Liber Ádám

Személyes adatok nemzetközi továbbítása. Az új adatvédelmi törvény margójára

Globális és infokommunikáción alapuló világunkban a személyes adatok határokat átlépő továbbítása mindennapi életünk integráns részévé vált. Nemzetközi adattovábbításra kerül sor többek között abban az esetben, ha egy adott országban található számítógéphez egy másik országban található számítógép útján hozzáférnek, ami különös jelentőséggel bír napjaink elosztott hálózati rendszereiben, ahol az adatfeldolgozás tényleges helye relatív, illetve meghatározhatatlan. A nemzetközi adattovábbítás kiszervezés útján lehetővé teszi, hogy egyes vállalatok az elektronikus ügyfélszolgálatuk fenntartását központilag, a fogyasztó, illetőleg a vásárló országától eltérő országból – akár Európán kívülről – olcsóbb és jobb anyagi feltételek mellett biztosítsák, ezáltal pedig erőforrásaikat és pénzeszközeiket kíméljék. A külföldre történő adattovábbítás lehetőségének gazdasági hasznossága tehát a globalizáció korában megkérdőjelezhetetlen, azonban mindemellett szükségképpen megnövekednek azok a szituációk is, melyek az adatalany személyes adatait (és ezzel együtt magánszféráját) veszélynek szolgáltatják ki.

A nemzetközi adattovábbítás veszélyt jelenthet az adatalany jogaira, mivel a személyes adatok olyan országba kerülhetnek, ahol az adatalany elveszíti ellenőrzését a magánszférája körébe tartozó információk felett, illetőleg amelynek jogrendszere nem garantálja megfelelően az adatalany magánszférájához / adatvédelemhez fűződő jogait. A szigorú szabályozás mellett szól, hogy az adatok határokat átlépő továbbításának az informatika mai feltételei között különösebb költsége nincsen. Emiatt – akár egyetlen gombnyomásra – személyes adatok, illetve érzékeny adatok tömege kerülhet külföldre, az adatalany és az adatvédelmi jog ellenőrzésén kívülre, ami azzal járhat, hogy az adatalany nem rendelkezik tudomással arról, hogy mire használják fel az adatait, esetlegesen nem kap tájékoztatást erről, illetve az adatok törlését és az adatalany egyéb jogorvoslati jogait nem biztosítják. Belátható, hogy könnyen megkerülhetőek lennének a személyes adatok védelmének jogszabályi garanciái, amennyiben korlátozás nélkül lehetőség lenne a személyes adatok külföldi (EGT-n kívüli) országokba történő áramlására.

Az adatvédelmi irányelv maga is számol azzal, hogy egyes harmadik államok olyan adatvédelmi szabályozással, illetőleg garanciákkal rendelkeznek, melyek adott esetben egyenrangúak az európai jog által nyújtott védelemmel. Ilyen esetben az adattovábbítás biztonságosságát az adott ország által nyújtott védelmi szint jelenti, ami származhat a harmadik ország jogrendszeréből vagy nemzetközi kötelezettségvállalásból.

1. AZ EURÓPAI UNIÓ SZABÁLYOZÁSA ÁLTALÁBAN

Az európai adatvédelmi jog azon a felismerésen alapul, hogy a személyes adatok kezelése az érintett viszonylatában jogkorlátozást valósít meg. Az adatvédelem célja, hogy az érintett magánszemély részére – akinek személyes adatait kezelik – a magánszférára kiterjedő védelmet nyújtson, melyet az egyénnek biztosított jogosultságok, illetőleg az adatkezelőre terhelt kötelezettségek kombinációjával érnek el. A külföldre történő adattovábbítás szabályozásának indoka, hogy egyes külföldi országokban nem létezik integrált és egységesen kodifikált adat- és magánszféra-védelem, illetőleg hiányoznak azok a jogok és kötelezettségek, illetve (alapjogi) garanciák, melyeket Európában az európai emberi jogi egyezmény 8. cikke, az alapjogi charta, az európai adatvédelmi irányelv (95/46/EK irányelv)[1], illetőleg tagállami szinten a nemzeti adatvédelmi alapjogok bástyáznak körül.

Az adatvédelmi jog európai uniós szinten az európai adatvédelmi irányelv által harmonizált joganyaga – ami az EU Bíróság joggyakorlata értelmében teljes harmonizációt nyújt[2] – biztosítja a személyes adatok tagállamok közötti szabad áramlását, míg harmadik országok esetében ugyanerre szigorú korlátozást érvényesít. Az irányelv az Európai Gazdasági Térség államai vonatkozásában egységes magas szintű védelmet teremt, és ennek megfelelően az ezen államokba irányuló adattovábbításokat a belföldi adattovábbításokkal azonos módon rendeli kezelni. Ezzel szemben az EGT-n kívülre irányuló (tehát harmadik országbeli) adattovábbításokra vonatkozóan az irányelv (57) preambulum-bekezdése azt rögzíti, hogy „*a személyes adatoknak a megfelelő védelmi szintet biztosítani nem tudó harmadik országokba irányuló továbbítását meg kell tiltani*". Az irányelv 25. cikke értelmében „*személyes adatok csak abban az esetben továbbíthatók harmadik országba, ha [...] az adott harmadik ország megfelelő védelmi szintet biztosít*".

Az irányelvi rendelkezés indoka a természetes személyek magánélet tiszteletben tartásához való jogának védelme Európán kívül is a védelem magas szintjének fenntartásával. Törékeny lenne ugyanis az az adatvédelmi rezsim, melyet meg lehetne kerülni a személyes adatok külföldre történő továbbításával.

Az adatvédelmi irányelv maga is számol azzal, hogy egyes harmadik államok olyan adatvédelmi szabályozással, illetőleg garanciákkal rendelkeznek, melyek adott esetben egyenrangúak az európai jog által nyújtott védelemmel. Ilyen esetben az adattovábbítás biztonságosságát az adott ország által nyújtott védelmi szint jelenti, ami származhat a harmadik ország jogrendszeréből vagy nemzetközi kötelezettségvállalásból.

Másrészről az irányelv azt is biztosítja, hogy – bizonyos esetekben – el lehessen térni a megfelelő szintű védelem követelményétől. Így lehetséges, hogy a harmadik ország nem nyújt megfelelő szintű védelmet, azonban az adatexportőr és az adatimportőr egyéb eszközökkel, így különösen magánjogi kötelezettségvállalások, illetőleg szerződések útján is megteremthetik a megfelelő, külföldi jogrendszer által nem biztosított adatvédelmi követelményeket. További lehetőségként létezik, illetőleg multinacionális vállalatok esetében praktikusnak mutatkozik a vállalat nemzetközi működéséhez szükséges adattovábbításai vonatkozásában egy olyan önszabályozás elvén

A szerző ügyvéd, a DataPrivacy.hu adatvédelmi blog szerkesztője.

nyugvó (adatvédelmi) szabályzat elfogadása, amely egy adott vállalatcsoport valamennyi tagját köti és ami érvényesítésre kerül a vállalaton belüli adattovábbítások vonatkozásában.

Végül az adattovábbítás nyugodhat olyan eszközön, illetve jogalapon, mely esetben nincs lehetőség a megfelelő szintű védelem biztosítására. Ez az irányelv hatálya alatt csak kivételes lehetőség lehet, illetve többletbiztosítékokhoz kötött, mint az adatvédelmi hatóság engedélye, nemzetközi szerződés létezése vagy akár valamely külön jogalap (pl. kifejezett hozzájárulás) alkalmazása.

Az európai adatvédelem irányelvi formában szabályozott, amely aktus címzettje a tagállam, és amely a konkrét célok megvalósításának módját az egyes tagállamokra bízza. Ekként a jelen tanulmány utolsó részében a hazai jog elemzésére térünk rá, különös tekintettel a jelenleg hatályos magyar adatvédelmi jog, illetve az új adatvédelmi törvény (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény[3]) 2012. január 1. napjával hatályba lépő szabályozására és annak változásaira az európai jogi nemzetközi adattovábbítási szabályok fényében.

2. A MEGFELELŐ SZINTŰ VÉDELEM ÉRTÉKELÉSE – BIZTONSÁGOS ORSZÁGOK

Az európai adatvédelmi irányelv nemzetközi adattovábbítással kapcsolatos kulcsfogalma a „megfelelő szintű védelem", melyről az irányelv 25. cikke rendelkezik, míg a 26. cikk az ettől való eltérés lehetőségét rögzíti.

2.1. A megfelelőségi teszt

Az irányelv (56) preambulum-bekezdése értelmében az irányelv nem áll útjában a személyes adatok továbbításának olyan harmadik országokba, amelyek megfelelő szintű védelmet biztosítanak (biztonságos országok). Az egyes országok értékelésének és ennek alapján az ún. biztonságos országok azonosításának egy „fehér lista" létrehozása jelentette a legegyszerűbb módját. Az értékelés mechanizmusának legalapvetőbb szabályait az irányelv rögzíti, melynek 25. cikk (2) bekezdése értelmében a harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni. Eszerint különös figyelmet kell fordítani (i) az adatok jellegére, (ii) a tervezett adatfeldolgozási művelet vagy műveletek céljára és időtartamára, (iii) a származási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogszabályokra, valamint (iv) az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre.

A 29. cikk szerinti adatvédelmi munkacsoport[4] „WP 4."[5] szám alatt állásfoglalást (munkaanyagot) bocsátott ki a „megfelelő szintű védelem" értékeléséről. A munkacsoport szerint az értékelés kockázat alapú megközelítést jelent, melynek két alapeleme (i) az adatvédelmi anyagi jogi szabályok léte, továbbá (ii) azok hatékony érvényesítésének eljárási eszközei. A munkacsoport állásfoglalásában számos olyan alapelvi szintű szabályt és végrehajtási mechanizmust rögzített, melyek a megfelelő szintű védelem minimumának minősülnek és amelyet összefoglalóan *„megfelelőségi teszt"*-nek neveznek. A megfelelőség anyagi jogi szabályai / alapelvei közül a munkacsoport az alábbiakat emelte ki:

(a) *Célhoz kötöttség:* Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak.

(b) *Adatminőségi, szükségességi/arányossági követelmények:* Ez a követelmény az adatkezelés tisztességességét, törvényességét; illetve pontosságát, teljességét, időszerűségét jelenti. Emellett az adatok tárolási módjának alkalmas kell lennie arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

(c) *Az adatkezelés transzparenciája:* az érintett tájékoztatása az adatkezelésről, az adatkezelő személyéről.

(d) *Az adatalany jogainak biztosítása:* Az adatalany megismerheti a rá vonatkozó adatokat, azokat helyesbítheti, kiegészítheti vagy töröltetheti.

(e) *Adattovábbítás korlátozása:* adatok továbbítása csak olyan személy részére megengedett, aki szintén megfelelő szintű védelmet biztosító rezsim hatálya alá tartozik.

(f) *Különleges személyes adatok kezelése:* többletgaranciák létezése az ilyen adatok kezelése esetében.

(g) *Direkt marketing* esetén: minimálisan az *opt-out* lehetőségének biztosítása az adatalany részére.

(h) *Automatizált egyedi döntés esetén az érintettnek joga van az* alkalmazott matematikai módszerről, illetve annak lényegéről tájékoztatást kapni; továbbá biztosítani kell az érintett jogos érdekeinek védelmét.

A munkacsoport az anyagi jogi szabályok vizsgálata mellett különös hangsúlyt fektet a végrehajtási mechanizmusok létezésének igazolására, mivel az adatvédelmi szabályok csak abban az esetben járulnak hozzá az egyén védelméhez, amennyiben azokat effektív módon követik és érvényesítik a gyakorlatban is. A munkacsoport a megfelelőség *végrehajtási mechanizmusai* közül ezért a következőket jelölte meg annak biztosítékaiként: (a) az adatvédelmi szabályok tényleges betartása/végrehajtása, illetve az adatkezelés hatósági felügyelete; (b) a hatékony jogérvényesítés lehetősége; továbbá (c) jogsértés esetén megfelelő jogorvoslat biztosítása.

A munkacsoport állásfoglalása ezt meghaladóan elismerte, hogy az ET 108-as számú adatvédelmi egyezményét ratifikáló államokba történő adattovábbítás feltehetően megfelel az irányelv 25. cikkében foglalt megfelelő szintű védelem követelményének.

2.2. A megfelelőség értékelése

A megfelelőség értékelésére az adatvédelmi irányelv az Európai Bizottságot jogosítja fel.[6] A Bizottság ugyanis határozatával megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít, melynek alapja a harmadik ország belső joga, vagy annak vállalt nemzetközi kötelezettségei. A Bizottság vonatkozó javaslatát a 29. cikk szerinti adatvédelmi munkacsoport és a 31. cikk szerinti bizottság véleményezése előzi meg, azt az Európai Parlament ellenőrizheti, majd a biztosok kollégiuma ezt követően fogadja el a vonatkozó határozatát, melyet adatvédelemre / adatforgalomra vonatkozó nemzetközi szerződés megkötése is kísérhet. A döntés gyakorlati jelentősége, hogy szinte a belföldi adattovábbítással teszi egyenrangúvá a személyes adatok továbbítását, ami különösen kedvező hatással járhat a kereskedelmi és pénzügyi kapcsolatokra az érintett harmadik országgal.

Az Európai Bizottság a mai napig a következő országokkal kapcsolatosan állapította meg, hogy azok jogrendszere az európai adatvédelmi irányelvnek megfelelő szintű védelmet biztosít a személyes adatok védelmére: Argentína, Svájc, Guernsey, Man-sziget, Kanada (olyan szervezetek tekintetében, melyek kereskedelmi tevékenységük keretében személyes adatot kezelnek, valamint PNR adatok továbbítására), Ausztrália (PNR[7] adatokra), Jersey, Feröer-szigetek és legutóbb Izrael.

2.3. Az USA speciális helyzete – Safe Harbor

Az Amerikai Egyesült Államok vonatkozásában abban az esetben biztosított a megfelelő szintű védelem, amennyiben az adattovábbítás olyan amerikai vállalat részére történik, amely szerepel a Biztonságos Kikötő (Safe Harbor) listán; vagy ha utas-nyilvántartási (PNR) adatokat továbbítanak az Egyesült Államok Vámügyi és Határvédelmi Irodájának.[8]

Az Amerikai Egyesült Államok az Európai Gazdasági Térségből származó adattovábbítások esetén speciális helyzetben van, mivel az USA nem rendelkezik általánosan kodifikált adatvédelmi szabályozással, ugyanis az amerikai gyakorlatot a szektorális adatvédelmi megközelítés jellemzi. Amerikai egyesült államokbeli adatkezelő, illetve adatfeldolgozó esetében többek között abban az esetben tekinthető biztosítottnak a személyes adatok megfelelő szintű védelme, amennyiben a személyes adatokat ún. Safe Harbor listán szereplő vállalat részére továbbítják.

Az Amerikai Egyesült Államok az Európai Gazdasági Térségből származó adattovábbítások esetén speciális helyzetben van, mivel az USA nem rendelkezik általánosan kodifikált adatvédelmi szabályozással, ugyanis az amerikai gyakorlatot a szektorális adatvédelmi megközelítés jellemzi. Figyelembe véve az EU és az USA közötti intenzív kereskedelmi kapcsolatokat és a tömeges adatforgalmat, az Amerikai Egyesült Államok Kereskedelmi Minisztériuma és az Európai Bizottság két évet szánt egy megfelelő egyezményes keret létrehozására, amely alapján amerikai adatkezelők az európai adatvédelmi irányelv követelményeinek – önszabályozás alapján – meg tudnak felelni. Ezek az ún. Safe

Harbor adatvédelmi elvek, melyek irányelvnek való megfelelőségéről 2000. július 26-án bocsátott ki határozatot az Európai Bizottság.[9]

Amerikai egyesült államokbeli adatkezelő, illetve adatfeldolgozó esetében többek között abban az esetben tekinthető biztosítottnak a személyes adatok megfelelő szintű védelme, amennyiben a személyes adatokat ún. Safe Harbor listán szereplő vállalat részére továbbítják.

A Safe Harbor elveknek való megfelelés önminősítés alapján történik, az érintett amerikai székhelyű vállalat (corporation)[10] önkéntes döntése alapján. A Safe Harbor programban való részvétele esetén egy vállalat (i) csatlakozik egy öntanúsítási programhoz, amely megfelel a Safe Harbor elveknek vagy saját adatvédelmi (ön)szabályozásnak veti alá magát; (ii) kinyilvánítja a Safe Harbor elveknek való megfelelőségét, melyet adatvédelmi szabályzatában is nyilvánosan közzétesz, továbbá (iii) minimális díj megfizetése mellett az USA Kereskedelmi Minisztériuma részére évente írásban kinyilvánítja (öntanúsítja), hogy az adatvédelmi elveknek megfelel és ezáltal feltüntetésre kerül a Safe Harbor listán.[11]

A Safe Harbor gyakorlati jelentőségét mutatja, hogy a legnagyobb amerikai adatkezelők, a Facebook, a Google, az Amazon, az eBay illetve a legnagyobb amerikai vállalatok a Safe Harbor listán való szereplés útján biztosítják azt, hogy adatkezelésük megfeleljen az európai adatvédelmi irányelv rendelkezéseinek.

Az EU–USA adattovábbításokat szabályozó Safe Harbor program tavaly ünnepelte tizedik évfordulóját, ami nem volt kritikus felhangoktól sem mentes. A Safe Harbor végrehajtásában ugyanis komoly hiányosságok mutatkoznak, mivel ez kizárólag az amerikai jogszabályok alapján történik meg – végső esetben a szövetségi kereskedelmi hatóság, a Federal Trade Commission (FTC) kikényszerítése útján, ami „megtévesztés" miatt szankcionálhatja az adatvédelmi elveknek való megfelelést tanúsító, de azoknak gyakorlatilag eleget nem tevő vállalatokat. A végrehajtás gyengeségét mutatja, hogy az FTC részéről a tíz év alatt eddig csupán hét (sic!) esetben került sor eljárásindításra a Safe Harbor megsértése miatt.[12]

3. ELTÉRÉSEK A MEGFELELŐ SZINTŰ VÉDELEMTŐL

Az adatvédelmi irányelv 26. cikke alapján akkor is sor kerülhet adattovábbításra, amennyiben a megfelelő szintű védelem nem biztosított az adat címzettje szerinti országban. Ennek egyik megoldása a megfelelő szintű védelem szerződési feltételek útján való biztosítása, kötelező erejű vállalati szabályok alkalmazása, vagy a 26. cikk (1) bekezdésében szabályozott valamely kivételre támaszkodás.

3.1. Szerződéses feltételek (egyedi és általános szerződési feltételek)

Az adatvédelmi irányelv 26. cikk (2) bekezdése értelmében a tagállamok engedélyezhetik a személyes adatok olyan harmadik országba irányuló továbbítását, amely nem biztosít megfelelő szintű védelmet, amennyiben az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében; ilyen garanciát jelenthetnek elsősorban a megfelelő szerződési feltételek. Az adatkezelőnek tehát nem feltétlenül szükséges a harmadik ország jogrendszere által nyújtott megfelelő szintű védelemre támaszkodnia, mivel magánjogi eszközök útján is elérheti a kívánt célt: a megfelelő szintű védelem szerződés útján való biztosításával. Ennek az uniós jog alapján jelenleg két eszköze létezik: egyrészről lehetőség van ún. *ad-hoc* szerződési feltételek alkalmazására, másrészről az Európai Bizottság határozatával engedélyezett általános szerződési feltételek használatára.

A szerződéses út lényege, hogy az megfelelő módon kompenzálja egy adott harmadik országban az általános adatvédelmi szint hiányosságait, ami gyakorlatilag azt követeli meg, hogy anyagi szabályok rögzítésével, továbbá azok hatékony érvényesítésének eljárási eszközeivel a felek szerződésben pótolják a hiányzó jogszabályi garanciákat.[13] Egy adattovábbítási szerződésnek tehát jóval többet szükséges nyújtania az adat-exportőr és adat-importőr közötti feladatmegosztásnál, mivel többletgaranciákat kell nyújtania az adatalany részére a megfelelő védelmi szint biztosítása érdekében. A megfelelőség szerződési megteremtésének tehát a fentebb bemutatott „megfelelőségi teszt" vonatkozásában irányadó adatvédelmi alapelveket és végrehajtási garanciákat szükséges átfognia, amely részletes rendezést igényel – cél, eszközök, feltételek meghatározásával – a teljes adatkezelés vonatkozásában. A szerződés által biztosított „megfelelőség" vizsgálata ebben az esetben megegyezik a harmadik országra vonatkozó megfelelőség értékelésével. A szerződésben szabályozandó kötelezettségek magukban foglalják (i) az adattovábbítás megtiltását olyan személyek részére, melyek a szerződés által nem kötelezettek; (ii) az adat importálójának az adattal kapcsolatos autonóm tevékenységének korlátozását/kizárását; (iii) felelőség telepítését az EGT területén letelepedett exportálóra stb. A munkacsoport a WP 12-es számú munkadokumentumában a szerződéses eszközök lényeges korlátjaként kiemeli, hogy olyan ország, amelyben az állam (annak szerve) olyan indokból is hozzáférhet az adatokhoz, melyek egy demokratikus társadalomban a szükségesség/arányosság sztenderdjét nem elégítenék ki, a szerződéses alapú adattovábbításnak nem lehet célállomása.

A szerződéses út lényege, hogy az megfelelő módon kompenzálja egy adott harmadik országban az általános adatvédelmi szint hiányosságait, ami gyakorlatilag azt követeli meg, hogy anyagi szabályok rögzítésével, továbbá azok hatékony érvényesítésének eljárási eszközeivel a felek szerződésben pótolják a hiányzó jogszabályi garanciákat. Egy adattovábbítási szerződésnek tehát jóval többet szükséges nyújtania az adat-exportőr és adat-importőr közötti feladatmegosztásnál.

Az irányelv 26. cikk (4) bekezdése alapján az Európai Bizottság határozatával *általános szerződési feltételeket* fogadhat el, melyek alkalmazását úgy kell tekinteni, hogy azok kielégítő biztosítékot nyújtanak az adattovábbítások megfelelősége vonatkozásában. A Bizottság 2001-ben két általános szerződési feltétel csomagot fogadott el a nemzetközi adattovábbítások megkönnyítésére. Az első az EGT-beli adatkezelő és harmadik állambeli adatkezelő közötti adattovábbításra vonatkozik, melyről a Bizottság 2001/497/EK határozata rendelkezik,[14] míg a második ilyen csomag EGT-beli adatkezelő és harmadik állambeli adatfeldolgozó közötti adattovábbításokra vonatkozik. Ez utóbbi a 2002/16/EK bizottsági határozat (általános szerződési feltételek személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására), melyet utóbb felváltott a 2010/87/EU bizottsági határozat, amely már lehetővé teszi adatfeldolgozók részére további adatfeldolgozó (ún. sub-processor) igénybevételét is.

Az általános szerződési feltételek alkalmazását a tagállamok kötelesek elismerni, azonban a tagállami adatvédelmi hatóságok azok alkalmazása esetén kérhetik annak benyújtását, illetve letétbe helyezését a tagállami adatvédelmi hatóságnál. A tagállamok felügyeleti hatóságai kulcsfontosságú szerepet játszanak e szerződéses adattovábbítási mechanizmusban. Amennyiben ugyanis fennáll a veszélye, hogy a felek bármelyike az általános szerződési feltételeket nem hajtja végre, nem tesz annak eleget, úgy a tagállami adatvédelmi hatóság ebben az esetben felfüggesztheti vagy akár megtilthatja az adattovábbítást. A szerződési feltételeket a felek nem módosíthatják, illetve azokat nem változtathatják meg, azonban az megköthető akár önállóan az exportőr és importőr között vagy akár valamely szerződés részeként is.

Az általános szerződési feltétel csomagok alkalmazásával ellentétben az ún. egyedi (*ad-hoc*) szerződési feltételek alkalmazásának tagállami engedélyezését be kell jelenteni az Európai Bizottság részére az irányelv 26. cikk (3) bekezdésének megfelelően,[15] míg az általános szerződési feltételeket csak abban az esetben, amennyiben a tagállam annak alapján felfüggeszti illetve megtiltja a külföldre irányuló adattovábbítást.

3.2. Kötelező erejű vállalati szabályok (BCR)

Az ún. „kötelező erejű vállalati szabályok" (Binding Corporate Rules – BCR) olyan multinacionális vállaltcsoportok által elfogadott belső szabályozó-együttesek (magatartási kódex, szabályzat stb.), melyek egységesen, az adatkezelő illetve adatalany nemzetiségétől függetlenül, az adott vállalat különböző EGT-n kívüli országokban is elhelyezkedő egységei közötti adatáramlás szabályozására szolgálnak. A kötelező erejű vállalati szabályok a megfelelő szintű védelmet tehát a vállalat(csoport) egyoldalú kötelezettségvállalása útján biztosítják.

A BCR-ok használatának alapja, hogy a szerződéses adattovábbítási megoldások alkalmazása nem minden esetben praktikus, illetve ezek adott esetben komoly adminisztratív terhet jelenthetnek az azt alkalmazó vállalat-

csoport részére. A BCR-ok jogalapja – a szerződéses feltételek alkalmazásához hasonlóan – az adatvédelmi irányelv 26. cikk (2) bekezdése, azonban a szerződéses konstrukciótól eltérően ez egyoldalú kötelezettségvállalást jelent az azt alkalmazó vállalatcsoport részéről. A BCR-t az érintett nemzeti adatvédelmi hatóságok hagyják jóvá az Irányelv 26. cikkének (3) bekezdése szerint, és engedélyezésük feltétele, hogy azok kötelező erővel bírnak az azt alkalmazó vállalat(csoport) minden egysége részére.

A BCR alkalmazásának megkönnyítése érdekében a 29. számú adatvédelmi munkacsoport több munkadokumentumot is kibocsátott, amelyek jelentősen könnyítenek a BCR-okkal kapcsolatos adminisztráción, illetőleg egyablakos ügyintézést vezettek be a multinacionális vállaltok részére. Ez az adattovábbítási mechanizmus tehát méltán nevezhető a munkacsoport egyik sikertörténetének. A munkacsoport által 2003-ban elfogadott WP 74-es számú dokumentum[16] általános kérdésekkel foglalkozik, míg az ezt követő dokumentumok a kooperációs eljárásról, a „vezér-hatóság" (lead authority) kiválasztásáról,[17] továbbá a BCR-ok összeállításával és azok engedélyeztetésével kapcsolatos tartalmi és formai követelményekről nyújtanak információkat.[18]

A BCR alkalmazásának megkönnyítése érdekében a 29. számú adatvédelmi munkacsoport több munkadokumentumot is kibocsátott, amelyek jelentősen könnyítenek a BCR-okkal kapcsolatos adminisztráción, illetőleg egyablakos ügyintézést vezettek be a multinacionális vállaltok részére. Ez az adattovábbítási mechanizmus tehát méltán nevezhető a munkacsoport egyik sikertörténetének.

A BCR engedélyeztetésének első lépése a vezér-hatóság kiválasztása. A vezér-hatóságot elsősorban a kérelmet előterjesztő vállalkozás anyavállalkozásának, vagy a vállalkozás központjának az EU valamely tagállamában található székhelye határozza meg. A kérelmező vállalkozáscsoport bármely adatvédelmi hatóságot felkérhet vezérhatóságnak, azonban a megkeresett adatvédelmi hatóság nem köteles elfogadni ezt a megkeresést, amennyiben egy másik hatóság általi eljárás alkalmasabbnak mutatkozik, továbbá két hetes határidőn belül bármely más hatóság is kifogást emelhet e megkereséssel szemben.[19]

A BCR elkészítése során az engedélyezés iránti kérelmet előterjesztő vállalkozásnak be kell mutatnia a saját vállalkozását, és az engedélyezendő adattovábbítások rövid leírását; igazolni kell, hogy a BCR-ok mind befelé – tehát a vállalkozáscsoport tagjai, munkavállalók és adatfeldolgozók irányában – mind kifelé, az adatalany irányában (egyoldalú kötelezettségvállalásként, amennyiben ez megengedett) kötelezőek. Ezt meghaladóan a BCR hatékony alkalmazása érdekében különböző eljárásokat, így munkavállalói képzéseket, belső panaszkezelési eljárásokat, illetve auditokat szükséges bevezetni.[20]

A BCR-ok tartalmával kapcsolatosan a munkacsoport azt a követelményt rögzítette, hogy abban egyértelmű kötelezettségvállalásként szerepelnie kell annak, hogy a vállalatcsoport Európai Unión belüli központja vagy EU-n belüli felelős tagja felelősséget vállal az EU-n kívüli vállalati tag jogsértéséért, illetve a szükséges lépéseket a jogorvoslat megfelelő biztosítása érdekében megteszi és szükség esetén kártérítést fizet. Ezzel összefüggésben a bizonyítási terhet a vállalatcsoport EU-n belüli felelős tagjának / központjának kell vállalnia. A BCR-oknak ezt meghaladóan tartalmazniuk kell, hogy az érintett ügyfél illetve munkavállaló panasszal élhet a nemzeti adatvédelmi hatóságnál és igényét a bíróságon is érvényesítheti, amennyiben a személyes adatainak kezelésével kapcsolatosan jogsérelem éri. A BCR által érintett valamennyi tagvállalatnak együtt kell működnie a tagállami adatvédelmi hatóságokkal, együttműködés hiányában pedig lehetőség van akár a megadott engedély visszavonására is.

A kooperációs eljárás keretében a vezér-hatóság körözteti az adatvédelmi hatóságok között a BCR tervezetét, melyre nézve a hatóságok egy hónapon belül nyújthatnak be észrevételeket. Ezt követően a tervezet végső változatát is körözteti és ahhoz a hatóságok jóváhagyását kérik. A munkacsoporton belül jelentős erőfeszítések történtek a kooperációs eljárás további gyorsítása érdekében, ezért jelenleg tizenkilenc adatvédelmi hatóság[21] már ún. MRP (mutual recognition procedure/ kölcsönös elismerési eljárás) keretében működik együtt a BCR-ok engedélyeztetésében. Amennyiben ennek keretében a vezér-hatóság elismeri a BCR megfelelőségét, az MRP-eljárás által nyújtott előny, hogy a további hatóságok ilyen esetben – külön vizsgálat nélkül – automatikusan bocsátják ki a saját jóváhagyásukat, ami jelentős eljárási könnyítést jelent a BCR engedélyeztetését kérő vállalat részére.

3.3. Kivételek

Az irányelv 26. cikk (1) bekezdése alapján akkor is sor kerülhet adattovábbításra, amennyiben a megfelelő szintű védelem nem biztosított, feltéve, hogy az alábbi feltételek valamelyike fennáll:

(a) az adatalany kifejezett, önkéntes hozzájárulást adott az adattovábbításhoz;

(b) adattovábbítás szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges vagy érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;

(c) a továbbítás fontos közérdekből szükséges;

(d) a továbbítás jogok bíróság előtti megállapítása, gyakorlása vagy védelme miatt szükséges;

(e) továbbítás az érintett létfontosságú érdekeinek védelme miatt szükséges;

(f) a továbbítást olyan nyilvántartásból végzik, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll.

Eltérést az irányelv a fent meghatározott adattovábbítási lehetőségektől csak konkrétan meghatározott esetekben engedélyez.

Mint azt az adatvédelmi munkacsoport 1998. július 24-én elfogadott „*A személyes adatok továbbítása harmadik országokba: az EU adatvédelmi irányelve 25. és 26. cikkének alkalmazása*" című munkadokumentumában kifejtette, a fent meghatározott eltéréseket – azok kivétel jellegéből adódóan – szűken kell értelmezni. Ezek olyan szűken meghatározott esetekre vonatkoznak, melyek esetében alacsony a kockázata az adatalany adatvédelemre vonatkozó jogának sérelmére, továbbá konkrétan meghatározott esetekre nézve – így különösen sérülékeny csoportok, mint munkavállalók vagy betegek (egészségügyi ellátást igénybe vevő vagy abban részesülő személyek) esetében – attól a tagállamok is eltérhetnek.

A nemzetközi adattovábbításhoz adott *hozzájárulás* vonatkozásában az irányelv „kifejezettséget" követel meg. Ennek megfelelően nem felel meg a kifejezettség követelményének az, amennyiben az adatalany nem tiltakozott a továbbítással szemben, illetve hozzájárulását csak ráutaló módon adta meg. A kifejezettséget meghaladóan a hozzájárulásnak önkéntesnek és határozottnak, illetve tájékozottnak kell lennie – ezek a hozzájárulás érvényességének feltételei. A tájékozottság követelménye vonatkozásában a munkacsoport rögzíti, hogy az adatalany megfelelő tájékoztatása a nemzetközi adattovábbítás kontextusában feltételezi a megfelelő szintű védelmet nem nyújtó országba irányuló adattovábbítás kockázatairól való kioktatást is. Amennyiben erre nem kerül sor, úgy a vonatkozó kivétel sem alkalmazható, azaz a hozzájárulás nem képezheti az adattovábbítás jogalapját.

A szerződési jogalapon szabályozott kivételek vonatkozásában kiemelendő, hogy valamennyi 26. cikkben szabályozott eset a szerződés teljesítéséhez (illetve szerződést megelőző teljesítéshez) szükséges adattovábbításokra korlátozódik, ami egyúttal szükségességi-arányossági teszt alkalmazását jelenti.

A „fontos közérdekből szükséges" adattovábbítások közigazgatási szervek közötti adattovábbításokra vonatkoznak, mely esetre az irányelv (58) preambulum-bekezdése az adó- vagy vámigazgatási szervek, vagy a társadalombiztosítási ügyekben illetékes hivatalok közötti nemzetközi adattovábbításokat emeli ki. A munkacsoport szerint ezen kivétel alapján pénzügyi felügyeleti szervek kooperációja keretében is történhet adattovábbítás. Lényeges korlátja e jogalapnak az, hogy ahhoz minősített közérdeket követel meg az irányelv, mivel az adattovábbítás „fontosságát" rögzíti. A másik ilyen kivétel a külföldi hatósági, továbbá bírósági eljáráshoz, illetve perhez szükséges adattovábbításokat foglalja magában.

Az érintett létfontosságú érdekeinek védelme miatt szükséges adattovábbításokat az irányelv (31) preambulum-bekezdése szűken határozza meg, mivel azt az érintett élete szempontjából alapvető érdekek védelme indokából lehet elvégezni, melynek példája az egészségügyi dokumentáció sürgős továbbítása lehet az egészségügyi kezelés szerinti nem biztonságos országba, feltéve, hogy veszélyhelyzet áll fenn.

Az irányelv végül lehetővé teszi az adattovábbítást olyan nyilvántartásból, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll. Ez a kivétel azt szolgálja, hogy egy tagállamban nyilvános regiszter (pl. cégnyilvántartás)

ne akadályozza az adattovábbítást csupán amiatt, hogy a betekintő személy harmadik országban található. Ez a kivétel – amint azt az irányelv (58) preambulum-bekezdése is megerősíti – azonban csupán egyedi betekintésre vonatkozik és tömeges adattovábbítás alapjául nem szolgálhat.

4. A NEMZETKÖZI ADATTOVÁBBÍTÁS MAGYAR SZABÁLYOZÁSA

Magyarországon az európai adatvédelmi irányelv – közöttük a nemzetközi adattovábbításokra vonatkozó szabályok – átültetését a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (régi adatvédelmi törvény, Avtv.) biztosítja, melyet 2012. január 1. napjától az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (új adatvédelmi törvény) szabályozása vált fel.[22]

4.1. Az adatvédelmi törvény hatálya

A nemzetközi adattovábbítással kapcsolatos hazai szabályok alkalmazásának első lépcsője annak megállapítása, hogy azok nemzetközi kontextusban milyen esetben irányadók egy külföldi adattovábbításra. Ez a magyar adatvédelmi törvény hatályával kapcsolatos rendelkezések vizsgálatát követeli meg.

Az adatvédelmi törvény hatályával kapcsolatos rendelkezések jelenleg az Avtv. 1/A. § (1) bekezdésében és 4/A. § (6) bekezdésében találhatóak. A hazai szabályozás – az irányelv szabályozásával,[23] illetőleg a 29. számú adatvédelemi munkacsoport alkalmazandó jogról szóló állásfoglalásával[24] ellentétben – kizárólag a territorialitás talaján áll. Az Avtv. 1/A. § (1) bekezdése értelmében *„e törvény hatálya a Magyar Köztársaság területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik."*[25]

A magyar adatvédelmi jogszabály hatályára vonatkozó szabály tág megfogalmazása azzal a gyakorlati következménnyel jár, hogy minden olyan esetben alkalmazásra jut(na) a magyar adatvédelmi jog és annak külföldi adattovábbítási szabályai (mégpedig akár egy másik tagállam nemzeti adatvédelmi jogával együttesen), mikor – akárcsak részben – magyar területet érint egy adatkezelési/adatfeldolgozási művelet, így különösen, ha Magyarország területéről vesznek föl személyes adatokat. Ez következik abból, hogy a magyar törvény hatályra vonatkozó rendelkezése – az irányelvvel szemben – az „*adatkezelési tevékenység keretére/kontextusára*" vonatkozó feltételt nem rögzít, ami a magyar adatvédelmi törvény hatályának és alkalmazásának univerzális értelmezése felé nyitja meg az utat. A hatályra vonatkozó magyar rendelkezések tehát az irányelv kontextusában felesleges túlszabályozást okoznak, ami nem kívánatos eredmény a harmonizált európai adatvédelmi jog hatálya alatt.

Ezt meghaladóan az adatvédelmi törvény a Magyarországon letelepedési hellyel rendelkező adatfeldolgozó megbízása esetében, vagy Magyarországon lévő – és nem Európai Unió területén átmenő adatforgalom célját szolgáló – eszközt felhasználó külföldi adatkezelő esetében szintén a magyar törvényt rendeli alkalmazni.

Megjegyzendő, hogy az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény hatályra vonatkozó szabályai [2. § (1)–(3) bekezdései] a fenti Avtv.-ben rögzített rendelkezéseket gyakorlatilag módosítás nélkül vették át. Megállapítható tehát, hogy a jogalkotó az új adatvédelmi törvényben elmulasztotta megteremteni az adatvédelmi irányelv szabályaival való összhangot és nem vette figyelembe a 29. számú adatvédelmi munkacsoport alkalmazandó jogról szóló állásfoglalását sem.

4.2. Az adattovábbítás fogalma

A régi és az új adatvédelmi törvény az értelmező rendelkezések között egyaránt meghatározza az adattovábbítás fogalmát. Eszerint adattovábbításra kerül sor, amennyiben a személyes adatot meghatározott harmadik személy számára hozzáférhetővé teszik. Lényeges szűkítés azonban, hogy harmadik személy olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval. Tehát az érintett, az adatkezelő és adatfeldolgozó közötti továbbítások esetében – belföldön – nem az adattovábbításra vonatkozó rezsim irányadó illetőleg nem minősül adattovábbításnak éppen ezért az adatkezelő és adatfeldolgozó közötti adatforgalom sem. További szűkítés, hogy az EGT-államokba irányuló adattovábbítást – összhangban az irányelv szabályozásával – úgy kell tekinteni, mintha a Magyar Köztársaság területén belüli adattovábbításra kerülne sor.

4.3. Az Avtv. nemzetközi adattovábbítási szabályai

Az Avtv. 9. § (1) alapján személyes adat (beleértve a különleges adatot is) az országból – az adathordozótól vagy az adatátvitel módjától függetlenül – harmadik országban lévő adatkezelő vagy adatfeldolgozó részére akkor továbbítható, ha

a) ahhoz az érintett *kifejezetten hozzájárult*, vagy

b) azt *törvény lehetővé teszi*, és a harmadik országban az átadott adatok kezelése, illetőleg feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

A személyes adatok megfelelő szintű védelme akkor biztosított, ha[26]

(i) az Európai Közösségek Bizottsága – külön törvényben meghatározott jogi aktus alapján – megállapítja, hogy a harmadik ország megfelelő szintű védelmet nyújt (lásd erről a jelen tanulmány 2. pontját), vagy

(ii) a harmadik országbeli adatkezelő vagy adatfeldolgozó az adatkezelés vagy adatfeldolgozás szabályainak ismertetésével igazolja, hogy az adatkezelés vagy adatfeldolgozás során megfelelő szinten biztosítja a személyes adatok védelmét, az érintettek jogait és azok érvényesítését, különösen, ha az adatkezelést vagy az adatfeldolgozást az Európai Unió Bizottsága külön törvényben meghatározott jogi aktusának megfelelően végzi (lásd erről részletesen a jelen tanulmány 3.1. és 3.2. pontjait).

A fenti adattovábbítási rendelkezések értelmezéséről az adatvédelmi biztos 2007. március 5. napján tájékoztatót bocsátott ki[27] „*a munkavállalói személyes adatok harmadik országba történő továbbításának szabályairól*" címmel, melynek lényegi és nem csupán munkavállalói adatok kezelésére irányadó megállapításai a következők.

A tájékoztató szerint a külföldi anyavállalat, illetve a harmadik országban található másik leányvállalata – a munkavállaló viszonylatában – harmadik személynek minősül és az oda irányuló adattovábbításokra a külföldi adattovábbításra vonatkozó rezsim irányadó. A tájékoztató elismeri, hogy a kifejezett hozzájárulás alapján történő adattovábbításhoz nem szükséges a megfelelő szintű védelem garanciáinak biztosítása, azonban munkavállalók esetében a hozzájárulás önkéntessége megkérdőjelezhető, ezért a tájékoztató szerint elvárható, hogy ebben az esetben a megfelelő védelem biztosítása is megtörténjen. Mivel a munkavállalói adatok kezeléséhez való hozzájárulás önkéntességének igazolása az adatkezelő kötelezettsége, ezért az adatvédelmi biztos gyakorlatában általánosan megfigyelhető tendencia – melyet a tájékoztató is alátámaszt –, hogy megfelelő szintű védelem biztosításának hiánya adott esetben a hozzájárulás önkéntességének megkérdőjelezéséhez is vezethet.

A harmadik országbeli adatfeldolgozók részére történő adattovábbítás esetén az adatfeldolgozásra vonatkozó törvényi szabályok (4/A. §) nem érintik az adatvédelmi törvény külföldi adattovábbításra vonatkozó szabályait, mivel a 9. § külön nevesíti az adatfeldolgozó részére történő adattovábbítást, melyhez emiatt – a belföldi adatfeldolgozási célú adattovábbításoktól eltérően – kifejezett hozzájárulás vagy törvényi felhatalmazás szükséges.[28] Tehát amennyiben általában adatfeldolgozás céljából történik az adattovábbítás, úgy nem szükséges ehhez az érintettek hozzájárulása, ez a szabály azonban harmadik országbeli adatfeldolgozók viszonylatában nem alkalmazható. Mint azt a tájékoztató rögzíti, az adatvédelmi törvény nem mentesíti az adatkezelőket azon kötelezettségük alól, hogy a munkavállalók kifejezett hozzájárulását kérjék adataik továbbításához, ha az harmadik országbeli adatfeldolgozókhoz történik.

Végül az adatvédelmi biztos tájékoztatója rögzíti, hogy munkavállalók személyes adatainak EGT-n kívüli államba való továbbítását *be kell jelenteni az adatvédelmi nyilvántartásba*. Az adatvédelmi törvény értelmében főszabály szerint minden adatkezelési tevékenységet be kell jelenteni az adatvédelmi biztos által vezetett nyilvántartásba, kivéve, ha a bejelentkezés alól a törvény kivételt tesz. Az Avtv. 30. § a) pontja értelmében azonban „*nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely az adatkezelővel munkaviszonyban, tagsági, tanulói viszonyban, ügyfélkapcsolatban álló személyek adatait tartalmazza*;". Az adatvédelmi biztos ezen kivételeket – hivatkozva a régi adatvédelmi törvény 28. §-hoz fűzött miniszteri indokolására – *szűken értelmezi*. Az adatvédelmi biztos szerint „*nem állnak*

fenn ugyanis a bejelentés alóli mentesség feltételei, ha az adatkezelés célja eltér a jogszabályokban minden munkáltató számára előírt adatkezelési céloktól. Mint a törvény indokolásában olvasható: »[...] e kivételekben meghatározott adatkezeléseket is be kell jelenteni, ha céljuk vagy tartalmuk több vagy más – például a továbbítást, a nyilvánosságra hozást vagy egyéb hasznosítást illetően [...]«."[29]

Az Avtv. adattovábbításra vonatkozó szabályai sajnálatos módon nem feleltek meg az irányelvi szabályoknak, ami számos esetben komoly gyakorlati problémát okozott. A magyar szabályozás sajátossága, hogy a megfelelő szintű védelem biztosítása mellett – illetve ezt meghaladóan – minden esetben *külön törvényi felhatalmazást* követelt meg a külföldre történő adattovábbításhoz. Ez azzal a következménnyel járt, hogy kifejezett törvényi engedély hiányában – mely felhatalmazással igen ritkán élt a magyar jog – kevés kivétellel, gyakorlatilag minden esetben az adatalany kifejezett hozzájárulásához volt kötve a nemzetközi adattovábbítás.

A magyar szabályozás sajátossága, hogy a megfelelő szintű védelem biztosítása mellett – illetve ezt meghaladóan – minden esetben *külön törvényi felhatalmazást* követelt meg a külföldre történő adattovábbításhoz. Ez azzal a következménnyel járt, hogy kifejezett törvényi engedély hiányában – mely felhatalmazással igen ritkán élt a magyar jog – kevés kivétellel, gyakorlatilag minden esetben az adatalany kifejezett hozzájárulásához volt kötve a nemzetközi adattovábbítás.

Megállapítható tehát, hogy a magyar jog alapján tapasztalható „hozzájárulás" misztifikálása – különösen a nemzetközi adattovábbítás kontextusában – többszörösen nem kívánt eredményhez vezetett, mikor az olyan összefüggésben is alkalmazásra került, mikor annak jogszerűsége megkérdőjelezhető. Ennek eklatáns példája a belső visszaélés-jelentési rendszerek nemzetközileg központosított létrehozása, amely vonatkozásban az adatvédelmi biztos gyakorlata a „feljelentett" munkavállaló kifejezett hozzájárulását (sic!) követelte meg egy jogsértés bejelentéséhez és kivizsgálásához.[30] Az Avtv. hozzájárulással, mint adatkezelési jogalappal kapcsolatos komoly hangsúlytévesztését erősítette az adatvédelmi biztos gyakorlata is, ami a 29. számú munkacsoportnak a hozzájárulás alkalmazását szűkítő és más jogalapok felhasználása (pl. jogos érdek) felé terelő megközelítését[31] a magyar viszonyokra is kiterjesztette, úgy azonban, hogy ennek az irányelvben létező jogszabályi feltételei (pl. a jogos érdeken alapuló jogalap) az Avtv. hibás hazai átültetése miatt nem álltak fenn.[32] Többszörösen igaz tehát a 29. számú adatvédelmi munkacsoport 15/2011. számú, a hozzájárulás fogalmáról kiadott állásfoglalásának megállapítása a magyar jogra, mely egyértelműsíti, hogy a hozzájárulás nem az egyetlen és nem is kizárólagos jogalapja az adatkezelésnek, mivel az irányelv öt további jogalapot is nevesít. A hozzájárulás tehát nem tekinthető minden esetben a legmegfelelőbb jogalapnak, illetve ez sem ad több manőverezési lehetőséget, mint az egyéb adatkezelési jogalapok, melyek az irányelv alapján léteznek.

4.4. Az új adatvédelmi törvény nemzetközi adattovábbítási szabályai

A 2012. január 1-jétől hatályos új adatvédelmi törvény abban az esetben teszi lehetővé az adattovábbítást harmadik országban adatkezelést folytató adatkezelő vagy adatfeldolgozást végző adatfeldolgozó részére, amennyiben

a) ahhoz az érintett kifejezetten hozzájárult, vagy

b) az adatkezelésnek az adatvédelmi törvény jogalap vonatkozásában (5. §-ban, illetve 6. §-ban) előírt feltételei teljesülnek, és a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

A fenti szabályozás régi adatvédelmi törvényhez képest bekövetkező változása, hogy abban az esetben teszi lehetővé a személyes adatok továbbítását, amennyiben a megfelelő szintű védelem biztosított és az adatkezelésnek megvan a megfelelő adatvédelmi törvény szerinti jogalapja. Amennyiben pedig a megfelelő szintű védelem nem biztosított az adattovábbítás célállomása szerinti harmadik országban, úgy az adattovábbítás kizárólag az adatalany kifejezett tájékozott hozzájárulása alapján engedélyezett.

Az új szabályozás pozitív hozadéka, hogy kibővítette az adattovábbítás lehetséges legitimált eseteit és azt immár nem szűkíti azt az adatalany kifejezett hozzájárulásának esetére, ami komoly előrelépést jelent a külföldre történő adattovábbítást korábbi indokolatlan és uniós jogba ütköző magyarországi korlátozásait illetően. Az új szabályozás tehát a törvényi jogalapot meghaladóan minden olyan esetben megengedi az adattovábbítást az EGT területén kívülre, amennyiben az adatkezelés megfelelő jogalapja vonatkozásában teljesülnek az adatvédelmi törvény feltételei, ami jóval tágabb a korábbi, csak törvényi jogalapon megengedett adattovábbításoknál. 2012. január 1. napjától abban az esetben is lehetséges személyes adatot külföldre továbbítani – feltéve, hogy a megfelelő szintű védelem biztosított –, amennyiben ahhoz jogos érdek fűződik (ún. méltányossági jogalapon), feltéve, hogy

– az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna; és

– az adatkezelés az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll;

vagy abban az esetben, ha a személyes adat felvételére korábban az érintett hozzájárulásával került sor és

– az adatkezelés jogi kötelezettség teljesítése céljából, vagy jogos érdekének érvényesítése céljából szükséges; és

– ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Ez utóbbi két esetben az adattovábbításra külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is sor kerülhet.

Rögzítendő azonban, hogy a jogos érdek alapján történő adattovábbítás feltételei jóval szűkebben kerültek meghatározásra az irányelv által meghatározottnál, mivel ahhoz szigorú feltételek igazolását követeli meg az adatvédelmi törvény. Így e jogalapra támaszkodás érdekében – az adatkezelő bizonyítási terhe mellett – annak igazolása szükséges, hogy a hozzájárulás beszerzése lehetetlen vagy aránytalan költséggel járna, illetve szükségességi-arányossági követelmény érvényesítését teszi kötelezővé, melynek feltételeit a 29. számú adatvédelmi munkacsoport és a tagállami adatvédelmi hatóságok gyakorlata alapján egyébként is szűken kell értelmezni.

Az adattovábbítás új magyar szabályozása sajnálatos módon több szempontból sem felel meg az irányelv rendelkezéseinek, mivel megfelelő szintű védelmet nem biztosító országokba az adattovábbítást – az irányelv 26. cikk (1) bekezdésében foglalt jogalapoktól eltérően – kizárólag az adatalany kifejezett tájékozott hozzájárulására szűkíti, míg az irányelv 26. cikk (1) bekezdése a további jogalapok mellőzését (lásd a jelen tanulmány 3.3 pontját) csak konkrétan meghatározott esetek vonatkozásában teszi lehetővé.

Másrészről az új törvény vonatkozásában komoly visszalépést jelent, hogy a korábbi adatvédelmi törvénynél jóval szűkebben határozza meg a „*megfelelő szintű védelem*" körét és azt kizárólag azokra az esetekre korlátozza [lásd a törvény 8. § (2) bekezdése], mikor a megfelelő szintű védelmet

a) az Európai Unió kötelező jogi aktusa megállapítja, vagy

b) a harmadik ország és Magyarország között az érintetteknek az adatvédelmi törvényben foglalt jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban.

Az Európai Unió kötelező aktusa csak ún. biztonságos országok vonatkozásában (lásd részletesen erről a jelen tanulmány 2. pontját), továbbá [a 3.1 pontban már bemutatott, irányelv 26. cikk (4) bekezdése alapján elfogadott] adattovábbítási általános szerződési feltételek tekintetében állapítja meg a megfelelő szintű védelem biztosítását, míg ebből a körből az adattovábbításra vonatkozó egyedi (*ad hoc*) szerződéses feltételek, továbbá a kötelező erejű vállalati szabályok (lásd 3.2 pontot) teljes egészében kimaradtak. 2012. január 1. napjától tehát az új magyar adatvédelmi szabályozás az irányelv 26. cikk (2) bekezdése alapján nem biztosítja az *ad hoc* szerződési feltételek, továbbá a BCR-ok alkalmazását, illetve nem garantálja ezek megfelelőségét, amely komoly visszalépésként értékelhető a korábban hatályos szabályozáshoz képest. Mivel a Nemzeti Adatvédelmi és Információszabadság Hatóság részéről hiányzik az adattovábbítások engedélyezésének irányelv szerinti egyedi jogalapja,[33] ekként a magyar jogban annak lehetősége is hiányzik, hogy Magyarország a 3.2. pontban már bemutatott MRP eljáráshoz szintén csatlakozni tudjon. A fenti változások egyben azt is jelentik, hogy 2012. január elsejétől a kötelező erejű vállalati szabályok alapján végzett, illetve egyedi adattovábbítási szerződéseken alapuló adattovábbítások esetében át kell térni az általános szerződési feltételek alkalmazására, ugyanis annak hiányában az adattovábbítás a továbbiakban kizárólag az adatalany kifejezett hozzájárulása alapján lehetséges (feltéve, hogy az adattovábbítás

címzettje szerinti ország nem biztonságos, illetve nem biztosít megfelelő szintű védelmet).

Az adatfeldolgozási célú adattovábbításokat illetően az új adatvédelmi törvény szintén komoly változást nyújt. A külföldi adatfeldolgozóhoz történő adattovábbítás kifejezett tájékozott hozzájárulás alapján vagy abban az esetben lehetséges, amennyiben megfelelő szintű védelem biztosítása megtörténik és az adatkezelés egyébként megfelelően legitimált az adatvédelmi törvény alapján. Az új törvény adatfeldolgozásra vonatkozó szabályai a 2010/87/EU bizottsági határozat szerinti adattovábbítási szerződési feltételek hazai alkalmazásában sajnálatos módon és előreláthatóan továbbra is komoly gyakorlati problémákat fog okozni, mivel a hivatkozott bizottsági határozat kifejezetten engedélyezi a külföldi adatfeldolgozó részéről további adatfeldolgozó (sub-processor) igénybevételét, míg ugyanerre az új adatvédelmi törvény 10. § (2) bekezdése[34] elvileg nem nyújt lehetőséget, amely szabály nem csupán idejétmúlt, de indokolatlan és a multinacionális vállalatok struktúráját figyelembe véve gyakorlatilag betarthatatlan is.[35]

Végül kiemelendőek az adattovábbítással kapcsolatos bejelentési/nyilvántartási követelmények az új adatvédelmi törvény alapján. Ebből a szempontból megállapítható, hogy a törvényalkotó – amellett, hogy komoly adminisztratív terheket teremtett az adatkezelők részére az adatvédelmi nyilvántartással kapcsolatosan – a korábbi kivételszabályok új törvénybe történő változatlan átemelésével elmulasztotta azok alkalmazásának egyértelmű tisztázását. Éppen ezért sajnálatos módon továbbra sem egyértelmű, hogy a személyes adatok külföldre történő továbbítását be kell-e jelenteni az adatvédelmi nyilvántartásba. Ebben a vonatkozásban támpontot az adatvédelmi törvénnyel kapcsolatos javaslat törvényhozási részletes vitáján Országgyűlésben elhangzottak adhatnak, melyen az előterjesztő részéről elhangzott, hogy az adatvédelmi biztos bejelentésekkel kapcsolatos – fentebb bemutatott – gyakorlatán nem kívántak módosítani. Ennek megfelelően feltehetően irányadó marad az adatvédelmi biztos tájékoztatójában foglalt jogértelmezés a 2012. január 1. napjától felálló Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatában is, ami a külföldre történő adattovábbítások esetében (amennyiben az munkavállalói vagy ügyfél adatokra vonatkozik), illetve a korábbi hozzájárulást követően jogos érdek alapján történt adattovábbítások vonatkozásában nyilvántartási bejelentést követel meg.

Kiemelendőek az adattovábbítással kapcsolatos bejelentési/nyilvántartási követelmények az új adatvédelmi törvény alapján. Ebből a szempontból megállapítható, hogy a törvényalkotó – amellett, hogy komoly adminisztratív terheket teremtett az adatkezelők részére az adatvédelmi nyilvántartással kapcsolatosan – a korábbi kivételszabályok új törvénybe történő változatlan átemelésével elmulasztotta azok alkalmazásának egyértelmű tisztázását.

5. KÖVETKEZTETÉSEK ÉS KITEKINTÉS

Az európai adatvédelmi irányelv felülvizsgálata hosszú ideje napirenden van. E folyamat 2010. november 4. napjával fontos állomásához jutott, mivel az Európai Bizottság ekkor tette közzé az európai adatvédelmi irányelv módosításával kapcsolatos koncepcióját,[36] melyben a nemzetközi adattovábbításokkal kapcsolatosan az adatvédelem nemzetközi dimenziójának erősítését tűzte ki. A Bizottság elismerte, hogy a nemzetközi adattranszferek mindennapossá váltak, gyakorlatilag irrelevánsnak tekinthető az adat kezelésének fizikai helye, mivel ugyanazon szervezet egyidejűleg több országban található szerveren is tárolhat személyes adatokat. A Bizottság legfontosabb törekvése, hogy a továbbiakban is fenntartsa az Európai Unió adatvédelemhez fűződő jog érvényesítésével kapcsolatos vezető szerepét, mely vonatkozásban a nemzetközi adattovábbítással kapcsolatos szabályozás kulcsszerepet játszik.

A Bizottság hivatkozott az Európai Bíróság Lindqvist ügyben meghozott határozatára,[37] ami megerősíti, hogy az európai adatvédelmi jog teljes harmonizációt valósít meg a tagállamok viszonylatában. Ennek ellenére számos komoly eltérés tapasztalható a tagállami adatvédelmi jogok között, melynek egyik oka, hogy az irányelv komoly manőverezési lehetőséget ad a tagállamoknak, másrészről a tagállamok sokszor hibásan ültették át az irányelv rendelkezéseit, ami a nemzetközi társaságok számára jelentős adminisztratív terheket okoz. Éppen ezért uniós szinten elkerülhetetlen a további harmonizáció biztosítása.

A nemzetközi adattovábbítással kapcsolatos szabályok azért jelentősek, mert a „megfelelő szintű védelem" megléte esetén gyakorlatilag megnyitja a lehetőséget a személyes adatok szabad forgalma előtt. A probléma a megfelelő szintű védelem elismerésével, hogy ennek kritériumai a Bizottság részére nincsenek pontosan rögzítve. Így a Bizottság mellett a tagállamok is jogosultsággal rendelkeznek ennek megítélésében, ami tagállamonként eltérő gyakorlatot is jelenthet, így az a veszély is előállhat, hogy tagállamonként eltérően ítélik meg az adott harmadik ország által az érintettek számára biztosított adatvédelem szintjét. A másik probléma, hogy a Bizottság adattovábbítási általános szerződési feltétel csomagjai (Model Clauses) nem alkalmazhatóak nem szerződéses szituációkban, így különösen mikor hatóság részére szükséges személyes adatokat továbbítani. Végül a Bizottság elismerte, hogy ugyanazon vállalatcsoporthoz tartozó vállalatok közötti jogszerű személyesadat-továbbítás hasznos eszközét jelenthetik az önszabályozás formájában kidolgozott egyéb eszközök, mint például a kötelező erejű vállalati szabályok (BCR), melyek további megerősítése és egyszerűsítése szükséges lehet. A Bizottság ugyanis kiemelt fontosságúnak tartja, hogy nemzetközi szinten fenntartsák az Európai Unió vezető szerepét a személyes adatok védelmének nemzetközi biztosításában.

A fent jelzett európai fejlemények fényében kérdéses, hogy ezen 2010. év végén kommunikált elvárásoknak mennyiben tett eleget a 2011 júniusában egy napos társadalmi konzultációt (sic!) követően és törvényhozási gyorsvágtában elfogadott információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, illetve annak külföldre történő adattovábbítással kapcsolatos szabályozása. Annak elismerése mellett, hogy az új rendelkezések immár egy élhetőbb szabályozást teremtettek – melyre a hatósági bírságolás lehetőségének egyidejű megteremtése mellett égető szükség volt –, lényeges előrelépésként értékelhető a nemzetközi adattovábbítás vonatkozásában a hozzájárulás hibásan túlmisztifikált koncepciójával való szakítás.

Ezzel szemben a „megfelelő szintű védelem" új adatvédelmi törvény szerinti szabályozása *komoly és indokolatlan visszalépést* jelent az Avtv. 9. § (2) bekezdésében rögzített rendezéséhez képest. Így Magyarország számára hátrányt okoz az a megközelítés, amellyel az adatvédelmi önszabályozás progresszív eszközét, a kötelező erejű vállalati szabályok alkalmazásának lehetőségét negligálta a jogalkotó, továbbá a jövőben immár az egyedi *(ad hoc* adattovábbítási szerződéses eszközök alkalmazását sem ismeri el a magyar jog. Mindez ugyanis azzal a következménnyel jár, hogy multinacionális vállalatok – Magyarország vonatkozásában – a megfelelő szintű védelem biztosítása érdekében költséges külön-utas megoldásokra, továbbá nyilvántartási bejelentés megtételére kényszerülnek, ami csökkenti többek között a magyar gazdaság versenyképességét más európai országokkal szemben. A megoldást a jelen problémára az jelentheti, ha a magyar jogalkotó törvénymódosítással a jövőben megteremti annak lehetőségét, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóság a megfelelő szintű védelem értékelését egyedileg – határozati aktussal – maga is elvégezhesse, amely lehetővé tenné, hogy Magyarország az adatvédelmi hatóságok nemzetközi adattovábbítással kapcsolatos szorosabb együttműködésében és az önszabályozó adatvédelmi megoldások támogatásában részt vehessen.

1 Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.)

2 Lásd ECJ Case C-101/01, 6 November 2003, Criminal proceedings against Bodil Lindqvist, 96. sarokpont első mondatát „The harmonisation of those national laws is therefore not limited to minimal harmonisation but amounts to harmonisation which is generally complete"

3 A törvényt az Országgyűlés 2011. július 11.-i ülésén fogadta el és az a Magyar Közlöny 2011. július 26-i számában került kihirdetésre.

4 A tagállami adatvédelmi hatóságok konzultatív szerve, ami különleges szerepet játszik az adatvédelmi irányelv értelmezésében.

5 WP 4 (5020/97) „Munkaanyag a személyes adatoknak harmadik országokba irányuló átadásával kapcsolatos elsődleges orientációról – a megfelelőség értékelésének lehetséges útjai", a munkacsoport által 1997. június 26-án elfogadott vitaanyag.

6 Lásd irányelv, 25. cikk (6) bekezdés

7 PNR (passanger name record) – az utas-nyilvántartási adatok szükségesek ahhoz, hogy a légitársaságok az utazási szolgáltatásaikat nyújthassák. A légitársaságok a légijáratok utasairól az utazásra és a helyfoglalásra vonatkozóan bizonyos információkat gyűjtenek, mint például az utas neve, elérhetőségei, útvonallal kapcsolatos részletek, a hitelkártya száma, vagy akár különleges személyes adatok is ide tartozhatnak mint az utazással kapcsolatos speciális/egészségügyi vagy akár vallási szükségletek. Ezen adatokat a foglalás során veszik föl az ügyféltől, illetve továbbítják azon légitársaságok részére, akikkel az utas utazik.

8 A 2004-ben megkötött EU–USA PNR egyezmény – ami indulást követő 15 percen belül 34 fajta adatkategória továbbítását tette kötelezővé a légitársaságoknak az Egyesült Államok Vámügyi és Határvédelmi Irodája részére – biztonságos kikötőt biztosított a PNR adatoknak, mellyel kapcsolatosan az Európai Bizottság megállapította, hogy az ilyen adattovábbítások az uniós jognak megfelelő szintű védelmet biztosítanak. Ezt az egyezményt az Európai Bíróság 2006. május 30-án érvénytelenítette (C-317/04 és C-318/04) arra való hivatkozással, hogy hiányzott az Európai Bizottság felhatalmazása annak megkötésére, mivel a szabályozott adattovábbításra közbiztonsági okból került sor, ami pedig az európai adatvédelmi irányelv hatályán kívül esett. Ezt követően 2007 júliusában újabb PNR szerződést kötöttek az USA-val. Hasonló egyezmények vannak hatályban Ausztráliával és Kanadával is, továbbá egyes tagállamok szintjén kétoldalú egyezmények szabályoznak, melyeket az EU egy uniós szintű egységes egyezménnyel törekszik felváltani.

9 Európai Bizottság 2000. július 26-i 2000/520/EK határozata (Hivatalos Lap L 215, 25/08/2000 o. 0007 – 0047)

10 Mivel csak vállalatok lehetnek alanyai e programnak, NGO-k ebben értelemszerűen nem vehetnek részt, így ezeknek az alanyoknak más adattovábbítási megoldást kell alkalmazniuk.

11 A Safe Harbor lista hozzáférhető és nyilvánosan kereshető a https://safeharbor.export.gov/list.aspx link alatt.

12 2010. áprilisban a német düsseldorfi kör (Düsseldorfer Kreis) olyan tartalmú nyilatkozatot bocsátott ki, hogy Németországból exportált adatok esetében – amennyiben adattovábbításra a Safe Harbor keretén belül kerül sor – az exportáló felelőssége, hogy meggyőződjön arról is, hogy az importáló Safe Harbor önminősítése nem pusztán deklaráció, hanem az valóban végrehajtásra kerül. Ezzel kapcsolatban komoly vita lángolt fel arról, hogy Németország e gyakorlata szembe megy-e az uniós joggal, mivel a megfelelő védelmi szint biztosításának bizottsági elismerését tagállami szinten nem lehet vitatni (igaz, az irányelv létesített egy mechanizmust, mellyel a tagállam értesítheti a Bizottságot és a többi tagállamot arról, ha úgy véli, hogy egy ország nem biztosít megfelelő szintű védelmet).

13 Lásd erről részletesen WP 12: „Személyes adatok továbbítása harmadik országok részére az EU adatvédelmi irányelve 25. és 26. cikkének alkalmazásával", a munkacsoport által 1998. július 24-én elfogadott munkaanyag IV. része; http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf, [2011. október 10.]

14 Ezt a Bizottság 2004/915/EK határozata módosította.

15 A tagállamok engedélyezhetik a személyes adatok olyan harmadik országba irányuló továbbítását vagy továbbítás-sorozatát, amely a 25. cikk (2) bekezdése értelmében nem biztosít megfelelő szintű védelmet, amennyiben az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében; ilyen garanciát jelenthetnek elsősorban a megfelelő szerződési feltételek. Mint azt az Európai Bizottság több jelentése elismeri, a tagállamok nem tesznek eleget ezen kötelezettségüknek. Lásd Commission Staff Working Document on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC) SEC(2006) 95; http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/sec_2006_95_en.pdf, [2011. október 10.]

16 Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 03.06.2003, MARKT/11639/02/EN

17 WP 107: Vélemény a közös állásfoglalások kiadására vonatkozó együttműködési eljárás meghatározása a vállalkozásokon belül kötelezően alkalmazandó belső adatvédelmi garanciák megfelelősége érdekében

18 WP 133 Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; WP 153, WP 154, WP 155

19 A lezárt kooperációs eljárásokat figyelembe véve bizonyos koncentráció figyelhető meg a vezér-hatóságok kiválasztásában, mivel eddig az ICO (Egyesült Királyság) nyolc ilyen eljárást folytatott le, a CNIL (Franciaország) hatot, míg Luxemburg adatvédelmi hatósága egyet. További adatvédelemi hatóságok ilyen eljárást vezérhatóságként nem folytattak. Forrás: List of companies for which the EU BCR cooperation procedure is closed, Article 29 Working Party http://ec.europa.eu/justice/ policies/privacy/binding_rules/bcr_cooperation_en.htm, [2011. október 10.]

20 Lásd részletesen WP 133.

21 Ezek az országok 2011 októberében: Ausztria, Belgium, Bulgária, Ciprus, Cseh Köztársaság, Franciaország, Németország, Izland, Írország, Olaszország, Lettország, Liechtenstein, Luxemburg, Málta, Hollandia, Norvégia, Szlovénia, Spanyolország és az Egyesült Királyság

22 Az adatvédelmi törvényt meghaladóan – ami az adattovábbításra vonatkozó általános szabályokat rögzíti – számos szektor-specifikus jogszabály (hitelintézeti törvény, biztosítási tevékenységről szóló törvény stb.) szabályozza a külföldre történő adattovábbítások és kiszervezések speciális feltételeit, ezek vizsgálata azonban meghaladja jelen tanulmány vizsgálati kereteit.

23 Az európai adatvédelmi irányelv 4. cikk (1) bekezdése értelmében: „*A személyes adatok kezelésére minden tagállam az ezen irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza, amennyiben:*
a) az adatkezelést a tagállam területén az adatkezelő egy telephelye tevékenységeinek keretében végzik; amennyiben ugyanaz az adatkezelő több tagállam területén is letelepedett, meg kell tennie a szükséges intézkedéseket annak biztosítása érdekében, hogy szervezeteinek mindegyike megfeleljen az alkalmazandó nemzeti jog által megállapított kötelezettségeknek;
b) az adatkezelő nem valamely tagállam területén telepedett le, hanem olyan helyen, ahol a nemzetközi közjog értelmében saját nemzeti jogát kell alkalmazni;
c) az adatkezelő nem telepedett le a Közösség területén, és a személyes adatok kezelése céljából *gépi vagy más olyan eszközt alkalmaz, amely a fenti tagállam területén található, kivéve, ha ezt az eszközt kizárólag a Közösség területén átmenő adatforgalom céljára használják.*

24 WP 179, 8/2010. számú vélemény az alkalmazandó jogról 2010. december 16., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_hu.pdf, [2011. október 10.]

25 A törvény eme szakaszának miniszteri indokolása szerint: „*indokolt ezért – figyelembe véve az Irányelv megfelelő rendelkezéseit (4. cikk, 25. cikk) is – a törvény személyi, tárgyi és területi hatályát pontosan meghatározni. Ennek megfelelően a módosítás kimondja, hogy a törvény hatálya a Magyar Köztársaság területén folytatott minden adatkezelésre és adatfeldolgozásra kiterjed, tekintet nélkül az adatkezelő vagy adatfeldolgozó állampolgárságára, székhelyére vagy lakóhelyére.*"

26 Személyes adatok megfelelő szintű védelme abban az esetben is biztosított, ha a harmadik ország és a Magyar Köztársaság között az érintetteknek az adatvédelmi törvény szerinti jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban. Ezen rendelkezésnek azonban gyakorlati jelentősége nincsen.

27 Lásd http://abiweb.obh.hu/abi/index.php?menu=1225&nyomtat=1, [2011. október 10.]

28 Lásd ezzel egyezően ABI-1925-I-2010-2. sz. állásfoglalást.

29 A bejelentési kötelezettség adatvédelmi biztos gyakorlatában elismert további esetei a következők: „*A munkavállalók személyes adatainak továbbítását, mivel az adattovábbítás címzettje az adatok tekintetében adatkezelővé válik, az adatvédelmi nyilvántartásba be kell jelenteni. Szintén bejelentési kötelezettség alá esik a munkaviszonnyal közvetlenül össze nem függő adatgyűjtés, így például a külföldi munkavállalók vízumügyintézése, külföldi anyavállalathoz történő továbbítása vagy munkavállalói részvényprogramhoz kapcsolódó adatkezelés.*" … „*Nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely az adatkezelővel munkaviszonyban álló személyek adatait tartalmazza. Be kell azonban jelenteni az adatkezelést, ha a munkáltató a munkavállalók személyes adatait más szervhez, vagy külföldre továbbítja. Szintén bejelentési kötelezettség alá esik a munkaviszonnyal közvetlenül össze nem függő adatgyűjtés, így például a külföldi munkavállalók vízum ügyintézése, külföldi anyavállalathoz történő továbbítása, vagy munkavállalói részvényprogramhoz kapcsolódó adatkezelés.*" (Adatvédelmi biztos 2006-os beszámolója) „*Az Avtv. 30. § a) pontjában meghatározott kivételek között (ti. munkavállalói adatok kezelése) megjelölt esetekben is „be kell jelenteni az adatkezelést az adatvédelmi nyilvántartásba, ha az adatokat az adatkezelő más személy, vagy szerv részére hozzáférhetővé teszi, nyilvánosságra hozza, vagy egyébként az eredetitől eltérő célra használja fel.*" (Lásd adatvédelmi biztos 2007-es beszámolóját). Tehát az adatvédelmi biztos egyértelmű gyakorlata alapján be kell jelenteni az adatkezelést illetve adattovábbítást, ha meghaladja a Munka Törvénykönyve hatálya alá tartozó adatkezeléseket. Mivel a főszabály a bejelentési kötelezettség, ezért abban az esetben, ha egy adatkezelés nem sorolható be teljes egészében valamely törvényi kivétel alá (pl. részben munkaviszonyon alapul az adatkezelés, részben pedig nem), akkor a bejelentési kötelezettséget teljesíteni kell. Ezzel kapcsolatban rögzítendő, hogy az adattovábbítás címzettje (pl. az anyavállalat)

az adattovábbítással kapcsolatosan szintén adatkezelővé válik, tehát nem csupán az exportáló, hanem az adattovábbítás címzettje (az importáló) vonatkozásában is vizsgálni kell az Avtv. 30. § a) pontjában írt kivételszabály fennállását. Mivel az anyavállalat nem áll munkaviszonyban az adatalany munkavállalóval, ezért ő harmadik személynek minősül a munkáltató leánycég és a munkavállaló viszonyában, értelemszerűen a kivételszabály sem alkalmazható és a bejelentési kötelezettség fennáll.

30 Lásd ABI-652/K/2007-3. sz. ügyet

31 Lásd különösen WP 48, 5062/01/EN/Final, Section 10. Consent „*The Article 29 Working Party has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.*"

32 Az adatvédelmi biztos ebben a vonatkozásban nem ismerte el azt, hogy az Avtv. hibásan ültette volna át az irányelvet. ABI-652/K/2007-3 állásfoglalásban kérdésként merült fel, hogy a magyar Avtv. jogalap meghatározásával kapcsolatos és irányelv szabályozásánál szigorúbb rendelkezései kollízióban állnak-e egymással [ti. az adatkezelés az Avtv. szerint kizárólag törvény vagy hozzájárulás alapján legitimált és nincs lehetőség méltányosságon alapuló adatkezelésre a 7. cikk f) pontja alapján]. Az adatvédelmi biztos álláspontja szerint kollízió nem áll fenn, „*[a]z Irányelv 7. cikke ugyanis a tagállamok hatáskörébe utalja az adatkezelések jogalapjának meghatározását, a felsorolt adatkezelési jogalapok határain belül.*" Eme vita lezárásaként az új adatvédelmi törvény miniszteri indokolása tekinthető, ami az uniós jogba ütközés tényét elismerte.

33 Vö. Irányelv 26. cikk (2) bekezdése

34 10. § (2) „Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe."

35 Az adatvédelmi biztos 2010-re vonatkozó éves beszámolójában az uniós jog primátusára hivatkozva nem kifogásolta az ilyen kiszervezéseket, amennyiben arra a 2010/87/EU sz. bizottsági határozat alapján került sor.

36 A comprehensive approach on personal data protection in the European Union; COM(2010) 609 final, 4.11.2010; Lásd http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [2011. október 10.]

37 Case C-101/01

Rippel-Szabó Péter

A televíziós sportközvetítési jogok használatának engedélyezésére irányuló szerződések*

A) BEVEZETÉS

A televíziós sportközvetítési jogok engedélyezésére irányuló szerződések a közvetítési jogok jogtulajdonosainak egyik legfontosabb bevételi forrását jelentik. Így például a magyar első osztályú labdarúgó bajnokságban szereplő sportszervezetek televíziós jogdíjakból származó bevétele a 2010/11-es szezonban 0,37 millió euró volt, mely a 2011/12-es szezonban előreláthatólag 0,45 millió euróra növekszik.[1] Bár ezen összegek jócskán elmaradnak a nyugat-európai klubok bevételeitől, fontosságuk egyáltalán nem alábecsülendő. Az, hogy a televíziós sportközvetítési jogok értékesítése a jogtulajdonosok egyik legfontosabb bevételi forrását jelenti, több okra vezethető vissza. Egyrészt a fogyasztók sokkal inkább „nézik" a sporteseményt, mint hallgatják a közvetítést. Másrészt a vizuálisan történő érzékelés során a sportversennyel összefüggésben – elsősorban az érintettek által kötött szponzorálási és arculat-átviteli szerződéseknek köszönhetően – felbukkanó reklámok sokkal hatásosabban jutnak el a célzott fogyasztói körökhöz. A jogtulajdonosokkal szerződő médiaszolgáltatók pedig azért hajlandóak az átlagosnál magasabb összegeket fizetni a népszerű sportágak – egyébként korlátozott számban rendelkezésre álló – sportközvetítési jogaiért, mert más médiaszolgáltatókkal szemben csak értékes műsortartalommal vehetik fel a versenyt.[2]

Jelen tanulmány célja a tévés sportközvetítési jogok engedélyezésére irányuló szerződések gyakorlati – és helyenként jogelméleti – aspektusainak áttekintése e szerződés alapvető tartalmi rendelkezéseinek bemutatásán és elemzésén keresztül. Az alábbiakban meghatározásra kerül a sportközvetítési jog és a tanulmányban bemutatandó szerződés fogalma; a szerződő felek személyéhez és a jogok engedélyezéséhez kapcsolódó kérdések; a megállapodás megkötését megelőző pályázati kiírás jelentősége; továbbá a szerződés legfontosabb tartalmi elemei, így többek között a sportműsorszám elkészítésének és sugárzásának módja, valamint a szerződés hatálya és a kapcsolódó kizárólagosság kérdései is.

B) A SPORTKÖZVETÍTÉSI JOG ÉS A TELEVÍZIÓS SPORTKÖZVETÍTÉSI JOGOK HASZNÁLATÁNAK ENGEDÉLYEZÉSÉRE IRÁNYULÓ SZERZŐDÉS FOGALMA

Általánosabb megfogalmazásban a sportközvetítési jog az érintett sporteseménynek, sportversenynek, sportverseny-sorozatnak, azaz a sportverseny-szervezés ötletének és megszervezésének, a résztvevő személyeknek (sportolók, sportszervezetek, sportszakemberek, játékvezetők stb.), a sportteljesítményeknek, a sportlétesítményeknek, valamint a sportfelszereléseknek és sportruházatoknak az összességéből álló, vagyoni értékkel bíró forgalomképes kereskedelmi termék, mely meghatározott technikai eszközökkel a nyilvánosság számára közvetítésre kerül.[3]

A sportközvetítési jog az érintett sporteseménynek, sportversenynek, sportverseny-sorozatnak, azaz a sportverseny-szervezés ötletének és megszervezésének, a résztvevő személyeknek (sportolók, sportszervezetek, sportszakemberek, játékvezetők stb.), a sportteljesítményeknek, a sportlétesítményeknek, valamint a sportfelszereléseknek és sportruházatoknak az összességéből álló, vagyoni értékkel bíró forgalomképes kereskedelmi termék, mely meghatározott technikai eszközökkel a nyilvánosság számára közvetítésre kerül.

A tanulmány kereteinek megfelelő behatárolása végett a bemutatandó

A szerző ügyvédjelölt, az ELTE ÁJK meghívott előadója.