés, elemzés, a projektszintű kockázatok meghatározására: kockázatok meghatározása, intézkedések tervezése, (szükség esetén) maradványkockázat kritikusságának elemzése.
b) Követelmények meghatározása: az intézkedések és a kritikusság elemzés alapján meghatározhatók az alvállalkozó információbiztonsági irányítási rendszerére és az általa szállított termékre vagy szolgáltatásra vonatkozó információbiztonsági követelmények.
c) Alvállalkozó kiválasztása fázis: pályázati kiírás az alapkövetelmények alapján, tanúsítások beszerzése alapján (pl. ISO 27001 vagy egyéb tanúsítások szerint, saját beszállítói információbiztonsági / kiberbiztonsági követelménylistának való megfelelés alapján, ami ellenőrizhető alvállalkozó általi checklista kitöltésével vagy előzetes beszállítói audit végrehjatásával), amik segítenek az alvállalkozó alkalmasságának megítélésében.
d) Alvállalkozói szerződéskötésben: a titoktartási és információbiztonsági követelmények előírása, érvényesítése, és azok teljesítése ellenőrzésének biztosítása.
e) Alvállalkozó nyomon követése: az alvállalkozó auditálása, a projektet lezáró jelentés; a felmért és számottevő alvállalkozói információbiztonsági kockázatok nyomon követése.

Ezek a lépések a következőket jelentik:

2.1 Előkészítés, elemzés, a projektszintű kockázatok meghatározása

Az egyes alvállalkozói, külső szolgáltatói együttműködések információbiztonsági kockázatát az határozza meg, hogy az adott alvállalkozó, külső szolgáltató által kezelt, tárolt vagy általuk hozzáfért adatok nem megfelelő biztonsága milyen lehetséges közvetlen vagy közvetett kockázatot jelent a Társaság számára.

Ezt az információbiztonsági kockázatfelmérést már a beszerzési folyamat igény-előkészítési fázisában a beszerzést igénylő szervezet maga meg tudja tenni. Ennek kapcsán meg kell határozni a következőket:

- mi az alvállalkozói, külső szolgáltatói együttműködés tárgya, témája, időbeli kerete;
- mely – a Társaság tulajdonát képező, illetve a Társaság számára fontos – adatok lesznek az alvállalkozó, külső szolgáltató által kezeltek, elérhetők, illetve hozzáférhetők;
- mi ezeknek az adatoknak a tartalma, jellege;
- tartalmaznak-e ezek az adatok személyes adatokat, ügyfélre vagy ügyfél termékére vonatkozó adatokat, és/vagy informatikai rendszerekre vagy azok működésére vonatkozó adatokat;
- mi ezeknek az adatoknak az adatérzékenységi besorolása;
- ki által, hol és milyen módon kerülnek ezek az adatok az alvállalkozó birtokába;
- hol és milyen formában jelennek meg ezek az adatok az alvállalkozó saját kezelésében (elektronikusan és papír alapon);
- hol és milyen módon kap az alvállalkozó hozzáférést ezeknek az adatoknak a Társaság rendszerében történő tárolásához;
- hogyan, milyen módon használja az alvállalkozó, külső szolgáltató ezeket az adatokat a szolgáltatása nyújtása során;

- milyen védelmi intézkedéseket tesz az alvállakozó, külső szolgáltató ezeknek az adatokban a biztonsága érdekében, (amennyiben ez előre ismert);
- van-e már titoktartási szerződés az alvállalkozóval, külső szolgáltatóval, és az mire kötelezi őt, (amennyiben ez előre ismert);

Ezen információk alapján lehet / szükséges meghatározni az adott alvállalkozói, külső szolgáltatói együttműködésre vonatkozó információbiztonsági kockázatokat. A kockázatok felméréséhez a következő szempontokat szükséges miminmum vizsgálni:

- Milyen káresemény(ek) következhet(nek) be a Társaság számára, ha ezeknek az adatoknak sérül a bizalmassága / rendelkezésre állása / integritása?
- Milyen káresemény(ek) következhet(nek) be a Társaság számára, ha az alvállalkozói, külső szolgáltatói együttműködés során a Társaság általi adatmegosztások biztonsága sérül (pl. illetéktelen adathozzáférés valósul meg)?
- Milyen módon sérülhetnek az alvállalkozó, külső szolgáltató saját működése során ezeknek az adatoknak a biztonsága?

Az alvállalkozók, külső szolgáltatók információbiztonsági kockázatainak meghatározását célszerű – a fenti szempontok figyelembe vételével – az adott együttműködési projekt egyéb alvállalkozói kockázatainak figyelembe vételével együtt felmérni, és szükség esetén a megfelelő intézkedéseket is meghatározni. Ezért ennek a kockázatfelmérésnek a módja lényegében a beszerzések előkészítésekor a már meglévő alvállalkozói kockázatfelmérés alkalmazása, annak a tárgyának/tartalmának a kiegészítésével a fenti szempontok által meghatározott kockázatokra.

2.2 Követelmények meghatározása

A fő cél annak biztosítása, hogy az alvállalkozó, külső szolgáltató általi információbiztonsági kockázatok az alvállalkozó, külső szolgáltató által kellő mértékeben kezelve legyenek. Ehhez szükséges az alvállalkozói követelmények előírásával és betartatásával biztosítani, hogy az alvállalkozó szerződésekkel a következő kérdésekre elfogadható válaszokat kaphassunk.

- Milyen módon biztosítja az alvállalkozó, külső szolgáltató saját rendszerén belül ezeknek az adatoknak a biztonságát?
- Milyen garanciákat ad számunkra az erről való meggyőződéshez, ellenőrzéshez?
- Milyen garanciát vállal az információbiztonság sérülése esetén elszenvedett károkért?

Az egyes alvállalkozói, külső szolgáltatói együttműködések információbiztonsági kockázatai határozzák meg, hogy az adott együttműködés során milyen titoktartási és egyéb információbiztonsági intézkedések szükségesek. Ezeket az intézkedéseket, mint követelményeket – a vonatkozó együttműködési megállapodások előkészítéséhez – kell maghatározni, és majd az alvállalkozói, külső szolgáltatói megállapodásokban érvényre juttatni.

Ezt már a beszerzési folyamat igény-előkészítése fázisában maga az igénylő szervezet tudja megtenni, rögtön az információbiztonsági kockázatok felmérését követően, együtt a beszerzendő termék/szolgáltatás specifikálásával.

A követelmények terjedelme, részletei és biztonsági szintje értelemszerűn alkalmazkodjon az együttműködés tartalmához, az alvállalkozó, külső szolgáltató által kezelt, illetve hozzáfért adatok volumenéhez, adatérzékenységéhez és a meghatározott információbiztonsági kockázatokhoz. A követelmények – ezen szempontok figyelembe vételével – terjedjenek ki minimum a következő témákra:

- a megállapodás tárgya;
- a megállapodás érvényességi ideje (ideiglenes vagy állandó);

- eljárás az ideiglenes titoktartási megállapodások érvényességi idejének nyomon követésére és azok kellő időben történő meghosszabbításának megkísérlésére;
- az érintett személyek/szervezetek, (az alvállalkozó, külső szolgáltató információihoz való hozzáférésre vagy azok átvételére jogosult beszállítói személyzet kifejezett listája);
- a megállapodás tárgyát képező információk (tartalmi) jellege és adatérzékenységi kategóriája;
- az információk elfogadható felhasználásának szabályai, beleértve szükség esetén az elfogadhatatlan felhasználást is;
- a megállapodásban érintett felek felelősségei, (azaz mindkét fél kötelezettségei);
- a titoktartási kötelezettség kimondása (beleértve az üzleti titok meghatározását és értelmezését, a titoktartás mibenlétét, szabályait és elvárásait, …);
- rendelkezések a bizalmas, titkos, vagy egyéb fajta titkot képező információknak a szerződéses jogviszonyon túli kezelésére vonatkozóan is;
- az adatok ill. IT infrastruktúra hozzáférésének függvényében, adatkommunikációra is értelmezve – a szükséges információbiztonsági követelmények;
- informatikai rendszerek karbantartására, konfigurálására, frissítésére és tesztelésére vonatkozó rendszabályok, kiterjesztve a mobil adathordózókra, hordozható számítógépekre, diagnosztikai- és tesztberendezésekre vonatkozó szabályokra is;
- az alvállalkozó, külső szolgáltató információbiztonsági rendszerére vonatkozó előírások, annak betartására vonatkozó képességek és bizonyítékok;
- az alvállalkozó, külső szolgáltató adott megállapodásban részt vevő munkatársainak biztonságtudatossága, biztonságtudatossági képzése;
- az incidenskezelési követelmények és eljárások (különösen az értesítés és az együttműködés az incidens helyreállítása során);
- az előírásoknak való megfelelés bizonyításának lehetőségei (pl. független harmadik fél általi felülvizsgálat vagy a Társaság általi ellenőrzési jogok biztosítása);
- a titoktartás kiterjesztése az al-alvállakozókra is – amennyiben releváns;
- a megállapított biztonsági követelmények nemmegfelelésének szankcionálása;

2.3 Alvállalkozó kiválasztása

Alvállalkozók kiválasztása a beszerzési folyamat részeként, jellemzően pályáztatási eljárás keretein belül történik. Az alvállalkozónak a fenti (meghatározott) információbiztonsági követelményeknek való alkalmassága a kiválasztási szempontrendszer alapját kell képezze.

Ehhez szükséges, hogy az előző pontok eredményeinek figyelembe vételével, az Ajánlatkérési dokumentáció tartalmazza (legalább) a következő elemeket:

- alvállalkozó nyilatkozata titoktartásról és az információbiztonsági követelmények elfogadásáról;
- (szükség esetén) alvállalkozói minősítések (pl. ISO/IEC 27001, PCI DSS, SOC3, TISAX, …);
- (szükség esetén) alvállalkozó nyilatkozata az előzetes információbiztonsági beszállítói audit elfogadásáról;

Az ajánlatok értékelése során az ajánlatok műszaki értékelése és az ajánlattevők biztonsági ellenőrzése folyamatlépés tartalamazza az információbiztonsági követelményeknek való alkalmasság, megfelelés értékeklését is. Ez különböző esetekben a következő módon valósulhat meg:

- Amennyiben az elbírálás a legalacsonyabb ár elvének megfelelően történik, úgy nem kerül sor az ajánlatok műszaki, szakmai értékelésére, hanem azok műszaki megfelelőség szempontjából kerülnek megvizsgálásra az ajánlatkérésben meghatározott specifikációnak való megfelelés tekintetében (megfelelő/nem megfelelő). Ebben az esetben az ajánlati dokumentációban az

információbiztonsági követelményeket és elvárásokat úgy kell előírni, hogy az azokra adott válaszok és nyilatkozatok alapján igen/nem válasszal egyértelműen eldönthető legyen a megfelelés.

- Amennyiben az elbírálás az összességében legelőnyösebb ajánlat elvének megfelelően történik, úgy a műszaki, szakmai értékelés két lépésből áll. Az értékelők először azt vizsgálják, hogy az ajánlatok megfelelnek-e az ajánlatkérésben meghatározott minimális műszaki-szakmai követelményeknek, paramétereknek, beleértve az azok közt előírt információbiztonsági elvárásokat is. A megfelelő és egyben érvényes ajánlatok esetén pedig az ajánlatok műszaki, szakmai és egyéb (köztük az információbiztonsági) szempontok szerinti értékelése történik, az értékelés szempontjaira vonatkozó egyedi szabályok szerint. Az értékelési szempontok a Társaság beszerzési eljárásrendje alapján meghatározott belső dokumentumban kerülnek jóváhagyásra. Ebben az esetben az értékelési szempontokat ki kell egészíteni az információbiztonsági szempontokkal, ahol a súlyozás mértékének a kezdeti feltárt információbiztonsági kockázatokkal kell arányban állnia.

Szükség esetén – pl. a versenyben lévő alvállalkozók közül a megfelelő alvállalkozó kiválasztására, – ellenőrizhető az alvállalkozó információbiztonsági követelményeknek való megfelelésre vonatkozó alkalmassága is, például külső (3. fél általi) tanúsítványok bekérésével, vagy saját követelményeket tartalmazó checklista alvállalkozói kitöltésének leellenőrzésével, vagy az alvállalkozó információbiztonsági beszállítói auditjának az elvégzésével. Ennek lehetőségét a Beszerzési eljárásrendnek kell tartalmaznia.

2.4 Alvállalkozói szerződéskötés

A titoktartási és információbiztonsági követelményeknek való megfelelés az alvállalkozói, külső szolgáltatói megállapodás részét kell képezze. Ezt ezért az alvállalkozói, külső szolgáltatói szerződés részeként dokumentálni kell annak biztosítása érdekében, hogy a Társaság és a beszállító, külső szolgáltató között ne legyenek félreértések a vonatkozó információbiztonsági követelmények teljesítésére vonatkozó mindkét fél kötelezettségeivel kapcsolatban.

Ezek a titoktartási, információbiztonsági követelmények – az együttműködés módjának, szerződés típusának függvényében – képezhetik maguknak a szerződésnek a törzs-szövegét, vagy lehetnek önálló és érvényes mellékletei is. Akármelyik módon is, de ezeknek tartalmazniuk kell mindenképp a 2.2. pontban az adott együttműködésre meghatározott követelmények szerződéses, mindkét fél által elfogadott előírását és elfogadását.

2.5 Alvállalkozó nyomon követése

Az alvállalkozókkal, külső szolgáltatókkal való együttműködés során nagy jelentőségű a meghatározott, és szerződésesen előírt titoktartási és egyéb információbiztonsági követelmények folyamatos betartása.

Ezek monitorozása, folyamatos megfigyelése az együttműködés részeként, az együttműködésben résztvevő társasági szervezet feladata.

Amennyiben a beszerzési folyamat tartalmaz az alvállalkozó teljesítményértékelésére vonatkozó eljárást, amely értékeli a szállítókat (alvállalkozókat, külső szolgáltatókat) a szerződéses kötelezettségeik teljesítése, illetve a vevői elégedettség szempontjából, akkor ajánlott ezt az értékelési szempontrendszert kiegészíteni az információbiztonsági követelményeknek való megfelelés szempontjából is.

Amennyiben nincs ilyen eljárásrend, akkor szükséges egy ilyent létrehozni az információbiztonsági követelmények teljesítésének nyomon követése, illetve a feltárt alvállakozói információbiztonsági kockázatok monitorozása céljából.

3 Infokommunikációs szolgáltatók információbiztonsági követelményei

Infokommunikációs (ICT) szolgáltatók esetén az információbiztonsági követelmények célja a szolgáltatott informatikai és kommunikációs rendszerben a Társaság adatainak védelme, valaminz az ICT szolgáltatás biztonságos és folyamatos működésének biztosítása.

A Társaság külsős vállalatok által üzemeltetett informatikai szolgáltatásai esetében az üzemeltetés és üzemeltetési biztonság szabályozását az üzemeltető vállalat saját maga, saját belső eljárásai alapján végzi.

A Társaság, mint az informatikai szolgáltatást igénybe vevő fél feladata a megfelelő, számára fontos és megkövetelendő információbiztonsági és üzemi követelményeket az adott szolgáltatási szerződésen keresztül érvényesíteni, majd azokat a szolgáltatás – szintén a szerződésben szabályozott feltételeknek megfelelően – számon kérni és felügyelni.

Külső szolgáltatók által nyújtott informatikai és kommunikációs (ICT) szolgáltatásokon keresztül a szolgáltatók (beszállítók) hozzáférnek (esetleg kezelik) a szolgáltatást igénybe vevő adatait, információit, használják infrastruktúráját, valamint a szolgáltatásokon keresztül (az adott szolgáltatási szintnek megfelelő mértékben) befolyásolják a szolgáltatást igénybe vevő üzleti folyamatainak teljesíthetőségét, eredményességét is. Ezeken, és az ezekkel kapcsolatos információbiztonsági kockázatokon keresztül kell az informatikai szolgáltatások külső fél általi üzemeltetésének a feltételrendszerét kialakítani, hogy védekezni lehessen a szándékos vagy véletlen adatszivárgás, az illetéktelen adathozzáférés, az informatikai szolgáltatások megfelelő rendelkezésre állásának hiánya stb. ellen.

3.1 A szolgáltatói (beszállítói) szerződések követelményei

A szállítókkal kötött megállapodásoknak (direkt vagy közvetve) tartalmazniuk kell azokat a követelményeket, amelyek azokkal az információbiztonsági kockázatokkal foglalkoznak, amelyek az információs és kommunikációs technológiák szolgáltatási és termékellátási láncaival kapcsolatosak, és ezek megoldását garantálják.

Szempontok a szerződések tartalmára vonatkozólag:

- Titoktartási nyilatkozat (az alvállalkozói szervezet részéről, és egyénileg a Társaság adataihoz hozzáférő alvállalkozó személyei réászéről is);
- Érintett (átadott, illetve hozzáfért) információk, és hozzáférésük szabályozásának és megvalósításának módszere;
- Az adott információk a Társaság szerinti biztonsági osztályba sorolása, és a biztonsági osztályokra vonatkozó, szolgáltatóval szemberni elvárások;
- A kapcsolódó jogszabályi elvárásoknak megfelelő követelmények támasztása;
- Adathozzáférések biztonsági ellenőrzése vagy ellenőrzésének megkívánt szintje, – mindkét oldalon;
- Az információ-feldolgozás ill. -kezelés megengedhető szabályai vagy a szállító azon személyzetéről lista, akik hozzáférhetnek az információkhoz;
- A konkrét szerződésre vonatkozó információbiztonsági szabályok (papír alapú és elektronikus adatkezelésre, valamint – amennyiben értelmezhető – fizikai biztonságra is);
- Incidensek esetén a követendő tájékoztatási, kapcsolattartási és együttműködési eljárások kialakítása;
- Elvárások megadása biztonságtudatossági képzésekre a szolgáltatás nyújtásában résztvevőknek;
- A szállító alvállalkozóira vonatkozó követelmények előírása (beleértve az ellenőrzéseket is);
- Információbiztonsági témában kapcsolattartó felelősök megnevezése;
- A Társaság adataihoz hozzáférő alvállalkozó alkalmazottainak nevesítése, megnevezése;

- Információbiztonsági beszállítói audit, illetve egyéb folyamatellenőrzések és/vagy biztonsági illetve biztonságtudatossági ellenőrzések (ha szükségesek) joga, előírása és feltételei, keretei;
- Hibakezelési (probléma-megoldási) elvárások;
- A szerződésben foglalt információbiztonsági követelmények megszegéséből származó szankciók;
- A szerződés megszűnésekor vagy lejártakor az információk és átadott információhordozók visszaadásának, a szerződéses partner adathordozóján lévő információk megsemmisítésének követelményei;
- A szolgáltatott ICT szolgáltatások validálási, minőségbiztosítási elvárásai;

3.2 A kiszervezett ICT szolgáltatások felügyelete

A Társaság kiszervezett informatikai szolgáltatást igénybe vevő szervezeti egységnek (vagy az azért felelőssé kinevezett szervezeti egységnek) rendszeresen figyelemmel kell kísérnie, értékelnie kell és felül kell vizsgálnia a szállítói szolgáltatások teljesítését, a következő szempontok mentén:

- A szolgáltatásteljesítés színvonalának (pl. SLA) figyelemmel kísérése, a megállapodások megtartásának ellenőrzése;
- A szolgáltató által készített szolgáltatási jelentések átvizsgálása, és – szükség esetén –rendszeres ülések megrendezése, ahogy a szolgáltatói szerződésben ez előírt;
- Beszállítói auditok, illetve egyéb folyamatellenőrzések és/vagy biztonsági illetve biztonságtudatossági ellenőrzések lehetőségének megteremtése;
- Az információbiztonsági incidensekről – a szolgáltatói szerződéseknek megfelelő – információszolgáltatás bekérése és átvizsgálása;
- A szolgáltatónak a szolgáltatás teljesítéséhez kapcsolódó auditkísérő dokumentumainak, valamint a szolgáltatásnyújtással kapcsolatos biztonsági események, az üzemeltetési problémák, meghibásodások, a hibák nyomon követése és a megszakadások feljegyzéseinek – a szolgáltatói szerződéseknek megfelelő – bekérése és átvizsgálása;
- Az azonosított problémák kezelése és megoldása;
- A szállítóknak a saját beszállítói vonatkozású információbiztonsági aspektusainak átvizsgálása;
- Annak ellenőrzése és felügyelete, hogy a szállító rendelkezik elégséges és megfelelő kapacitással (és képességgel) és megfelelő alkalmas tervekkel ahhoz, hogy biztosítsa a megállapodott szolgáltatás folytonosságot, a szolgáltatási hibák és katasztrófák nélkül.

Dátum: ……..

Megbízó: …… Megbízott: ……