Adatbiztonság tervezése adattovábbítások esetén

Data security planning for data transfers

dr. Csekő Katalin
adatvédelmi tisztviselő,
Magyar Adatvédelmi Tudatosságért Társaság Egyesülete főtitkára
e-mail: fotitkar@madat.hu

Bevezetés

A személyes adatok kezelése kapcsán annak biztonságos megvalósítását – tekintettel arra, hogy mind a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016. április 27-i (EU) 2016/679 az Európai Parlament és a Tanács rendelet (a továbbiakban: általános adatvédelmi rendelet vagy GDPR) 5. cikk (1) bekezdésének f) pontja (integritás és bizalmas jelleg elnevezéssel) , mind pedig az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 4.§ (4a) bekezdése – alapelvként határozza meg az adatbiztonságot, minden adatkezelési művelet, így az adattovábbítások előkészítése, tervezése, illetve a gyakorlati megvalósítása során szem előtt kell tartani.

Az adattovábbítások jogszerű megvalósításához természetesen a többi adatkezelési alapelv betartása is szükséges, viszont ebben a tanulmányban nem cél ezeket bemutatni, a fókusz az adatbiztonságon van. Ugyanígy nem tér ki jelen tanulmány a GDPR és az Infotv. adatbiztonsági fogalomrendszerénél tágabb fogalmi kört jelentő információbiztonsági kritériumokra, amelyek egyébként részhalmazként magukba foglalják a személyes adatok biztonságát is.

Introduction

In relation to the processing of personal data, its secure implementation - given that that both Regulation (EU) 2016/679 (EU) of 27 April 2016 on the protection of natural persons with regard to processing of personal data and ont he free movement of such data, and repealing Directive Directive 95/46/EC (hereinafter: General Data Protection Regulation or GDPR) Article 5 (1) point f) of paragraph (under the name of integrity and confidentiality), and that CXII of 2011 on information self-determination and freedom of information Act (hereinafter: Infotv.) Section 4 (4a) - it is defined as a basic principle data security, all data processing operations, such as the preparation of data transfers,must be kept in mind during planning and practical implementation. Of course, the other data management principles apply to the legal implementation of data transfers compliance is also necessary, but this study does not aim to present them, the focus is on that is on data security. In the same way, this study does not cover the GDPR and Infotv. information security, which has a broader conceptual scope than the conceptual system of data security criteria, which otherwise include personal data as a subset safety as well.

Kulcsszavak: adattovábbítás, biztonságos, adatbiztonság

Keywords: data transfer, secure, data security

Jogszabályi háttér

A fent hivatkozott jogszabályok fogalomrendszere alapján a személyes adatok továbbítása is adatkezelési műveletnek minősül, ugyanis a GDPR 4. cikk 2. pontja alapján „adatkezelés”: „a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.” [1 ppt. 2 dia]

Az Infotv. 3.§ 10. pontja alapján: „adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése”.

[2 ppt 2. dia]

Az tehát egyértelmű, hogy amennyiben adattovábbításról beszélünk, az adatkezelésekre vonatkozó előírások irányadók és betartandók. Érdekesség viszont, hogy magának az adattovábbításnak közvetlenül a GDPR-ban nincs olyan egzakt fogalma, mint az Infotv-nek. Az Infotv. 3.§ 11. pontja alapján: „adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele”. [2 ppt. 2. dia] Azonban a magyar tagállami jogalkotásnak köszönhetően az adatkezelő nem marad bizonytalanságban a fogalmat illetően, ugyanis ugyanez a fogalom vonatkozik a GDPR hatálya alá tartozó adatkezelésekre is, tekintettel az Infotv. 2.§ (2) bekezdésére, amely ezt a fogalmat kiterjeszti ezen adatkezelésekre is.

Így tehát jelen tanulmányban adattovábbítás alatt, igazodva ehhez a fogalomhoz, mind az adatok fizikai átadását, mindpedig azok tényleges átadás nélküli hozzáférhetővé tételét adattovábbításként értelmezzük.

Az adattovábbítások biztonságosságára vonatkozó elvárások mind a GDPR, mind pedig az Infotv. rendelkezései között megjelennek.

A GDPR 24. cikk (1)-(2) bekezdései a technikai és szervezési intézkedések alkalmazására vonatkozó kötelezettség kapcsán hangsúlyozzák – egyéb szempontok, úgy, mint „az adatkezelés jellege, hatóköre, körülményei és céljai” mellett a kockázatalapú megközelítést és az intézkedések felülvizsgálatának és naprakészen tartásának kötelezettségét. [1 ppt 3. dia]

Adatbiztonsági szempontokat a GDPR 25. cikk (1)-(2) bekezdései – a beépített és alapértelmezett adatvédelemre vonatkozó rendelkezés – is tartalmaznak, akárcsak a GDPR 32. cikk (1) bekezdése. Utóbbiban már konkrét adatbiztonsági intézkedések is találhatók, nemcsak elvi szinten jelenik meg ez a kérdéskör.

Az Infotv. 25/I. § (1)-(3) bekezdéseinek kritériumrendszere egzaktabb, több konkrét feltételt tartalmaz a fentiekhez képest. Ezzel együtt nagyon hasonló megközelítést alkalmaz, tekintetbe veszi, hogy sor kerül-e különleges adatok kezelésére, illetve figyelembe veszi „különösen a

tudomány és a technológia mindenkori állását, az intézkedések megvalósításának költségeit, az adatkezelés jellegét, hatókörét és céljait, továbbá az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.” [2 ppt. 7. dia]

Fontos kiemelni, hogy az adatbiztonság biztosításában való közreműködés mindkét jogszabály alapján egyaránt terheli az adatkezelőt és az adatfeldolgozót is.

Az adattovábbítások tervezésének gyakorlati szempontjai

A jogszabályi rendelkezések tükrében, illetve a gyakorlati tapasztalatok alapján az alábbiakat szükséges és érdemes vizsgálni egy adattovábbítás biztonságos kialakítása érdekében:

- A továbbított adatok jellege, kategóriái, mennyisége, vagyis, hogy milyen személyes adatok továbbítására kerül sor, és mennyi adatot fog az adatkezelő a fogadó fél rendelkezésére bocsátani. Nem mindegy ugyanis, hogy pl. kapcsolattartókra vonatkozó információ kicserélése érdekében történik egy egyszeri adatátadás vagy a felek között rendszeres információcsere fog megvalósulni nagy mennyiségű személyes adat kapcsán. Ennek az előzetes vizsgálata azért nagyon lényeges, mert az határozza meg azt az alapkockázatot, amit az adattovábbítás akkor is hordozni fog, ha minden terv szerint zajlik, és nem következik be adatvédelmi incidens.
- Az adattovábbítás célja, vagyis, hogy miért és milyen másik félnek lesz erre szüksége, milyen jellegű tevékenység indokolja, pl. egy átvett feladatról van szó, aminek az átadás-átvétele során az adatok gazdát cserélnek, vagy valamely, önálló adatkezelők között létrejött szerződés teljesítéséről van szó, amely rendszeres vag egyszeri adatátadással jár.
- A küldésre és fogadásra/betekintésre jogoultak körének meghatározása: A személyes adatok bizalmasságának megőrzése érdekében elengedhetetlen ennek az átgondolása, hiszen ez biztosítja, hogy a folyamat során mindvégig csak az arra jogosultak férjenek majd hozzá az adatokhoz. Ez fokozottan igaz azokra a helyzetekre, ha az adatok több fél közreműködésével jutnak el rendeltetési helyükre, hiszen a továbbítás láncolatának hossza, a jogosultak magasabb száma már önmagában növelheti az adattovábbítás alapkockázatát.
- Az adattovábbításra igénybe vehető legális csatornák számbavétele: ezek kizárólag akkor határozhatóak meg reálisan, ha az előző lépéseket megtette az adatkezelő, hiszen az adatok mennyisége, jellege, a folyamat jellege, az adattovábbítás gyakorisága és az abban résztvevők ezt mind meghatározzák. Ilyenkor már körvonalazódnak a lehetséges opciók, hogy pl. elegendő és lehetséges-e az adatokat csak betekintéssel rendelkezésre bocsátani, vagy a már felsorolt szempontokra tekintettel szükséges-e fizikai adathordozón vagy elektronikus úton átadni azokat. A csatornák kapcsán a legális csatorna kiemelése nem véletlen. Amennyiben az adattovábbítás tervezésekor nem veszi figyelembe az adatkezelő a már felsorolt szempontokat, előfordulhat, hogy olyan csatornát választ, ami ugyan biztonságos, de nem támogatja az adatkezelő területet abban, hogy az átadási, hozzáférési folyamat gördülékenyen működjön. Ez sajnálatos módon arra indíthatja a szakterületeket, hogy az adatkezelőnél legálisan nem alkalmazható alternatívákat keressen, és elindítsa az adatbiztonsági szempontból jogszerűtlen és kockázatos, ún. shadow IT megoldások igénybevételét. Így tehát az adatkezelő szervezet által adatbiztonsági szempontból elfogadott, hivatalosan alkalmazható csatornák közül kell választani, a hatékonyság és alkalmasság figyelembe vétele mellett.

- Fokozatosság alkalmazásának vizsgálata, vagyis, hogy mi a személyes adatokhoz való hozzáférésnek a másik fél számára leghatékonyabb, de legkisebb rendelkezési lehetőséget (és így majd a legalacsonyabb kockázatot) jelentő eszköze, igazodva az adattovábbítás céljához. Így tehát, ha a cél eléréséhez elegendő, hogy a másik fél kizárólag eseti hozzáféréssel betekintsen az adatokba, pl. egy tanácsadás elvégzése céljából, akkor nem lesz szükség arra, hogy állandó hozzáférést kapjon vagy fizikailag is a birtokába kerüljenek a személyes adatok.
- Kockázatértékelés, vagyis a reálisan lehetséges veszélyek, veszélyforrások számbavétele, az általuk okozott kockázatok valószínűségének, súlyosságának értékelése. A realitásokon azért van hangsúly, mert az adatkezelők sokszor hajlamosak alábecsülni a kockázatot, ugyanakkor adatbiztonsági szempontból nem megfelelő, nem is hatékony és gazdasági szempontból sem kifizetődő, ha minden kockázatot magasnak minősítünk.
- A kockázatok kezelésére szolgáló technikai és szervezési intézkedések kiválasztása, melynek során, összhangban a jogszabályok kockázatalapú megközelítésével, az intézkedéseket a kockázatokhoz szabja az adatkezelő azzal, hogy az intézkedésekkel lefedett kockázatok mellett vállalt kockázatok is megjelenhetnek. Az intézkedések meghatározásakor figyelemmel kell lenni még arra is, hogy a technikai és szervezési intézkedések olyan kombinációja jöjjön létre, amelyek egymást hatékonyan kiegészítik. Ennek során nem hagyható figyelmen kívül, hogy rendszerben szükséges gondolkodni, hiszen ritka, hogy egy adatkezelő mindösszesen egy folyamattal rendelkezik és minden erőforrását arra tudja allokálni. Így tehát az új adattovábbítást annak eredendő és egy lehetséges incidensből eredő kockázataival együtt rendszerbe kell helyezni, és az adatkezelőnél folyó más adatkezelések relációjában meghatározni a kockázatkezelési intézkedéseket a kiválasztott adattovábbítási csatorna vagy mód kapcsán. Az intézkedéseket természetesen dokumentálni is kell, hiszen ennek hiányában nem felelne meg az adatkezelés az elszámoltathatóság elvének, amely alapelv minden más alapelvi megfelelést áthat.
- Amennyiben az adattovábbítást az adatkezelő nem egyedül szervezi meg vagy bonyolítja le, az ebben az egyes partnereknek jutó szerepet – a résztvevők státuszától függően – rendezni kell adatfeldolgozói szerződésben, illetve közös adatkezelői megállapodásban, hogy minden érintett fél tisztában legyen azzal, hogy az adatbiztonság terén milyen konkrét intézkedések kapcsán terheli felelősség.

Annak tényével, hogy az adatkezelő döntést hozott a fentiekről, még nem áll készen az adattovábbítás biztonságos megvalósítása, ehhez ugyanis az intézkedések megfelelőségének lehetséges felülvizsgálati ellenőrzési módjairól is dönteni szükséges, ugyanis ellenőrzés nélkül az adatkezelő nem fog tudni folyamatos bizonyosságot szerezni az adatkezelés hatékonyságáról és biztonságáról. Erre azért is szükség van, mert az adatkezelés körülményei változhatnak, és előfordulhat, hogy a korábban biztonságosnak minősülő adattovábbítás az új körülmények között már nem tekinthető annak.

Összefoglalás és következtetés

A személyes adatok kezelése kapcsán az integritás és bizalmas jelleg, illetve az ennek bizonyítására való képesség (elszámoltathatóság) megkerülhetetlen tervezési pontok. Az adatkezelés fogalmi körébe eső adattovábbítások során a biztonságos megvalósításhoz számos tényezőt kell figyelembe venni, melyeknek sora akkor látható át igazán, ha a vonatkozó jogszabályi rendelkezések mögé nézve, a gyakorlatot is vizsgálva, a tervezés, cselekvés, ellenőrzés és a tapasztalatok ismételt beépítése négyesre támaszkodva jár el az adatkezelő. Az így kialakított adattovábbítások segítik az adatkezelőket abban, hogy a jogi megfelelés mellett profi, megbízható partnerként, hiteles, biztonságos adatforrásként tekintsenek rájuk tevékenységi területükön.

Irodalomjegyzék

[1] A személyes adatok kezelése kapcsán – tekintettel arra, hogy mind az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről – 2024.12.15-én hatályos szöveg

[2] az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény – 2024.12.15-én hatályos szöveg