KOVÁCS RÉTI SZEGHEŐ
ÜGYVÉDI IRODA

Rés a pajzson 2. rész – ha adatkezelő és harmadik országba továbbít adatot (Pl. Mailchimpet használ) feltétlenül olvassa el cikksorozatunkat!

Az egyes kiegészítő garanciák felsorolása az ajánlás alapján

A harmadik országokba való adattovábbítás legnagyobb problémája, mint ahogy azt korábbi cikkünkben is említettük, hogy annak hatóságai jogszabályi keretek között, néha még a harmadik ország adatfeldolgozója tudta nélkül is jogosultak hozzáférni az adatokhoz. Az Európai Adatvédelmi Testület által közzétett ajánlás (1/2020. számú ajánlás) kiemeli például az amerikai FISA egy rendelkezését, amely alapján bármilyen beérkező adat vonatkozásában az adatfeldolgozó köteles hozzáférést biztosítani az amerikai hatóságok számára, amely egyben a titkosított adatok hozzáférést biztosító kulcsának átadását is jelenti. Ebből az is következik, hogy egy titkosított adattovábbítás sem garantál önmagában az EU által megkövetelt megfelelő védelmet. Az itt felsorolt egyes kiegészítő garanciák elsősorban technikai jellegűek, és elsődleges céljuk annak biztosítása, hogy a harmadik ország hatóságai még jogszabályi keretek között, a harmadik ország adatfeldolgozója közreműködésével sem juthasson személyes adatok birtokába.

Biztonsági mentés

Az ajánlás alapján csak abban az esetben elfogadható biztonsági mentés céljára tárolni adatokat harmadik országban (így például egy webtárhely szolgáltató útján), amennyiben a technika és tudomány jelenlegi állása szerint, a tárolás időtartamához igazítottan megfelelően titkosítva vannak az adatok. Szintén fontos kritérium, hogy a titkosításhoz szükséges kulcs mindig az adatkezelő birtokában marad, a biztonsági követelményeknek megfelelő tárolási módon.

Álnevesített adatok kezelése

Az álnevesítés célja, hogy az adat többletinformáció nélkül többet ne legyen hozzáköthető egy adott személyhez, azaz megszűnik a GDPR hatálya aló tartozó személyes adat minősítése. Ez az eszköz kifejezetten a kutatások során bizonyulhat hatékonynak, amely során a többletinformáció minden esetben az adatkezelő birtokában kell, hogy maradjon, a megfelelő technikai védelemmel ellátva. E körben kiemeli az ajánlás, hogy a GDPR szigorúan értelmezi a személyes adat fogalmát, így fizikai, szociális jegyek, vagy az internethez való hozzáférés időpontja és helyének rögzítése már önmagában is személyes adatnak minősül, hiszen egyértelműen beazonosítható az adott személy.

Titkosított adatok továbbítása harmadik országon keresztül

Amennyiben az adat továbbítása harmadik országon keresztül valósul meg, az adattovábbítás vonatkozásában is szükséges titkosítással rendelkezni. Az adattovábbítás során alkalmazandó titkosítás funkciója a kommunikáló felek között létrejövő kapcsolat biztonságának biztosítása, elsősorban a végpontok közötti titkosítási folyamattal, valamint az úgynevezett backdoor, azaz hátsó kapu lehetőségének kizárásával mind szoftveres, mind hardveres szinten.

Védett adatfeldolgozó

A harmadik országok jogrendjében is általános jelleggel védelem alá esnek bizonyos tevékenységek, így például az ügyvédi, orvosi szolgáltatások. Ezen tevékenységek védelme elsősorban a titoktartási kötelezettség jogszabályi szinten való átvezetésével és garantálásával valósul meg, amely a

hatóságokkal szemben is képes érvényesülni. Amennyiben ilyen védelem alá eső tevékenységi körből eredő adatokról van szó, amelyet a harmadik ország jogszabálya is hatékonyan szabályoz, úgy a többi technikai megoldás alkalmazása mellett (titkosítás például, különösen a végpontok közötti titkosítás) jogszerű lehet az adattovábbítás a harmadik országba.

Osztott feldolgozás

Lehetőség van továbbá harmadik országba történő adattovábbítás során az EU által megkövetelt védelmi szint elérésére olyan esetekben is, amikor az adatkezelő több, egymástól független adatfeldolgozó együttes közreműködésével kíván adatot feldolgozni. Ehhez az szükséges, hogy az adatfeldolgozók különböző államok joghatósága alá tartozzanak, egymás tevékenységéről nem tudva, egymástól függetlenül dolgozzák fel az adatokat úgy, hogy a felosztott adatból ne lehessen az érintett személyre következtetni, illetve ne lehessen az eredeti, felosztott adatot rekonstruálni.

Amikor kiegészítő garancia sem tud megfelelő védelmi szintet nyújtani

Végezetül az ajánlás kifejezetten kiemeli, hogy felhőszolgáltatásba (Drive, SkyDrive, Dropbox, iCloud) feltöltött és közvetlenül hozzáférhető adat (tehát nem biztonsági mentés céljából lementett) esetében, tekintettel arra, hogy a felhőszolgáltatást nyújtó – és így a hatóságok is - minden esetben hozzáfér(het) az adatokhoz, nem lát olyan kiegészítő garanciát, technikai megoldást, amely az EU által minimálisan megkövetelt védelmi szintet tudná biztosítani harmadik országba való adattovábbítás esetén.

Hasonlóan nem talált az Adatvédelmi Testület megoldást arra az esetre sem, amikor személyes adatokat tesz az adatkezelő elérhetővé távoli hozzáférés útján harmadik országban tartózkodó személyek számára, üzleti célból (így különösen szolgáltatás nyújtása céljából rendelkezésre bocsátott HR adatok, vagy ügyfelekkel való kommunikáció). Tekintettel arra, hogy ilyen esetek mindig hagyományos hírközlési hálózat útján valósulnak meg, ahol az adatfeldolgozó közvetlenül fér hozzá az adatokhoz, az ajánlás álláspontja szerint még a jelenleg ismert titkosítási folyamatok alkalmazásával sem tekinti az EU által minimálisan megkövetelt védelemmel ellátva az érintett személyes adatot.