MISKOLCI EGYETEM
ÁLLAM- ÉS JOGTUDOMÁNYI KAR
DEÁK FERENC ÁLLAM- ÉS JOGTUDOMÁNYI DOKTORI ISKOLA

DR. MAKSÓ BIANKA

A kötelező erejű vállalati szabályok (Binding Corporte Rules) a megújuló európai adatvédelmi jogban

(PhD értekezés)

Deák Ferenc Állam- és Jogtudományi Doktori Iskola

A doktori iskola vezetője: Prof. Dr. Bragyova András

A doktori program címe: A magyar állam- és jogrendszer jogtudomány továbbfejlesztése, különös tekintettel az európai jogfejlődési tendenciákra

Tudományos vezető: Prof. Dr. Majtényi László DSc.
tanszékvezető egyetemi tanár

MISKOLC
2019

DOI: 10.14750/ME.2019.022

Az Emberi Erőforrások Minisztériuma ÚNKP-17.3. kódszámú
Új Nemzeti Kiválóság Programjának támogatásával készült.

A kézirat lezárásának dátuma: 2019. március 10.

Hivatkozási forma:
MAKSÓ (2019)
Maksó Bianka: A kötelező erejű vállalati szabályok (Binding Corporte Rules) a megújuló európai adatvédelmi jogban, PhD értekezés, Miskolci Egyetem, Miskolc, 2019.

DOI: 10.14750/ME.2019.022

A TÉMAVEZETŐ AJÁNLÁSA

Dr. Maksó Biankát egyetemi hallgató kora óta ismerem, mondhatom tehát, tanítványom, ma viszont, ezen túl, már kollégaként is tekintek rá. A tehetség és a szorgalom nem mindig jár kéz a kézben. A magas intellektus gyakran lustasággal, szerencsés esetben hasznos, máskor tévutakra vezető önfejűséggel párosul, aminthogy a közepes képességűeket pedig olykor segíti az átlag feletti szorgalom. Dr. Maksó Bianka inkább a kivételekhez sorolható szerencsés alkat, nála a tehetség és a tudásszomj, valamint a tudományos kutatás iránti alázat kéz a kézben együtt jár. Önfejűsége pedig önálló gondolkodás. Jól mutatja ezt ma is kiterjedt szakirodalmi tevékenysége, amely a publikációk számát, de azok minőségét is tekintve, már most jelentősen meghaladja PhD fokozat megszerzéséhez szükséges mértéket.

Kívánom, hogy ezeket a kutatói tulajdonságokat – noha ez manapság nem könnyű –, és az ettől nehezen elválasztható szakmai és személyes tisztességét is, Dr. Maksó Bianka őrizze meg.

***

Az alapvető jogok kritikusai az alapjogokra általában, így a személyes adatok védelmére is, gyakran úgy tekintenek, mint a jogági kidolgozottságot, szakmai precizitást nélkülöző, a jogrendszer belső logikai szerkezeteit fellazító ideologikus képződményekre. Ez a kritika általában is igazságtalan, másrészt konkrétan az adatvédelmet tekintve, a tárgy egyediségét nézve tarthatatlan is. A személyes adatok nemzetközi jogi jogrendje, de hazai szabályozása is, miközben a szabályozás egyúttal problematikus, súlyos megoldatlanságoktól terhes, mind általános, mind pedig szektorális tekintetben, kielégíti a legkényesebb dogmatikai igényeket is. Ennek következménye, hogy a joganyag, nem is beszélve a bírói jogról, terjedelmes, olykor részletező és benső ellentmondásoktól sem mentes.

DOI: 10.14750/ME.2019.022

Ebbe a környezetbe épül be napjainkba az Európai Unió Adatvédelmi Rendelete, amely közvetlen alkalmazhatósága folytán nem csak átalakítja az európai és a nemzeti jogrendeket, nem csupán szemléleti változásokat okoz, de hatályba lépésével azonnal felül is írta azokat. Volt is Európa-szerte és itthon is, nagy rémület. Nem ok nélkül, a most hatályba lépett szabályozás a jogalkalmazókat és a jogtudomány képviselőit jelentős kihívások elé állítja. Ebben a környezetben készült el Dr. Maksó Bianka értekezése.

Tegyük hozzá, hagyományosan is, és aktuálisan is az adatvédelmi szabályozás egyik legneuralgikusabb eleme a harmadik országokba történő adattovábbítás. Gyakorlatilag nehéz, elméletileg úgyszólván lehetetlen az adatalany alapvető jogainak és a globálissá váló piacgazdaság jogszerű érdekeinek összhangját kialakítani. Szokás emlegetni a témaválasztás újszerűségét. Itt ez nemcsak nyilvánvaló, de a hazai szakirodalomban abszolútnak mondható. Az értekezés a harmadik országokba történő adattovábbítás egy viszonylag új, az alkalmazás során félreértésekkel terhelt, és az adatvédelmi rendelet által újrakodifikált intézményét: a Kötelező Erejű Vállalati Szabályokat (Binding Corporate Rules) helyezi az elemzés középpontjába. A dolgozat fontos erényének tartom, hogy a Kötelező Erejű Vállalati Szabályok amúgyis szerteágazó problémáit nem önmagukban, hanem az alkotmányjogi, jogvédelmi összefüggéseken is túl, a problémahalmaz jogági komplexitásában tárgyalja. Miközben ez az értekezés kifejezetten jogi elemzést nyújt, a szerző, ha nem is explicit módon, ugyancsak kitér a társadalmi és a gazdasági környezet igényeire és érdekeinek közrehatására is. A probléma ugyanis az, hogy a harmadik országba történő adattovábbításnak, jogszerű és alapvetően gazdasági érdeket szolgálva, adott esetben van több (az érintett beleegyezésétől a transzatlanti forgalomban például a Privacy Shieldig) alkalmazható jogintézménye, illetve jogalapja. A Kötelező Erejű Vállalati Szabályok alkalmazhatóságát az alapjogok, a jogági szabályhalmaz és az üzleti érdek figyelembe vételének hálójában lehet feltárni.

DOI: 10.14750/ME.2019.022

Az értekezés figyelmes olvasója mindezen kérdésekre talál, persze nem végső, de fontos válaszokat. Ezzel az adatvédelem művelőinek és az üzleti világ képviselőinek továbbá a gyakorlatban dolgozó ügyvédeknek, az adatvédelmi ügyekre szakosodott jogi szakembereknek nyújthat komoly segítséget.

Budapest, 2018. június 26.

Dr. Majtényi László DSc.
tanszékvezető egyetemi tanár
témavezető

DOI: 10.14750/ME.2019.022

TARTALOM

DOI: 10.14750/ME.2019.022

DOI: 10.14750/ME.2019.022

DOI: 10.14750/ME.2019.022

DOI: 10.14750/ME.2019.022

I. FEJEZET
BEVEZETŐ GONDOLATOK

I.1. Az értekezés célja és tárgya

Miért készült el ez a disszertáció? Miért éppen most és miért éppen ebben a tárgyban? A PhD értekezés elkészítése a tudományos karrier kezdetének első olyan mérföldköve, amelyben a többéves kutatás önálló eredményei kaphatnak nyilvánosságot. Reményeim szerint ez az értekezés nemcsak személyes tudományos életutam első mérföldköve lesz, hanem egyfajta hiánypótló „kézikönyv" azoknak az olvasóknak, akik a kötelező szervezeti szabályozással (a továbbiakban a szakirodalomban általános elnevezése szerint a binding corporate rules rövidítéseként: BCR) mint a hazai adatvédelmi jogban előzmény nélküli jogintézménnyel kerülnek kapcsolatba.

Tudományos kutatásom tárgyát elsősorban konzulensi ajánlás és a piaci szféra adatvédelmi gyakorlata iránt érzett személyes érdeklődésem irányította az adatvédelmi reform és annak egy különleges, hazánkban alig ismert jogintézménye, a BCR vizsgálata felé. A nemzetközi szakirodalmi források csekély száma, a hazai irodalomban csak elvétve fellelhető említések, a hazai jogalkalmazói jó gyakorlat még alakuló állapota indokolta, hogy a BCR jogtudományi, komplex elemzését állítsam dolgozatom fókuszába, tekintettel arra is, hogy a BCR bevezetését a magyar jogrendszerbe egyes szerzők lehetetlennek tartották,[1] mégis a multinacionális gazdasági társaságok egyik kiemelten fontos adatkezelési eszközévé válhat.

A kutatásoknak, különösen a támogatásból megvalósulóké,[2] a versenyképes jogi környezet kialakítását kell szolgálnia.

[1] LIBER (2011) (1)

[2] Az Emberi Erőforrások Minisztériuma ÚNKP-17.3. kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

DOI: 10.14750/ME.2019.022

E szakmai és tudományos körben elsődleges, hogy helyesen válassza meg a jogi, társadalmi, kulturális és gazdasági igény követelte aktuális tárgyát és kérdéseit, majd bemutassa illetve javaslatot tegyen a helyes jogalkotási és jogalkalmazási illetve jogkövetési válaszokat illetően. Az általam kutatott témakör a személyes adatok védelméhez való jog, különösen a harmadik országba irányuló adattovábbítás jogi környezetének alakulása. Megjegyzem, nem csak számomra kellene égetően fontos témának lennie, hanem mindenkinek több odafigyeléssel kellene gondolnia rá, mivel egyes statisztikák[3] szerint 2013 óta több, mint 9 milliárd személyes adat veszett el vagy került jogosulatlan kezekbe, különösen a digitális közeg és az új technológiák alkalmazásának hatására. Ezzel persze nem azt mondom, hogy az új technológiák alapvetően rosszak és alkalmazásuk szükségképpen adatvédelmi incidensekhez vezet, hanem azt kívánom bizonyítani, hogy a jognak milyen új szemléletű válaszokat kell adnia a felvetődő újszerű adatvédelmi kérdésekre, különösen a harmadik országba irányuló adattovábbítások vonatkozásában.

Az információs önrendelkezési jog gyakorlásának súlypontja ma már kevésbé a személyes adataink feletti ellenőrzési jogosultság személyes gyakorlását jelenti, hanem inkább elvárás arra nézve, hogy az adatkezelő olyan magatartást tanúsítson, amellyel biztosítja a személyes adatok védelméhez való alapvető jog érvényesülését. Ezen az alapelvi elváráson nyugszik a 2018. május 25. napjától hazánkban is közvetlenül alkalmazandó Általános Adatvédelmi Rendelet (a továbbiakban: a szakirodalomban használatos elnevezés szerint a General Data Protection Regulation rövidítéseként: GDPR[4]) is.

[3] http://breachlevelindex.com/ A forrás egy adatbiztonsági szolgáltatásokat kínáló gazdasági társaság statisztikája. [2017. október 15.]

[4] Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) OJ L 119, 4.5.2016, p. 1–88.

DOI: 10.14750/ME.2019.022

Ebből az alapállásból kívánom a harmadik országba irányuló adattovábbítás szabályainak napjainkban zajló átfogó reformját és a BCR bevezetésének és jövőbeni alkalmazásának jogi kihívásait tudományos vizsgálat tárgyává tenni. A témaválasztást objektíve indokolja – a konzulensi ajánláson túl – a technológia fejlődése indukálta változó jogi környezet, a piaci szféra növekvő érdeklődése és a megfelelési kötelezettség.

A disszertáció célja olyan nemzetközi vonatkozásokat is felmutató kutatás eredményeinek bemutatása a személyes adatok védelme jogterületén, amely középpontjában az európai reformfolyamat eredményeként kulcsszerepet nyert, a harmadik országba irányuló adattovábbítás új szabályainak és a BCR magyarországi bevezetésének helyes alkalmazásának témái állnak. Ugyancsak célom az adatvédelmi szabályoknak megfelelni akaró és azt bizonyítani képes adatkezelők segítése, akik vállalkozáscsoportjuk számára BCR-t kívánnak létre hozni és alkalmazni. A kutatás egyik része jogalkotási szempontú, amely kiterjed a BCR anyagi jogi és a jóváhagyására vonatkozó hatósági eljárás eljárásjogi tudományos vizsgálatára, a további része a BCR-rel kapcsolatos végrehajtási feladatok tudományos elveinek és empirikus elemeinek feltérképezése, amelyet megelőz a pozitív jogi környezet elemzése és a jogintézmény fogalmának, tartalmának és funkciójának vizsgálata.

A jogterület ezen szektorális vizsgálata hozzájárulhat a hazánk előtt álló és napjainkban aktuális adatvédelmi jogi jogalkotási és jogalkalmazási feladatok megoldásához, a digitalizált gazdaság, benne az információs társadalom és a változó adatvédelmi trendek terjedésével járó kihívásoknak megfelelni tudó állam és hatékony közigazgatás kialakításához.

DOI: 10.14750/ME.2019.022

I.2. Az értekezés szerkezete

Az értekezésben a kutatás irányainak megfelelően a tématerület egyes szeletei egymásra épülve fejezetekre tagolódnak. Jelen bevezetést követően bemutatom a jogharmonizációs folyamatot, amely hazánkban zajlott le az adatvédelmi jog, különösen a harmadik országba irányuló adattovábbítások szabályozására vonatkozóan. Ezt követően napjaink jogegységesítési folyamatait vizsgálom, fókuszában a GDRP mint az adatvédelmi jog reformjának eredményeként megszületett közvetlen hatállyal bíró uniós jogforrás és annak a BCR-re vonatkozó rendelkezései. A fejezetben igazolni kívánom azt is, hogy a BCR nem csak a jogalkotó által megkonstruált jogi eszköz, hanem a piaci igényeken alapuló, az adatvédelmi reform tendenciájába illeszkedő új alkalmazási lehetőség. Ezt követően a pozitív jogi környezet elemzését végzem el akként, hogy alapul véve a közvetlenül alkalmazandó GDRP szabályait, a BCR helyét és szerepét vizsgálom, majd a hazai szabályozás és az Infotv. vonatkozó rendelkezéseit teszem a vizsgálat tárgyává.

A jogi környezet több szempontú és komplex megértését követően a BCR mint az értekezés központi elemét képező jogintézmény fogalmi elemzését végzem el, amely során megfogalmazásbeli, értelmezési és jogalkalmazási nehézségekre hívom fel az olvasó figyelmét az egyes fogalmi elemek egyenkénti bírálata során.

A BCR fogalmi eleme és érvényességi kelléke a hatósági jóváhagyása, helyesen engedélyezése is. Pozitív jogi környezet hiányában a vonatkozó fejezetben arra teszek kísérletet, hogy egy jóváhagyási eljárás modelljét készítsem el, és de lege ferenda javaslatot tegyek az eljárásjogi környezet kialakítására, annak egyes bonyolult kérdésinek megoldására.

DOI: 10.14750/ME.2019.022

Különösen fontos ezen eljárásjogi környezet kialakítása, mert egyrészt jelenleg csak soft law jellegű forrásokra tud támaszkodni a hatósági jogalkalmazás, másrészt meg fog élénkülni ezen eljárások száma hazánkban is. A disszertációban is elemzés alá vont határozatában a NAIH az adatkezelőt a vállalkozáscsoportjánál alkalmazott BCR jóváhagyásának kérelmezésére is kötelezte. A vizsgált határozat az első ezen a jogterületen, ezért is hangsúlyos annak helyes értelmezése.

A hatóság jóváhagyása a vállalkozáscsoport teljes adatvédelmi politikájának vizsgálatán alapul, amelynek a BCR törzsszövege képezi a központi elemét. E körben egy teljes fejezetet szentelek annak, hogy már jóváhagyott BCR-k tartalmát elemezzem, bemutatva az egyes pontokat egy modell-struktúra szerkezetére felfűzve.

Tekintettel arra, hogy a BCR jogi természete, a pontos tartalmi elvárások és a hatósági jóváhagyás számos megválaszolandó kérdést vetett fel, egy olyan stratégiai tervezési-elemzési módszer alkalmazását választottam a BCR analizálására, amely széles körben ismert és alkalmazott, ez a SWOT elemzés. A BCR előnyeit, hátrányait, az alkalmazásából eredő lehetőségeket és veszélyeket csoportosítva sorakoztattam fel szempontokat, amelyek segítségére lehetnek bármely adatkezelőnek akkor, ha a BCR alkalmazásáról kell döntenie.

A BCR nagy előnye, hogy a vállalkozáscsoport struktúrájára és tevékenységére lehet szabni, valamint bármely harmadik országba irányuló, vállalkozáscsoporton belüli adattovábbítás esetén megfelelő lehet. Ezzel szemben léteznek ország-specifikus megoldások, mint például az Adatvédelmi Pajzs az USA államai, vagy a CBPR az APEC tagállamok esetében, amely rendszerek tanúsításra épülő mechanizmussal kívánják a megfelelő védelmi szint biztosítását elérni.

DOI: 10.14750/ME.2019.022

Összehasonlítva a BCR-rel alapvető különbségek tapasztalhatók, jellemzően a BCR javára.

A komplex, jellemzően a tételes jogi szabályokon alapuló elemzéseket követően az értekezés lezárásaként az adatvédelmi jogot és annak alakulását alapjogi illetve jogelméleti megközelítésben helyezem el, hangsúlyozva, hogy a személyes adatok manapság a digitális közegben jelentős piaci értékekkel bíró javak, amelyek nemcsak az érintett számára bírnak jelentőséggel.

I.3. Az alkalmazott kutatási módszerek

A kutatás, különösen a BCR mint az értekezés szűken vett tárgya tekintetében rendelkezésre álló csekély számú szakirodalmi forrás és a tulajdonképpen hiányzó jogalkalmazói gyakorlat okán, alapvető kérdések megválaszolásán túl arra is kiterjedt, hogy a BCR hazai bevezetése és a jó gyakorlatok kialakulása hogyan valósítható meg, e körben de lege ferenda javaslatot tartalmaznak az egyes fejezetek. Azon túl, hogy a GDPR vonatkozó részének elemzése alapvető, elsődleges jogforrásként pozitív jogi ismeretek biztosít, a 29. cikk szerinti Adatvédelmi Munkacsoport[5] munkadokumentumai nyújtottak nélkülözhetetlen iránymutatást a kutatás eredményeihez.

[5] Az Adatvédelmi Munkacsoport az egyes tagállamok által kijelölt felügyelő hatóság képviselőjéből, az uniós intézmények és szervek nevében létrehozott szervek képviselőjéből, továbbá az Európai Bizottság egy képviselőjéből áll. Magyar tagja jelenleg Dr. Péterfalvi Attila, a Nemzeti Adatvédelmi és Információszabadság Hatóság elnöke. Az Európai Bizottsággal szoros együttműködésben lép fel minden nemzeti intézkedés és kérdés vonatkozásában, amely a személyek személyes adatai védelméhez való alapvető jogainak veszélyeztetésével, sérelmével járhat. Meghatározó szerepet játszik az uniós tagállamok és harmadik országok védelmi szintjének meghatározásában. Ajánlásokat tehet, megállapíthatja a megfelelő szintű adatvédelem hiányát, erről a Bizottságot értesíti. Az Adatvédelmi Irányelv 30. cikk (1) bekezdés a) pontja szerint az Adatvédelmi Munkacsoport megvizsgál minden, az Adatvédelmi Irányelv értelmében elfogadott nemzeti intézkedések alkalmazása körébe tartozó kérdéseket azok egységes alkalmazása érdekében, valamint a (3) bekezdés értelmében saját kezdeményezésére ajánlásokat tehet a személyes adatok közösségen belüli feldolgozása tekintetében a személyek védelmével kapcsolatban. Véleményeit és ajánlásait az uniós végrehajtási intézkedések megtételének végrehajtásához az Adatvédelmi Irányelv 31. cikkében foglaltak szerint az Európai Bizottság és a mellé felállított segítő bizottság részére továbbítja. Ezen hatásköri és eljárási szabályok mentén a Munkacsoport „Magyarázó dokumentumokat" (a továbbiakban: WP) bocsát ki, melyek normatív erővel nem bírnak, de az uniós és tagállami végrehajtáshoz nyújtanak követendő iránymutatást a nemzeti hatóságok és más érintett jogalanyok számára. Az Adatvédelmi Irányelv hatályon kívül helyezésére tekintettel az Adatvédelmi Munkacsoport megszűnt, helyét és szerepét az Európai Adatvédelmi Testület veszi át.

DOI: 10.14750/ME.2019.022

A szakirodalmi források a tárgykörben szinte kivétel nélkül csak idegen nyelven állnak rendelkezésre, a soft law jellegű források többsége sem érhető magyar nyelven. Így a kutatás a jogfogalmak olykor alapvető különbözősége, például a magánélet – privacy, vagy a cég – vállalkozás – szervezet – jogi személy, a hatósági eljárásban a hiánypótlás – módosítás viszonya kapcsán alapvető értelmezési és jogalkalmazási kérdések a hazai jogfogalmak szerinti átültetését és értelmezését kívánta meg.

A jogszabályi környezet, különösen a GDPR és a harmadik országba irányuló adattovábbításra vonatkozó jogi környezet elemzése analitikus, komparatív és kritikai szemlélettel készült, normatív módszertan alkalmazásával. A BCR magyar elnevezése és fogalmi elemeinek megnevezése, valamint a hatósági eljárás kategórizálása, a rendszertani elhelyezésére tett javaslat és az eljárás elnevezése vonatkozásában a jogszabályszövegek logikai, nyelvtani és rendszertani elemzésére is sor került. A BCR fogalmi megalapozása és a hatósági eljárás modellezése körében a fogalomalkotó és fogalomelemző módszerek kerültek előtérbe, valamint a rendszer- illetve folyamatszemléletű értékelés. A vizsgálatok alapjaiban analitikus, jogterületeken átívelő természetű, elemző és összehasonlító jellegűek.

A kutatás tárgyának újszerűségére és aktualitására tekintettel a jogharmonizációs folyamat, a Safe Harbor valamint a CBPR rendszer elemzése bizonyos történeti módszertan szerinti leíró jellegű elemzést is megkívánt, azonban jellemzően ebben a körben is az összehasonlító módszerek alkalmazása vezetett eredményre. A SWOT elemzés során elsősorban az analízis klasszikus négyelemű táblázatának elkészítését, majd a szempontok tartalmi, súlyozott értékelését végeztem el.

Az értekezés záró fejezete jellemzően dogmatikai, jogelméleti megközelítésű, ugyanakkor hangsúlyosan jelenik meg a gyakorlatias amerikai nézőpont bemutatása is a személyes adatok mint piaci javak értelmezéseként.

DOI: 10.14750/ME.2019.022

1.4. Kutatási kérdések, kiinduló pontok

A BCR a hazai jogirodalom és joggyakorlat kevéssé ismert, mégkevésbé alkalmazott jogintézménye. 2015. évi bevezetése óta ez a helyzet nem sokat változott. Az értekezés alapvető célkitűzése az, hogy megváltoztassam ezt az állapotot. Célom, hogy a gazdasági szereplők érdeklődését felkeltsem a jogintézmény és az alkalmazásából eredő lehetőségek iránt, az érdeklődő megismerje a BCR-t, a szakember munkája során felhasználja erősségeit, a jogalkotó pedig felismerje a megválaszolandó kérdéseket és a hiányosságokra – reményeim szerint az általam javasolt megoldásokkal – választ adjon.

A harmadik országokba irányuló adattovábbítások jogi szabályozása sem uniós, sem hazai szinten nem volt megfelelő a kor adattovábbítási gyakorlatának[6] rendezésére. A GDPR hatályba lépésével fémjelzett adatvédelmi reform gyökeresen érintette a jogterület ezen szeletét, de vajon kellően átformálta a jogi környezetet ahhoz, hogy a gyakorlatban felmerülő alapvető és kérdéses vagy vitás helyzeteket életszerűen rendezze?

Az átalakított jogi környezeteben a BCR, mint a piaci igényeken alapuló, gyakorlatiasnak tűnő jó megoldás kiemelt szerepet kapott. Ennek ellenére az ezidáig jellemzően soft law jellegű forrásokra felépített jogintézményről maguk a szabály címzettjei, a gazdasági szereplők csak keveset tudtak. Ezen változtatni szükséges.

Bevett jó gyakorlatok hiányában szinte előzmény nélkül kell napjainkban felépíteni és megismertetni, elterjeszteni egy, a jogterületre egyébként nem jellemző jogintézményt, meghatározni valós céljait, kihasználható funkcióit.

[6] Álláspontom szerint a Lindquist-ügy (2003) óta.

DOI: 10.14750/ME.2019.022

A fogalomalkotáson túl azonban számos nyitott pont maradt. Milyen a BCR jogi természete? Milyen tényleges jogi és gazdasági célokat szolgál az egyébként vindikált vélt célok mellet? Hogyan alkalmazható sikerrel egy vállalkozáscsoport működése során? Álláspontom szerint megkerülhetetlen a fenti kérdések megválaszolása ahhoz, hogy a jogintézmény a jogterület széles körben alkalmazott megoldása legyen.

A BCR-k nyilvános része jogszabályi kivonat. Legalábbis ezt a benyomást kelti az online elérhető néhány példa. Azon túl, hogy a gazdasági szereplő a kazuisztikus szabályozást elkerülve a lehető legáltalánosabban rendelkezik saját magatartásáról, mivel lesz több a BCR egy adatvédelmi szabályzatnál vagy egy céges etikai kódexnél? Ezen kérdésekre tartalmi elemzéssel keresem a válaszokat.

A GDPR által megteremteni célzott egységes adatvédelmi jogi környezetben a nemzeti hatóságoknak egyértelmű szerepkörük van és azonos jogosítványaik. Eljárási szabályaikat és eljárásrendjüket azonban nemzeti szinten kell megalkotniuk. A BCR jóváhagyására vonatkozó nemzeti eljárásrend jogi szabályozása még nem készült el, amely álláspontom szerint sürgető hiányosság, amelyet de lege ferenda javaslatommal kívánok pótolni.

Vannak persze más megoldások is arra, hogy az adattovábbítások jogszerűségét a gazdasági szereplő biztosítsa, de adódik a kérdés, hogy miért kellett még egy módszer Alkalmasabb-e a jogszerűség biztosítására a BCR, mint a korábbi jól ismert megoldások? Amennyiben igen, miért és hogyan vezet jobb eredményre a BCR alkalmazása? Alapvető kérdések, amelyekre a válaszok a jogintézmény létjogosultságát kérdőjelezhetik meg.

DOI: 10.14750/ME.2019.022

II. FEJEZET
AZ ADATVÉDELMI JOGHARMONIZÁCIÓ – TÖRTÉNETI SZEMPONTOK

Az Európai Unió mint eredendően gazdasági integráción alapuló együttműködési szervezet fejlődése mára bizonyos területeken, így például az adatvédelem területén, egyre inkább a szupranacionalitás, közvetlenül alkalmazandó jogi szabályozás és a harmadik országokkal szembeni egységes fellépés irányába halad. A jogközelítés igénye azonban nem csak korunk kihívása, hanem az eredményes együttműködés záloga már az integráció kezdetétől. Ebben a fejezetben azt vizsgálom, hogy hazánk a jogközelítés, az általános adatvédelem,[7] különösen a külföldi adattovábbítás területén milyen lépéseket tett a csatlakozási folyamat megindulásától napjainkig. A fejlődési folyamat fontosságát tanúsítja az is, hogy a Lisszaboni Szerződéssel elsődleges jogforrási szintre emelték a személyes adatok védelmét biztosító szabályokat,[8] 2018. május 25. napjától pedig alkalmazandó joggá válik a GDPR valamennyi tagállamban, így az adatvédelem tárgykörének szabályozása a jogforrási hierarchiában is magasabb szintre lép.

II.1 A jogharmonizáció történeti jellemzői

A XIX. századi jogfejlődés eredményeként a jog nemzetivé vált, ez volt „a nemzeti magánjogi kodifikációk dicsőséges időszaka."[9] Az 1940-es évek végétől, elsősorban a gazdasági és kereskedelmi jog területein, a *jogegységesítés iránti igény megélénkült*. Az első ilyen törekvések a Benelux államok 1943. évben elkezdődő, és 1958-ban az Európai Gazdasági Közösségbe beleépülő eredményei lettek.

[7] Az általános jelző itt azt a célt szolgálja, hogy jelen fejezet tárgyát lehatárolja; jelen fejezetnek nem tárgya a szektorális adatvédelmi szabályozás pl. banki adatok továbbítása szabályozásának harmonizációjának vizsgálata.
[8] Az Európai Unió Alapjogi Chartája 7. és 8. cikke, Hivatalos Lap C 83, 2010. március 30.
[9] KECSKÉS (2009) p. 430-436.

DOI: 10.14750/ME.2019.022

A Közösség jogharmonizációs igényei már az integráció első éveiben megjelentek a jog-összehasonlítás gyakorlati igényének támogatásaként. A tagállamok és a Közösség intézményei között komplex kapcsolatrendszer alakult ki a jogalkotás és a végrehajtás vonatkozásában[10] csakúgy, mint az egymás mellett párhuzamosan érvényesülő, ugyanakkor *a közösségi jognak primátust biztosító*[11] közösségi és nemzeti jog között.

Az egymás mellett érvényesülő jogrendszerek és jogalkalmazások az egyre szélesebb körű, elmélyülő gazdasági integráció és a négy alapszabadság általános érvényesülése felé vezető úton az azonos értelmezés[12] igényét hívták életre az egyre több területre kiterjedő szupranacionális jogi szabályozás körében. Így a bizonyos szempontok szerint nemzetek fölött álló szervezet jogalkotással támogatta a szorosabb kapcsolat kialakítását a tagállamok között.

A jogharmonizáció a jogrendszerek közötti különbségek mérséklésére, közelítésére vagy egyenértékűségek kialakítására irányuló folyamat.[13] Az Európai Unió keretei közötti *jogharmonizáció* az a minden tagállamában - és a tagjelölt országokban is - folyamatosan végrehajtandó általános és különös intézkedések összessége, jellemzően *jogalkotási tevékenység*, amelynek célja a tagállami jogi környezet az Európai Unió jogával összeegyeztethetőségének maradéktalan kialakítása, amelynek jogalapjának az ún. általános belső piaci jogharmonizációs klauzula[14] tekintendő, amely az egyes szakpolitikák és ágazatok szabályozására is kiterjed.

[10] Az Európai Unió és a tagállamok hatalmi ágak szerinti differenciált munkamegosztása mint közigazgatástani fogalom szerinti értelmezéséről és elemzéséről lásd bővebben: Közigazgatási Jog IV. Európai Közigazgatás (Szerk.: Dr. Torma András, Miskolci Egyetemi Kiadó Miskolc, 2013
[11]KECSKÉS (2009) p. 575.
[12] Ismert példa a C-2/74. Reynes-ügyben (Határozatok Tára 1974 00631) az önálló vállalkozó meghatározása a letelepedés szabadsága körében vagy az IP-cím személyes adatként való elismerése a 29. cikk szerinti Munkacsoport WP184 vélemények alapján.
[13] KECSKÉS (2009) p. 430-436.
[14] EUMSZ 114. cikk HL C 326., 2012.10.26., 47—390. o.

DOI: 10.14750/ME.2019.022

A tagállamok már a csatlakozás előtt – a tagfelvételhez – és azt követően folyamatosan kötelesek arra, hogy „elősegítsék az Unió feladatainak teljesítését, valamint tartózkodjanak minden olyan intézkedéstől, amely veszélyeztetheti az Unió célkitűzéseinek megvalósítását."[15]

A szupranacionális szervezet *általános eszközévé az irányelvi jogalkotás vált*, amely a deklarált célok elérését a címzett tagállamok kötelezettségeként állapítják meg, a cél elérésének eszközét és formáját a tagállam maga határozhatja meg. Eredményeként a tagállami jogrendszer a rendes nemzeti jogalkotási rendben az annak megfelelő jogforrási típus alkalmazásával módosul. Tekintettel arra, hogy a rendeletek viszont közvetlen hatállyal bírnak és közvetlenül alkalmazandók, így esetükben deregulációs feladatok vagy nemzeti szintű - a szubszidiaritás elvével összhangban - végrehajtási típusú jogalkotási munkát kell elvégezni.[16]

A jogharmonizációs kötelezettségek elmulasztása vagy nem megfelelő teljesítése következtében lefolytatandó kötelezettségszegési eljárások illetve egyéb jogkövetkezmények - például kényszerítő bírság, egyes alapokból lehívható támogatás korlátozása, megvonása - a nemzeti jogalkotási feladatok időben és megfelelő módon történő teljesítésével elkerülhetők. Ezen feladatok ütemezése a nemzeti és az uniós jogalkotással párhuzamosan, komplex programrend mentén zajlik az Európai Unió jogának való megfelelés érdekében szükséges jogszabály-előkészítési feladatok teljesítéséről szóló 302/2010. (XII. 23.) Korm. rendelet előírásai szerint.

[15] Igazságügyi Minisztérium: Jogharmonizációs ügyek intézése, http://eujog.im.kormany.hu/jogharmonizacios-ugyek-intezese [2017. október 15.]
[16] i.m.

DOI: 10.14750/ME.2019.022

II.2 Jogharmonizáció az adatvédelmi jogi környezetben

Az információs jogok alkotmányos alapjogként tételezett, egyetemes, kultúrától és nemzettől független szabadságok, emberi jogok. Tételes joggá válásukat a XIX. századtól egyre terjedő jogpozitivista nézőpont, a jogvédelem egyetemességének, az alkotmányosság, a különleges garanciák biztosításának és új alapjogok elismerésének, majd deklarálásának igénye hívta életre. A XX. század hetvenes éveiben terjedő számítógéppel végzett, és emiatt szinte korlátlan adattárolás és adatkezelés okán keletkezett egy erős szabályozási igény, majd a „nyolcvanas-kilencvenes években a jogalkotás már nem a technikára összpontosít, hanem *az adat mögött álló személyre*."[17] Érvényesülésük az állami beavatkozás és szabályozás eredménye volt.[18] A személyes adatok védelme jellemzően a magánélet védelme körében nyert elismerés,[19] amely az állam részéről aktív, de sokkal inkább támogató beavatkozást igényel. Az 1949. évi XX. törvény, a Magyar Köztársaság Alkotmánya az Alapvető Jogok és Kötelességek fejezetben, az 59. § és a 61. §-ban, Magyarország Alaptörvénye a Szabadság és Felelősség részben a VI. cikk (2) bekezdésében deklarálja a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jogot, a két alapjogot egy bekezdésben, a magánélet külön is nevesített védelmével.

Az Európai Unióról Szóló Szerződés[20] 6. cikke úgy hivatkozik az *Alapjogi Chartára*[21] mint az emberi jogok gyűjteményére. Rendelkezései, így 7. cikke a magánélet védelmére, és 8. cikke explicit módon a személyes adatok védelmére vonatkozóan normatívak, *elsődleges jogforrási* szinten.

[17] SZIKLAY (2010)
[18] SÁRI (2006)
[19] Az Emberi Jogok Egyetemes Nyilatkozata és az Emberi Jogok Európai Egyezménye a magánélet védelmét nevesíti. A Polgári és Politikai Jogok Nemzetközi Egyezségokmánya 17. cikke a magánélet elleni jogtalan támadást tiltja. Az Európai Unió Alapjogi Chartájának 8. cikke rendelkezik a személyes adatok kezelésének feltételeiről.
[20] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata, Az Európai Unióról szóló szerződés, HL C 83., 2010.3.30., 361—366. o.
[21] Az Európai Unió Alapjogi Chartája, Hivatalos Lap C 83, 2010. március 30.

DOI: 10.14750/ME.2019.022

A *másodlagos jogforrási* szintű adatvédelmi szabályozása több területre osztható:[22] i) általános adatvédelem ii) az unió intézményeire irányadó adatvédelem iii) adatvédelem az elektronikus szektorban iv) szektorális adatvédelem pl. bűnügyi adatok vonatkozásában.

Ebben a fejezetben a dolgozat tárgyához igazodóan *az általános védelem szabályanyagát vizsgálom*.

A személyes adatok általános védelme jogi kereteinek Európai Uniós jogharmonizációs folyamata a *95/46/EK irányelv*[23] *(*a továbbiakban: Adatvédelmi Irányelv*)* megalkotásával kezdődött meg, a jogterületet általánosságban szabályozó irányelvet 1995. évben fogadták el.

„Mivel az adatfeldolgozási rendszerek célja az emberek szolgálata", rögzíti az Adatvédelmi Irányelv (2) preambulumbekezdése, és mert az élet számos területén egyre többször az informatika terén elért haladás eredményeként a személyes adatok nagy mennyiségének összegyűjtése, tárolása és feldolgozása sem okoz problémát, az egyének jogai és szabadságai védelme, különösen a magánélet tiszteletben tartásához való jog védelmének érdekében szükségessé vált a tagállamonként eltérő védelem szintjei közötti eltérések mérséklése, a végső cél az azonos védelmi szint minden tagállamban. Indokolja ezt az is továbbá, hogy az eltérések akadályozhatják a személyes adatok egyik tagállamból a másikba történő továbbítását. „Ez a célkitűzés alapvető fontosságú a belső piac szempontjából", deklarálja az Adatvédelmi Irányelv (8) preambulumbekezdése, amelynek szükségességét az (56) preambulumbekezdésben rögzítettek szerint a nemzetközi kereskedelem bővülése igényelte.

[22] OROS-SZURDAY (2003) p. 6.
[23] HL L 281., 1995.11.23., 31—50. o.

DOI: 10.14750/ME.2019.022

A technológia fejlődésére reagálva a szabályozás tárgyi hatálya kiterjed az automatizált módon történő adatkezelési műveletekre, valamint a nem automatizált módon való személyes adat feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

A tagállamoknak az Adatvédelmi Irányelvet átültető nemzeti intézkedések hatályba léptetésére legfeljebb hároméves időszakot lehetett engedélyezni a teljes megfelelés biztosítására.[24] Tekintettel hazánk 2004. évi csatlakozására, az egyes irányelvek implementálásának határidejét a Magyar Köztársaság jogharmonizációs programja tartalmazta a törvényalkotás általános szabályainak megfelelő eljárásban.[25]

Kiemelendő, hogy hazánk a személyes adatok védelme vonatkozásában *példaértékű szabályozást alakított ki a személyes adatok védelméhez való jog alkotmányos elismerésével*, az 1981. évi Európa Tanács által megalkotott adatvédelmi egyezmény kihirdetésével,[26] továbbá az általános törvényi és a szektorális szabályozással, az adatvédelmi biztos tevékenységével, a jogérvényesítés biztosításával. Ennek eredményeként már 2000. évben az Európai Bizottság megállapította,[27] hogy hazánk mint akkor még harmadik ország[28] *biztosítja a megfelelő védelmi szintet* a személyes adatok a Közösségből történő továbbítása esetére.

[24] 95/46/EK irányelve 32. cikk (1) bekezdés, Hivatalos Lap L 281 , 23/11/1995 o. 0031 - 0050
[25] A jogharmonizáció Magyarországon http://www.parlament.hu/biz37/eib/link1/jogharm.htm [2017. október 15.]
[26] Az Európa Tanács az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezményét hazánk a 1998. évi VI. törvénnyel hirdetett ki.
[27] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary OJ L 215 2000.08.25. 4-6. p.
[28] Történik mindez Svájc minősítésével egyidejűleg.

DOI: 10.14750/ME.2019.022

Hazánk a térségben egyedülállóan korán[29] törvényi szintű szabályozást dolgozott ki az 1992. évi LXIII. törvény (a továbbiakban: Avtv.) rendelkezéseivel, így a 2002. évi az Európai Bizottság által készített országjelentés[30] már *a jogközelítés befejezéséről szól*. Magyarország jogharmonizációs kötelezettségének az Avtv. 1999-től kezdődően több lépésben, kiemelten a 2004. január 1. napjával valamint 2005. június 1. napjával hatályba lépő módosított szövegével tett eleget.

A legjelentősebb módosítások a következők:
- a törvény hatályának deklarálása,
- a különleges adat fogalmának pontosítása,
- az adatállomány és nyilvántartó rendszer fogalmának pontosítása,
- jogszerű adatkezelés lehetőségeinek szélesítése,
- a tiltakozás jogalapjának bevezetése,
- adatkezelési jogalapok pontosítása,
- az automatizált egyedi döntéssel kapcsolatos szabályozás bevezetése.

A jogharmonizációs céllal módosított jogszabály záró rendelkezései a jogharmonizációs záradékban rögzítették az Adatvédelmi Irányelvnek való megfelelés tényét.

A jogharmonizáció *stílusa totálisnak* minősíthető, az Adatvédelmi Irányelvet olyannak tekintették, mint amely nagyon csekély[31] mozgásteret hagyott a tagállami jogalkotó számára a szabályozás kialakításában, a részletes, esetenként szigorúbb rendelkezések elfogadására. Megjegyzendő azonban, hogy a GDPR megalkotásának egyik indikációja viszont éppen az volt, hogy az Adatvédelmi Irányelvet a tagállamok jelentős eltérésekkel ültették át

[29] Az első adat- és magánéletvédelmi törvények elsősorban az állam által végzett adatkezelésekre vonatkozóan Svédországban 1973. évben és az USA-ban 1974. évben születtek meg, míg Lengyelországban 1997. évben, Romániában 2001. évben, Szlovákiában 2002. évben.
[30] Az európai bizottság éves jelentése: Magyarország előrehaladásáról a tagság felé, 2002. www.eski.hu/new3/eucsat/eu/2002/2002hu.doc [2015. november 2.]
[31] OROS-SZURDAY (2003) p. 14.

DOI: 10.14750/ME.2019.022

jogrendjükbe, ami végső soron a jogterület inkoherenciáját okozta és ellentmondásos helyzeteket teremtett. Egyik ilyen jellemző eltérés az *adatkezelés fogalma* vonatkozásában tapasztalható: a magyar szabályozás elkülöníti az adatkezelés és az adatfeldolgozás fogalmát, amely az uniós jogban összeolvad. „A jogalkotó célja az volt, hogy az Adatvédelmi Irányelvben foglaltakkal összhangban az adatkezelő mellett olyan alany is megjelenjen a törvényben, amely pusztán az adatkezelő által meghatározott célból, módon és keretek között kezelhet adatot”[32] (t.i. az adatfeldolgozó), de a magyar törvény módosítása nem szolgálta „a magyar adatvédelmi jog fogalomrendszerének átláthatóságát, illetve nem közelítette azt” az Adatvédelmi Irányelvhez éppen e fogalom vonatkozásában. Az Adatvédelmi Irányelv által biztosított további eltérés lehetősége megjelenik a különleges adatok kezelése, a nemzeti azonosító szám és a történelmi, statisztikai vagy tudományos célokra történő további felhasználása vonatkozásában.[33]

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.) - amely az Avtv-t váltotta fel - a harmonizált szabályokat megőrizve további rendelkezéseket tartalmaz a szektorális irányelveknek történő megfelelés körében: ezek a környezeti információkhoz való nyilvános hozzáférés, a közszféra információinak további felhasználása és a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelmének tárgyában született irányelvek.[34] Szükséges megemlíteni, hogy a magyar szabályozás egyedisége az is, hogy az Infotv. – tehát egyetlen jogszabály – rendezi az adatvédelemre és az közérdekű adatok megismerésére vonatkozó szabályokat is.

[32] JÓRI (2003) p. 393-408.
[33] 95/46/EK irányelve 6. cikk (1) bekezdés b) pont; 8. cikk (1) és (7) bekezdések
[34] Ezen szektorális adatkezelésekre vonatkozóan külön jogszabályok vannak hatályban, például: 2009. évi XLVII. törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról,

DOI: 10.14750/ME.2019.022

Az adatvédelmi jogharmonizációs kötelezettség utóhatása a hazai adatvédelmi modell átalakításakor a hazánkkal szemben lezajlott *kötelezettségszegési eljárás*. Magyarország 2012. január 1. napjával az adatvédelmi biztos intézményét felváltó felügyeleti hatóságot állított a személyes adatok védelmén való őrködés céljából: a Nemzeti Adatvédelmi Információszabadság Hatóságot (a továbbiakban: NAIH). Hazánk az adatvédelem területen korábban mutatott példaértékű rendszerében – az ombusdman-like jellegű intézményrendszer kialakítása és működtetése – ezen intézkedését – t.i. az adatvédelmi biztos intézményének megbízatási idejének lejárta előtti megszűntetését és helyére a Hatóság felállítását és elnökének más személy kinevezését – az Európai Unió Bírósága *ellentétesnek találta az uniós joggal*.[35] A Bíróság szerint a függetlenség mint kulcsfontosságú jellemző akkor tartható tiszteletben, ha a megbízatás eredetileg megállapított időtartamát annak leteltéig tiszteletben tartják. Megállapítást nyert, hogy a biztos megbízatása a törvényben rögzített megszűnési okok egyikére sem illett rá. Azon objektív tény, hogy az adatvédelmi felügyelet modellváltáson, újraszervezésen[36] ment keresztül, nem indokolta a függetlenségi követelmény, így a megbízatási időtartam tiszteletben tartásának megsértését.[37]

Jogharmonizációs mérföldkőhöz érkeztünk el 2018. május 25. napjával, hiszen az Infotv-t és a szektorális jogszabályokat a 2016/680 európai parlamenti és tanácsi irányelv implementálása és a „GDPR-t kiegészítő vagy ahhoz képest meghatározott irányban eltérő szabályok megalkotása körében”[38] módosítani vált szükségessé.

[35] C-288/12. sz. Európai Bizottság kontra Magyarország, ECLI:EU:C:2014:237
[36] Az unió több tagállamában hatósági forma működik (görög, dán, finn, francia, portugál, spanyol hatóságok ..etc.), noha az Adatvédelmi Irányelv nem deklarálja a forma kialakítását, csupán a függetlenségi követelményt írja elő.
[37] Az ítélet megszületését követően a volt adatvédelmi biztostól az igazságügyért felelős miniszter nyilvánosan bocsánatot kért, a biztos kártérítést kapott.
[38] NAIH: Tájékoztató közlemény a személyes adatok védelmére vonatkozóan alkalmazandó előírásokról, továbbá az adatkezelőket, illetve adatfeldolgozókat terhelő bejelentési kötelezettségek teljesítéséről

DOI: 10.14750/ME.2019.022

Az Európai Uniós adatvédelmi szabályrendszerének újraalkotását hazánk azonban nem egy közvetlenül alkalmazandó és közvetlenül hatályosuló jogforrás útján látta támogathatónak. Tekintettel arra, hogy Magyarországon 1992-től példaértékűen szigorú szabályozás volt hatályban, ezen magas szintű védelem fenntartására pedig akkor lett volna mód, ha irányelvi szabályozás marad és azt a tagállamok saját jogalkotási eljárással ültetik át. Ezzel szemben, meghiúsítva azt, hogy a multinacionális vállalkozáscsoportok „a tagállamok eltérő adatvédelmi rezsimjeit kijátszva a számukra legkedvezőbb szabályokat biztosító országokban folytassák adatkezelési tevékenységüket", az uniós intézmények és a tagállamok többsége is a rendeleti szabályozás kialakítását támogatták, amely csak szűk keretek között enged eltérést a tagállamok számára,[39] jellemzően intézményi és végrehajtási jellegű kérdésekben, az egyes szabályok közvetlenül alkalmazandók és közvetlen hatállyal bírnak.

Az Európa Tanács szintén napirendjére vette a személyes adatok védelmének kérdését és 2018 májusában az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény módosításáról határozott.[40] Az egyetlen globálisan kötelező erejű egyezmény megteremtette a kapcsolatot a különböző adatvédelmi szemléletű szabályozások között, ugyanakkor az új információs technológiák alkalmazására tekintettel a modernizálására volt szükség. Megtartva elvi jellegű szabályozási módszerét és technológiai semlegességét olyan, a GDPR-ral egybehangzó új rendelkezéseket deklarál, mint az adatvédelmi incidensek jelentésére vonatkozó kötelezettség és az adatminimalizálás alapelve, az adatkezelő elszámoltathatósága és az átlátható adatkezelés kötelezettsége. Deklarálja a „privacy by design" elvet és garanciákat vezet be az automatizált döntéshozatali mechanizmusok alkalmazása esetére.[41]

[39] Iromány száma: T/335, Parlex azonosító: W838KPW50003, Általános indokolás
[40] 128th Session of the Committee of Ministers (2018)
[41] Európa Tanács: Enhancing data protection globally: Council of Europe updates its landmark convention

DOI: 10.14750/ME.2019.022

II.3. Harmonizáció a külföldi[42] adattovábbítás körében

A személyes adatok általános védelmének körében a *külföldi adattovábbításra vonatkozó szabályok alapjaiban történő megváltoztatása* vált szükségessé hazánk jogharmonizációs kötelezettségei teljesítése körében, hiszen a megfelelő védelem biztosítása mellett a korlátozásmentes, szabad áramlás is elvárássá vált.

> *[„9. § Személyes adat az országból - az adathordozótól vagy az adatátvitel módjától függetlenül - külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek.”]*

A harmonizáció előtti Avtv. mindösszesen egyetlen paragrafusának egyetlen, fenti bekezdése számos újabb szabállyal egészült ki a külföldi adattovábbítás megkönnyítése érdekében. Az a már fennálló alapvető értelmezési kérdés is rendezésre várt – a bizonytalan jogfogalmak miatt – hogy az adatkezelő és az adatfeldolgozó közötti adatforgalom törvényen alapuló adattovábbítás-e.

A hatályos magyar szabályozás alapján, amely a harmadik személy fogalmát ekkor még nem határozta meg, *törvényen alapuló adattovábbításnak minősülhetett*, ezért alkalmazni kellett a fentebb idézett szakaszt.

https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=09000016808ac976 [2018. június 23.]

[42] A külföldi jelző nem elírás, a vizsgálat időállapotában hatályos jogi környezet terminológiáját követem.

DOI: 10.14750/ME.2019.022

Ha más értelmezés szerint nem minősül adattovábbításnak – például a jogharmonizáció alapjául szolgáló Adatvédelmi Irányelv fogalomrendszere szerint sem –, akkor *a külföldön történő adatfeldolgozás* - amely nem is adatkezelés – „nem esik a 9. § hatálya alá, tehát az olyan országokban is végezhető, amelyek nem biztosítják a magyar jognak megfelelő védelmi szintet a személyes adatok számára."[43] Ezzel szemben az adatvédelmi biztos arra a következtetésre jutott,[44] hogy a külföldi kutató vagy kutatóintézet számára „csak akkor lehet személyes adatot tartalmazó iratot kiadni, ha a kutató származási országa szerinti adatvédelmi joga a személyes adatok védelme tekintetében azonos biztosítékokkal rendelkezik," hiszen harmadik országba történő adattovábbításnak minősül. Álláspontom szerint is a megengedő értelmezés a jogalkotó céljával ellentétes értelmezés volna, noha a törvény szövegének betűje, amely adatkezelést rögzít, valóban nem alkalmazandó az adatfeldolgozás eseteire.

2004. január 1. napjától az alábbi változások léptek hatályba az első nagy módosítási-bumm eredményeként: *i)* a különleges adatok vonatkozásában is teljesülnie kell a szabályoknak, *ii)* a harmadik országba továbbítás feltétele, hogy a harmadik ország joga - az Európai Unió által meghatározott - *megfelelő védelmet biztosítson* az átadott adatok kezelésekor *iii)* az adatfeldolgozási célú adattovábbítás is a jogszabályhely hatálya alá került. A különleges adatok mint a személyes adattól eltérő fogalmi körbe tartozó, a magánszféra érintettségére tekintettel fokozottabb védelmet igénylő információ kiemelése szintén a fenti értelmezési és kivételi szabály kiküszöbölésének tekinthető.

A megfelelő védelmi szint ismeretlen jogfogalom volt a hazai adatvédelmi terminológia körében, megjegyzem az Adatvédelmi Irányelv sem definiálta, továbbá a megfelelőséget is csak az Európai Bizottság állapíthatta meg.

[43] JÓRI (2009) p. 186.
[44] Az Adatvédelmi Biztos beszámolója (2000): III. vizsgálatok, http://abi.atlatszo.hu/index.php?menu=beszamolok/2000/III/1/2/10&nyomtat=1 [2017. november 15.]

DOI: 10.14750/ME.2019.022

Tehát egy olyan értelmezési nehézség állt elő ismét, amely a több országot, köztük harmadik országot is érintő adattovábbítások megítélését tovább bonyolította, noha az adatkezelés – adatfeldolgozás kettősségére a módosítás választ adott.

2004. május 1. napjától a magyar jogalkotó az Avtv. hatályát is (újra)értelmező rendelkezést deklarált, amely szerint az Európai Unió[45] tagállamaiba irányuló adattovábbítást úgy kell tekinteni, mintha a Magyar Köztársaság területén belüli adattovábbításra kerülne sor. A harmonizált jogi környezet előirányozta, hogy a tagállamok közötti adattovábbítás az országon belüli továbbításnak tekintendő.

A *jogalapok* tekintetében az érintett hozzájárulása, valamint a törvény által biztosított esete - illetve a törvény egyes időállapotaiban[46] nemzetközi szerződés alapján biztosított lehetőség - további konjunktív feltételeként a *megfelelő védelmi szint követelménye* a 2005. június 1. napján hatályba lépett törvénymódosítás szövegében már bevett rendelkezés volt. Az Avtv. igy kifejezetten szigorú és a „nemzetközi kereskedelmi forgalmat is hátráltató szabályt tartalmaz", mivel az „érintett hozzájárulásának megléte esetén is ahhoz köti a személyes adatok külföldre történő továbbítását, hogy a magyar adatvédelmi jogszabályoknak megfelelő feltételek külföldön is fennálljanak."[47] A kevésbé szigorú adatvédelmi jogi környezettel rendelkező harmadik országok irányába tehát tilalmazott, de legalábbis korlátozott az adatexport. „Az ilyen szabályozás természetesen ellene hatott az egységes belső piac kialakításának."[48]

[45] Nem elírás, ebben az időállapotban EU tagállam a törvényszöveg, majd 2015. június 1. napjától került be az Európai Gazdasági Térség tagállamaiba szövegezésű megfogalmazás.
[46] Például a 2004.V.1. - 2005.V.31. között.
[47] JÓRI (2003) p. 405.
[48] i.m. p. 405.

DOI: 10.14750/ME.2019.022

A megfelelő védelmi szint a harmadik országok megkülönböztető jellemzője, de fogalmát nem tartalmazta egyetlen nemzeti vagy uniós jogforrás sem. Az Avtv. sem rendezte, hogy ki jogosult a külföldi adatkezelőnél az adatvédelem feltételek teljesülését, a megfelelő védelmi szint meglétét vizsgálni. Az adatvédelmi biztos és az igazságügyi miniszter közösen kiadta a 8001/1999. (IK. 6.) számú IM tájékoztatót a megfelelő védelmi szintet biztosító országokról, az Amerikai Egyesült Államok például - igazolható okokból - nem szerepelt az országok között. Az Európai Bizottság az Adatvédelmi Irányelv 31. cikke szerinti hatásköre, hogy komitológiai eljárás keretében megállapítsa, hogy harmadik ország megfelelő védelmi szintet biztosít-e vagy sem.[49]

2015. évben a bírói gyakorlat adott iránymutatást a kérdésben. „A „megfelelő védelmi szint" kifejezést úgy kell érteni, mint amely megköveteli, hogy e [az USA] harmadik ország – belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján – az Unióban a Chartával összefüggésben értelmezett 95/46/ irányelv által biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítson ténylegesen az alapvető jogok és szabadságok számára. […] azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket a Chartával összefüggésben értelmezett ezen irányelvből eredő követelmények tiszteletben tartásának biztosítása céljából az Unióban alkalmaznak, ezen eszközöknek a gyakorlatban mégis hatékonynak kell lenniük ahhoz, hogy az Unióban biztosított védelemmel lényegében azonos védelmet biztosítsanak"[50]

[49] Csatlakozásunk előtt Magyarországról is megállapította, mégpedig Svájccal együtt elsőként a megfelelő védelmi szint meglétét, jelenleg például Andorra, a Feröer-szigetek, Argentína, Svájc, Guernsey, Man-sziget, Kanada tartozik e körbe. Bővebben: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71 [2015. november 2.] Az USA vonatkozásában a 2000/520 Bizottsági határozat szerinti biztonságos kikötő elvek és a gyakran felvetőtő kérdések mint kötelező mellékletként csatol útmutató szabályozta e jogterületet.

[50] C-362/14. ítélet 73. pontja, amely a főtanácsnoki indítványt idézi valamint a 74. pontja. ECLI:EU:C:2015:650
http://curia.europa.eu/juris/liste.jsf?td=ALL&language=hu&jur=C,T,F&num=C-362/14.
[2017. október 10.]

DOI: 10.14750/ME.2019.022

A 2005. évi módosítás indokolása rámutatott arra is, hogy a *nemzetközi jogsegélyek* teljesítésével összefüggő adattovábbítási szabályokat is rendezni szükséges, mivel bizonyos országokba jogsegély nem teljesíthető a megfelelő védelmi szint hiánya miatt.[51] Az indokolás rögzíti továbbá, hogy az ilyen országokra vonatkozó uniós aktusokra történő hivatkozást „a törvény egyszerű többséggel elfogadandó, záró rendelkezései között célszerű elhelyezni."

Az Infotv. tartalmában csupán kissé módosult az Avtv. utolsó hatályos időállapotában hatályos szabályokhoz képest a megfelelő védelmi szint kérdésében, habár az „Avtv. külföldre irányuló adattovábbítással kapcsolatos rendelkezései az EU csatlakozás küszöbén indokolatlanul szigorúnak, végiggondolatlannak és – az Avtv. számos más rendelkezéséhez hasonlóan – szerencsétlenül megfogalmazottnak minősíthetők" - állította Jóri[52] az Infotv. tervezetét vizsgálva. A nemzetközi jogsegély biztosíthatóságának szabálya az adóügyi információcseréről, valamint a kettős adóztatás elkerüléséről szóló nemzetközi szerződések esetével bővül. A megfelelő védelmi szint biztosítottnak tekintendő, ha *i)* Európai Unió, az Avtv-ben még Európai Bizottság, kötelező jogi aktussal deklarálja azt *ii)* az érintett jogait és az adatkezelés jogalapját teljes körűen biztosító nemzetközi szerződés esetén.

A harmadik esetkör, hogy *az adatkezelés szabályainak ismertetésével igazolt a megfelelő védelmi szint, szövegszerűen ma már nincs hatályban, noha álláspontom szerint a BCR jogalapjául szolgáló jogszabályhely is lehetett volna*, mivel a jogintézmény esszenciája és célja megfeleltethető a jogszabályhely céljának és szövegének. Mivel hazánkban a harmadik országba történő adattovábbítás nem engedélyköteles illetve előzetes jóváhagyáshoz, bejelentéshez sem kötött és nem is volt az, így BCR létrehozása hazai vállalkozáscsoport tagja számára *valós előnyt hazánkban nem jelentett volna*, a

[51] Itt csak utalok arra, hogy a hazánkban 2005. évben felmerült aggály utóbb a 2009. évi társadalmi hatásvizsgálat körében is megfogalmazódott.
[52] JÓRI (2003) p. 405.

DOI: 10.14750/ME.2019.022

hatósági jóváhagyás vagy engedélyezés kérésének hiánya sem lehetett kötelezettség elmulasztása, így természetszerűleg folytatták le más tagállamokban az engedélyeztetési eljárásokat, figyelemmel a gazdasági és kereskedelmi viszonyokra is. Másrészt mivel nemzeti hatóságunknak nem volt hatásköre a jóváhagyás, így további eljárási szabályokat sem kellett alkotni.

Az Infotv. „által megfogalmazott feltételrendszerbe *sem jogalapként, sem pedig megfelelő védelmi szintet nyújtó dokumentumként nem illeszkedik* bele" a BCR – írta állásfoglalásában a NAIH[53] még a 2013. évben.

Más tagállamok gyakorlatára és a piaci szféra igényeire reagálva azonban 2015. október 1. napján hatályba lépő rendelkezések biztosítanak további lehetőséget a megfelelő védelmi szint biztosítására a BCR beiktatásával. Megjegyzendő, hogy ezen megoldás kizárólag az adatkezelő vagy adatkezelők csoportja számára, de *nem a harmadik ország vonatkozásában biztosítja a megfelelő védelmi szintet*. A kötelező szervezeti szabályozás[54] olyan önkéntesen elfogadott magatartási kódex,[55] „adatvédelmi szabálycsomag"[56] amely lehetővé teszi a vállalkozáscsoportok számára, hogy a saját belső szabályrendszerükben lefektetett rendelkezéseket - érvényesíthető jogokat - és elveket betartva a vállalkozáscsoporton belül személyes adatokat külföldre továbbítsanak úgy, hogy a harmadik országban lévő vállalkozáscsoporti tag adatkezelése megfeleljen az Európai Unió rendelkezéseinek, azaz biztosítsa a megfelelő védelmi szintet.[57]

[53] Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalása, Ügyszám: NAIH-2223-2/2013/V
[54] A jogszabályi fogalom: Infotv. 3. § 25. pont.
[55] http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporaterules/index_en.htm [2015. november 6.]
[56] Európai Bizottság: Milyen előnyökkel jár az uniós adatvédelmi reform az európai vállalkozások számára? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_hu.pdf [2016. január 10.]
[57] A BCR fogalmának tisztázáshoz lásd az V. fejezetben foglaltakat.

DOI: 10.14750/ME.2019.022

Kiemelést érdemel, hogy a BCR 2015. októberi bevezetésével *hazánk ismét – mint az Avtv. példájával – megelőzte számos tagállam jogalkotását*[58] és jogharmonizációs kötelezettségét is, mivel – amint arra a törvénymódosítás indokolása és a közzétett hatásvizsgálat is utalt –, a jogintézmény bevezetését a hatályos uniós szabályozás[59] mellett a tagállami adatkezelők gyakorlata indokolta, továbbá a piaci szféra régóta jelzett igénye volt.[60] Azt azonban meg kell említeni, hogy Jóri[61] már egy évtizeddel korábban felismerte, hogy a külföldi adattovábbítás és a törvényen alapuló harmadik országban végzett adatfeldolgozás megítélésének bizonytalansága a multinacionális vállalatok szervezetén belüli adattovábbítások megítélését is vitathatóvá teszik, amelynek óriási a jelentősége az adatalanyok és a cégek szempontjából is. Kivételként rögzítette az Infotv. az alábbi esetet: ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt megfelelő védelmi szint hiányában is továbbíthatók külföldre személyes adatai.

A jogharmonizációs folyamat következő jogalkotási lépését készítette elő a magyar jogalkotó 2017. év végén, tekintettel arra, hogy a törvényalkotási programban[62] az Infotv. közepes szabályozási terjedelmű módosításának elfogadását tervezték már 2017 decemberében a GDPR szabályaira tekintettel.

[58] Ebben az időszakban a BCR-t nem ismerte el például Baden-Württemberg tartomány, Bréma, Hamburg, Bajorország, Mecklenburg- Nyugat-Pomeránia, Szászország, Schleswig-Holstein Németországban, Írország, Lettország, Portugália, Szlovákia és az Egyesült Királyság sem.
[59] A 95/46/EK irányelv a BCR-t nem nevesítette, a GDPR tervezete pedig további felhatalmazó rendelkezéseket biztosít a tagállami adminisztrációk részére a 38. cikk f) pontjában és 43. cikkben arra vonatkozóan, hogy a rendelet helyes végrehajtása érdekében, amelyet a szubszidiaritás elvére figyelemmel tagállami szinten kell megvalósítani, eljárási szabályok megalkotására ösztönöz, különösen a harmadik országokba történő adattovábbítások esetére.
[60] A módosítás további indoka volt még a 4/2015. AB határozatban előírt kötelezettség, amely az adatminősítés tartalmi felülvizsgálatának bírói úton igénybe vehető eljárásának megteremtését írja elő.
[61] JÓRI (2003) p. 393-408.
[62] 2017. őszi ülésszak törvényalkotási programja:
http://www.parlament.hu/documents/10181/56621/tvalkpr_2017osz.pdf/3b362b76-01b0-426b-81b8-e5d8eb2cc3b6 [2017. október 20.]

DOI: 10.14750/ME.2019.022

A lépés a jogforrás jogi természete miatt elkerülhetetlen volt, hiszen az irányelvi szabályozást rendeleti szintű szabályozás váltotta fel. A rendelet általános hatállyal bíró jogi aktus, amely kötelező és közvetlenül alkalmazandó valamennyi tagállamban. Külön nemzeti jogalkotás nélkül, közvetlenül érvényesül jogforrási természeténél fogva. Ennek a ténynek két jelentős következménye lesz: egyrészt tilos átültetni a nemzeti jogba, másrészt érvényesül a záróhatás. A tagállam az uniós jogalkotás hatályba lépésével kvázi lemond jogalkotási szuverenitásáról, így szükséges a hatályos jogszabályok hatályon kívül helyezése is, e körben az Infotv. gyökeres felülvizsgálata. További feladatot ró a tagállamokra az is, hogy a GDPR- ral egyidejűleg elfogadták „a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló (EU) 2016/680 európai parlamenti és tanácsi irányelv”-et, amely vonatkozásában implementálási kötelezettség áll fenn, azaz erre tekintettel is módosítani szükséges az Infotv. szabályait. A jogalkotási feladat tehát kettős irányú: főként de nem kizárólag *dereguláció*, azaz kivezetni illetve átalakítani a GDPR szabályaival ellentétes rendelkezéseket, illetve *átültetni az új irányelv rendelkezéseit, alapvetően az Infotv. módosításával*.

A fentiek szerint kialakuló hazai jogi környezet azonban azt a nehézséget is magában hordozza a jövőre nézve, hogy az alkalmazandó szabályokat az egyes helyzetekben akként kell megválasztani, hogy az Infotv. csak a 2016/680 irányelv hatálya alá tartozó esetekben alkalmazható, valamint azon részletszabályok körében, amelyek megalkotására a GDPR külön tagállami felhatalmazást adott, minden más esetben közvetlenül a GDPR szabályai alkalmazandók.

DOI: 10.14750/ME.2019.022

Ugyanakkor *jogfejlesztő kötelezettsége is keletkezik az Uniós jogalkotónak*, amely a rohamos technológiai fejlődés miatt – így például a külföldi adattovábbítás gyakorisága, a felhő technológia, a dolgok internete, a forum shopping jelenségeket követő szerver-telepítések valamint a WEB2 elterjedése okán is – kiemelt feladat. Már az Adatvédelmi Irányelv vonatkozásában is felmerültek az alkalmazandó joggal kapcsolatos értelmezésre váró kérdések, tekintettel arra, hogy a származási ország elvén alapuló szabályozás a forum shopping jelenséget erősíti, így az „EU-s adatalanyok felé irányultság”[63] volna célravezetőbb, ez utóbbi elvi megalapozottságot pedig a GDPR már meg is valósította.

Az Európai Unió valamennyi tagállamának jogalkotási – jellemzően deregulációs - kötelezettsége keletkezett a GDPR-ra tekintettel. Egy 2018. január felmérés szerint[64] két tagállamban - Ausztriában és Németországban – megtörént a jogalkotási lépés, tizenhárom tagállamban már a jogalkotó előtt van a módosítás tervezete, hét tagállamban tervezett a jogalkotás, de még nincs nyilvános tervezet, és öt tagállamban nincs nyilvános előrelépés e körben. A helyzet 2018 augusztusára akként változott, hogy tizennyolc tagállamban megtörtént a jogszabály módosítás, tíz tagállamban pedig a törvénytervezet elkészült és megismerhető.[65]

Magyarországon a NAIH 2018 januárjában több, a GDPR végrehajtását biztosító jogharmonizációra irányuló kezdeményezést[66] is tett a jogalkotó felé.

[63] LIBER (2011) (2)
[64] Baker McKenzie International: GDPR National Legislation Survey, 2017. május http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/GDPR%20National%20Legislation%20Survey%20-%20as%20of%20January%2019%202018.pdf [2018. február 9.]
[65] Baker McKenzie International: GDPR National Legislation Survey, 2018. augusztus https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2018/08/gdpr_national_legislation_survey_4_aug2018.pdf [2019. február 20.]
[66] NAIH-579-2-2018-J, NAIH-579-3-2018-J

DOI: 10.14750/ME.2019.022

2018 júniusában az Infotv. jogharmonizációs célú módosításáról[67] döntött az Országgyűlés, azonban a NAIH mint nemzeti hatóság kijelölésén és az első jogsértés esetén alkalmazandó figyelmeztetés szankciójának az Infotv-be iktatásán túl más érdemi rendelkezéssel nem élt. Ezt követően 2018. július 27. napján kihirdették az Infotv. átfogó és részeltes módosítását.[68] Ezzel a 2016/680 európai parlamenti és tanácsi irányelv implementációja történt meg, a törvény GDPR-hoz fűződő viszonyát pedig a 2. § (2) bekezdése rendezi. A szektorális törvények régóta várt módosítása azonban jelen dolgozat lezárásáig nem történt meg, noha a GDPR-saláta[69] elkészült még 2018 októberében. Ajavaslat a NAIH álláspontja[70] szerint hiányos volt, a célzott deregulációt nem valósította meg, elfogadása „a jogbiztonság érvényesülését veszélyeztetné". Hiányolták az érintett szakmai érdekképviseletek bevonását, tekintettel arra, hogy enek következményként fontos és jelentős számú koncepcionális és tartalmi kérdések vizsgálata és megoldása maradt ki a javaslatból. A javaslat elfogadása a NAIH értelmezésében csak tovább fokozta volna a koherenciazavart. A NAIH tételesen vitatta a javalat egyes rendelkezéseit is, mert azok között szerepelt olyan, amely tagállami „norma nem tartható hatályban, nem alkotható meg", illetve amely „nem alkalmas arra, hogy az adatkezelés célhoz kötöttségének alapelvi – és alkotmányossági – követelményét teljesítse". A javaslat végül nem került az Országgyűlés elé.

A fentebb hivatkozott 2018. felmérés tagállamonként veszi sorra a GDPR-ral kapcsolatos általános kérdéseket és vitás illetve kérdéses rendelkezéseket.

[67] Az Országgyűlés asztalán lévő előterjesztés: Iromány száma: T/335., tartalmáról részletesen lásd a VI. fejezet I. pontjában.
[68] Az Országgyűlés asztalán lévő előterjesztés: Iromány száma: T/623.,tartalmáról részletesen lásd a IV. fejezet 5.1. pontjában.
[69] http://www.kormany.hu/download/6/49/71000/GDPR_sal%C3%A1ta_eloterjesztes_180926.pdf#!DocumentBrowse
[70] NAIH/2018/6123/2/J. https://www.naih.hu/files/NAIH_2018_6123_2_J_2018-10-09.pdf

DOI: 10.14750/ME.2019.022

A harmadik országba irányuló adattovábbítás vonatkozásában Málta aggályát fejezte ki az USA-ba irányuló adattovábbításokkal kapcsolatban az Adatvédelmi Pajzs továbbra sem igazolt hatékonysága miatt, valamint az Egyesült Királyság vetette fel érdemben a Brexit kapcsán azt, hogy a Bizottság megfelelőségi határozatának - amelynek meghozatala a nyomozati hatáskörökről szóló brit törvény okán meghiúsulhat -, helyettesítő eszközeként BCR vagy szerződéses klauzulák szükségeltetnek majd az adattovábbítások jogszerűségéhez.

Álláspontom szerint az uniós reform is elkésett, tekintettel arra, hogy számos precedens jellegű ítélet,[71] a 29. cikk szerinti Adatvédelmi Munkacsoport soft law jellegű jogforrásai,[72] valamint a tagállami adatvédelmi hatóságok joggyakorlata[73] igyekeztek jellemzően fikcióval orvosolni a technológia fejlődése okán létre jött joghézagokat.

Szőke[74] is akként foglal állást, hogy bizonyos technológiai és társadalmi kérdéseket, például a Big Data jelenséget és az adatbányászatot, nem kellő súllyal kezel a GDPR, sőt az egy „korábbi" technológiai-társadalmi helyzetre reagál. Megjegyzem, az adatkezelők már túlléptek a fentiekben kiemelt problémán, különösen azért, mert az adatkezelés jogalapját szinte minden esetben biztosítani tudják. Az esetek többségében ugyanis a tartalmilag kiüresedett, ám alakilag így is érvényes adatkezelési jogalap – t.i. az érintett hozzájárulása az adatkezeléshez – szinte automatikusan megszerezhető.

[71] Például a C-131/12 számú Google Spain és Google vagy a C-362/14. számú Maximilian Schrems kontra Data Protection Commissioner ügyben hozott ítélet.
[72] Például a cloud computing, a cookiek, az álnevesítés, az incidens jelentések vagy a model klauzulák vonatkozásában, és még hosszasan sorolhatnám.
[73] Például a holland hatóság a MAC addresst személyes adatnak minősítő z2010-00582 számú jelentése vagy a NAIH a joghatósági, hatásköri kérdéseket is felvető Weltimmo S.R.O. ügyében hozott határozata, amely eredményeként az Euróai Unió Bírósága előzetes döntéshozatali eljárás során foglalt állást az Adatvédelmi Irányelv személyi, tárgyi és területi hatálya kérdéseiben.
[74] SZŐKE (2015) p. 117.

DOI: 10.14750/ME.2019.022

Számos, az Adatvédelmi Irányelv 1995. évi elfogadása óta felmerült kérdésre újabb és újabb, jellemzően irányelvi[75] formában adtak részben jó választ, ami a jogterület felaprózódásához vezetett, miközben a szektorális szabályok mellett *az általános joganyag fejlesztése lett volna célravezető*.

A GDPR szabályozási filozófiája több technológiai *kihívásra is reagál*. Fogalomként deklarálja az álnevesítést vagy a profilalkotást illetve külön cikkben szabályozza az elfeledtetéshez való jogot. Összességében azonban megerősíti azt is, hogy *az adatvédelmi szabályozás új generációját alakítja ki*: az érintetti, egyébként kevéssé érvényesített és érvényesíthető jogok gyarapítása helyett – megtartva az információs önrendelkezés filozófiáját is – az adatkezelők és immár az adatfeldolgozók elszámoltathatóságát, valamint ön- illetve társszabályozását és tanúsítását támogatja. Ezzel a cselekvés lehetőségét és egyben kötelezettségét a jogviszonyok hatalmi helyzetben, információs fölényben lévő résztvevőjére helyezi át. Érdekeltté teszi az adatkezelőt és az adatfeldolgozót is saját adatvédelmi szabályok létrehozásában, például BCR alkalmazásában, és az elszámoltathatóság elvére alapítva a cég bevételéhez arányosítva és a jogsértés súlya szerint differenciálva emeli meg a kiszabható bírság összegét.

Azonban a GDPR-t alkotók mintha nem gondoltak volna arra, hogy a rohamosan fejlődő technológiai környezetre reagálni célzott rendeleti szintű jogforrás módosítását nem lehet majd olyan ütemben meglépni,[76] amelyre adott esetben szükség lenne, és a fenti kisegítő folyamatokra – esetjog, soft law iránymutatás, hatósági gyakorlat, szektorális túlszabályozás – lesz igény a megfelelő jogalkalmazáshoz. Az irányelvi szabályozással szemben az volt a

[75] Például a 2002/58/EK Elektronikus hírközlési adatvédelmi irányelv vagy a C-293/12 és C-594/12 egyesített ügyekben hozott ítélet által hatályon kívül helyezett 2006/24/EK irányelv (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról

[76] A GDPR jogalkotási folyamata 2012. január 25. napjától 2016. április 27. napjáig, több mint 4 évig tartott.

DOI: 10.14750/ME.2019.022

legfőbb ellenérv, hogy a tagállami átültetés miatt széttagolt adatvédelmi jogrendszerek voltak alkalmazandók párhuzamosan, amely a határon átnyúló harmadik országokba irányuló adattovábbítások esetén is eredményezhetett, illetve eredményezett is kérdéses helyzeteket, mivel az Európai Uniós tagállamok a főbb elveket és szabályokat már átültették. Tehát elegendő lehetett volna az Adatvédelmi Irányelv módosítása a technológiai viszonyokra tekintettel és egy új irányelv megalkotása a harmadik országokba irányuló adattovábbítások esetére. Igaz, ez a megoldás is csak a jogi környezet további széttöredezettségéhez vezetett volna, viszont alkalmas lehetett volna annak elősegítésére, hogy az adattovábbításokat nem a célországok, hanem az egyes adatkezelők vagy adatfeldolgozók vonatkozásában lehessen megítélni, amelyre egyébként a GDPR is törekszik. Noha a GDPR hatása ugyan túlmutat személyi és területi hatályán, ezzel az európai polgár illetve az Európai Unió területén tartózkodó adatalanyok jogérvényesítését és jogvédelmét támogatja, a harmadik országokban az adatkezelőknél vagy adatfeldolgozóknál fellépő állami intézkedések ellen hatástalan, hacsak nem magát az adattovábbítás lehetőségét tiltja meg amiatt, hogy a címzett nem képes a megfelelő védelmi szintet biztosítani. Az persze kevéssé vitatható, hogy az egységes rendeleti szabályozás jobb, mint a fragmentált jogi környezet és a digitális egységes piac rendeltetésszerű működéséhez is szükségszerű egy közös jogi alap. Jelen értekezés a harmadik országba irányuló adattovábbítás szabályozási környezetét és a BCR jogintézményét vizsgálja, erre tekintettel határolt a további vizsgálódás.

DOI: 10.14750/ME.2019.022

III. FEJEZET
AZ ADATVÉDELMI REFORM ÉS AZ ÚJ GENERÁCIÓS SZABÁLYOZÁS

Kialakult tehát egy irányelven alapuló standard, amelyet a tagállamok számával azonosan növekvő számú, erősen tagolt nemzeti joganyag szabályozott „újra". Az Adatvédelmi Irányelvben megfogalmazott célok, irányok a nemzeti jogokban nyertek tényleges jogintézményekként elismerést, azonban tagállamonként eltérően, tehát a szabályozási koncepció végső célját – t.i. egy egységes jogi környezet létrehozása – nem (teljesen) érte el.

Ezzel párhuzamosan a technológia a jog által csak nehezen követhető fejlődési pályán suhan előre, amely vívmányai - például a helymeghatározás, a viselkedésen alapuló profilozás, a dolgok internete (IoT) - kétség kívül a magánélet és a személyes adatok védelmének ugyanolyan ellenségei lettek, mint amennyire fontos kényelmi funkciót ellátnak. Ezt felismerve vált szükségessé egy átfogó reform megvalósítása Európai Uniós szinten, globális hatásokkal, erős magánéletvédelmi szemlélettel.

Az Európai Unió 2012. évben az adatvédelmi szabályozás átfogó reformját kezdte meg a globális gazdasági kapcsolatok, a digitálisan összekapcsolt világ, az egyre nagyobb méreteket öltő online adatgyűjtés és adatmegosztás adatvédelmi kihívásainak kezelése érdekében az Adatvédelmi Irányelv és a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében továbbított személyes adatok védelméről szóló 2008. évi kerethatározat felülvizsgálatával.[77] Jelen fejezetben azon túl, hogy a reform átfogó jellegét demonstrálva igyekszem széles körű betekintést nyújtani, kiemelten a harmadik országba irányuló adattovábbítás és a BCR tárgykörét vizsgálom, mert a teljes reform részletes bemutatása és elemzése meghaladja e dolgozat tárgyi és formai kereteit.

[77] http://www.consilium.europa.eu/hu/policies/data-protection-reform/ [2017. október 15.]

DOI: 10.14750/ME.2019.022

III.1. A társadalmi igényről

Széleskörű társadalmi egyeztetés[78] eredményeként már 2009. évben kirajzolódtak azok a tématerületek, amelyek szabályozása jelentős átalakításra várt.

A megkérdezett természetes személyek mint érintettek és adatalanyok elsődleges aggálya, hogy a fennálló jogi környezet alkalmazható-e megfelelően az új technológiákkal szemben, mint például a megfigyelés, a profilozás, a magatartáson alapuló hirdetések vagy az IP címek személyes adatokkénti kezelésének adatvédelmi kihívásai. Ugyanezen tárgyban a hatásvizsgálatban részt vevők egy része azt állította, hogy az online hirdetési piac számos szereplője az adatvédelmi szabályrendszer közvetlen és szándékos megsértésével jár el. A megkérdezettek kiemelték az internetes anonimitás kérdését és a hozzájárulás megfelelőségét az internetes szolgáltatások és a közösségi médiumok használata esetén. Egyesek a hozzájárulás visszavonása esetére javasoltak komplex jogi keretrendszert. Az adatkezelési kockázatok és az incidensekről történő tájékoztatás, az egészségügyi adatok fokozottabb védelme, a felügyelő hatóságok hatásköreinek kiterjesztése és a szigorúbb kikényszerítés körében azonosították a jogalkotástól elvárt fejlesztéseket. Alapelvi hangsúlyt kapott a célhoz kötöttség, főként a jogérvényesítés céljából felhasznált magáncélú adatgyűjtésekre vonatkozóan. Az adatkezelő és adatfeldolgozó szerepek megfelelő elkülönítését igényelték, különösen az interneten igénybe vehető szolgáltatások körében, ahol elvárás volna az alapvetően a személyes adatokat alapértelmezetten védő környezet kialakítása. Ugyancsak alapvető elvárás, akárcsak eddig egy teljesen független és szakértőkből álló felügyeleti hatóság.

[78] European Commission: Summary of replies to the public consultation about the future legal framework for protecting personal data, Brussels, 2010 http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf [2017. október 15.]

DOI: 10.14750/ME.2019.022

A cégek, fenntartva, hogy az adatvédelmi kötelezettséget egyensúlyban szükséges kezelni a tulajdon szabadsága és a gazdálkodás szabadsága tiszteletben tartásával - itt elsősorban saját profitorientált tevékenységükkel együtt járó adatkezelések védelmében - kiemelték, hogy az új technológiák alkalmazása körében a jogi szabályozásnak mozgásteret kell hagynia a gyakorlati megvalósítás lehetőségeinek. Egyetértve az adatvédelem szükségességével, a jól megválasztott adatbiztonsági megoldások és adatkezelési és adatfeldolgozási technológia növeli az ügyfelek és a vásárlók bizalmát is, amely összeségében az ő előnyükre is válik. Az adattárolás és a feldolgozási műveletek elvégzésének kiszervezés terjedése okán szükségessé vált a felelősségi szabályok pontosabb rögzítése az adatkezelők, adatfeldolgozók és további megbízottjaik között. A tagállamok eltérő jogi környezetét, továbbá az alkalmazandó jog kérdésére adott eltérő tagállami jogalkalmazói válaszokat a gazdasági tevékenység folytatásának akadályaként azonosították, ugyanígy az adatkezelő és az adatfeldolgozó fogalmának inkoherens alkalmazását is, kiemelten a WEB.2.0. szolgáltatások körében, ahol az adatalany egyben adatkezelő is lehet. Több szervezet a hozzájárulás online megadható formáinak tisztázását kívánták. A személyes adat fogalmának újragondolását is szorgalmazták azok, akik személyes adatnak minősülő adathalmazokkal dolgoznak, de nem céljuk például az IP-cím mögött álló tulajdonos természetes személy azonosítása, és felmerül a közlekedési, a szakmai vagy üzleti adat fogalmi kérdése is az álnevesítésre vonatkozó rugalmas szabályozás kialakításának igényével együtt.

A Nemzetközi Kereskedelmi Kamara közleménye szerint[79] a szabályozási környezetnek a jó gyakorlatokra is reagálnia kell, rugalmasan kell alkalmazkodnia a folyamatosan változó társadalmi és technológiai igényekhez valamint az üzleti strukturális változásokhoz.

[79] International Camber of Commerce: Data, https://iccwbo.org/global-issues-trends/digital-growth/data/ [2017. novmeber 21.]

DOI: 10.14750/ME.2019.022

A magánszférát védő szabályoknak az adatok áramlása és a fejlődés akadályozása nélkül kell érvényesülniük. Az adatok szabad áramlása a gazdasági folyamatok vezéreleme, az internet alapú adattovábbítások a kis- és középvállalkozások versenyképességének és a globális gazdaságba történő belépésének lehetőségét teremtik meg. A fizikai vagy szabályozási korlátozások költségnövekedést, a fejlesztések elmaradását, az innováció és a hatékonyság visszatartását és indokolatlan adminisztratív terhek felhalmozódását jelentik, noha a Kamara által is elismerten a tranzakciók biztonsága, a fogyasztók védelme érdekében szükséges az állami beavatkozás szabályozók útján. Ezek közül kiemeli a kereskedelmi megállapodások és a szerződéses klauzulák fontosságát, amelyek a nemzeti joggal együtt segíthetik a harmadik országba irányuló adattovábbítások megfelelését. [80]

A harmadik országba irányuló adattovábbítások körében az önszabályozás lehetőségét és külön nevesítve *a BCR elismerését valamennyi tagállamban*, ehhez kapcsolódva az együttműködési eljárások elfogadását szorgalmazták, kiiktatva a túlzott adminisztratív bejelentési, jóváhagyási és engedélyezési kötelezettségeket és az ehhez társuló magas költségeket.
A cégek megfogalmazták az igényt a vállalkozáscsoport jogi személyként történő explicit deklarálására, amely a BCR hatálya és alkalmazási területére vonatkozó kulcsfogalom, amely még a gyakorlatban sem volt kiforrott.
A jogalkotással való szorosabb szakmai párbeszédet és szektor-specifikus alkalmazási kérdések tisztázását várták a reform eredményeként.
A régóta alkalmazott szerződéses klauzulák már nem képesek ellátni céljukat, alkalmazhatatlanok a tömeges adattovábbítások esetére, az Európai Bizottság megfelelőségi határozatai pedig csak kevés állam vonatkozásában állapítják meg a megfelelő védelmi szint fennállását.

[80] International Camber of Commerce: Trade In The Digital Economy A Primer On Global Data Flows For Policymakers Prepared by the ICC Commission on Trade and Investment Policy and the ICC Commission on the Digital Economy https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf [2017. november 21.]

DOI: 10.14750/ME.2019.022

Az USA területén működő adatkezelők részére történő továbbítások esetére a Safe Harbor rezsim kiterjesztését szorgalmazták[81], illetve azt, hogy ezek az adattovábbítások kerüljenek kivételi körbe. Az adatkezelők a megfelelés és elszámoltathatóság kérdésében arra tettek javaslatot, hogy a jogi megközelítés inkább arra irányuljon, hogy az adott adatkezelő képes-e megtenni és valóban megtette a szükséges intézkedéseket, és saját felelősségi láncolatot alakíthasson ki ahelyett, hogy a jog deklarálja a jogsértésért felelősséget vállaló személyét.

Érdekes az a tény, hogy időben jóval korábbi – 1999-es[82] – és napjainkban elterjedt európai és amerikai nézőpontok[83] szerint is az adatvédelmi önszabályozásra mint az állami szabályozást kiegészítő, piaci igényeken alapuló szabályozó mechanizmusra igény mutatkozik, bár tényleges adatvédelmi funkciója – mindinkább a piaci szereplők érdekeinek megfelelő céljai – miatt kritika éri. A GDPR nagy jelentőséget biztosít a tanúsítás, a magatartási kódexek, a hatásvizsgálatok szerepének, noha ezek hatékonysága az európai környezetben még kevéssé ismert, azt azonban tapasztalatból tudjuk, hogy az USA-ban megbuktak az ilyen jellegű próbálkozások.[84]

Az Európai Bizottság „átfogó megközelítése”[85] szerint is „tisztázni és pontosítani” szükséges az adatvédelmi elvek az új technológiákra történő alkalmazását. Felismerve az erősebb intézményi struktúra igényét, kiemeli a bíróság előtti jogérvényesítés kérdéskörének újraszabályozását, e körben kiterjesztését, és a szankciók szigorítását, az adatvédelmi hatóságok

[81] Ekkor még hatályos volt a Safe Harbor határozat.
[82] BERMAN-MULLIGAN (1999) p. 552-582.
[83] SZŐKE (2015) vagy IAB Europe: Self-Regulation, https://www.iabeurope.eu/category/policy/self-regulation/ (2017.11.21.)
[84] A Safe Harbor rendszer legerősebb kritikája az ellenőrizetlenség és a megfelelés tényleges hiánya volt. Az ön- és társszabályozás amerikai sikertelenségéről részletesen: GELLMAN (2016) p. 53-77.
[85] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A személyes adatok Európai Unión belüli védelmének átfogó megközelítése, COM(2010) 609 végleges, Brüsszel, 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf [2017. október 15.]

DOI: 10.14750/ME.2019.022

jogállásának, hatásköreinek tisztázását[86] és erősítését a 29. cikk szerinti Adatvédelmi Munkacsoport szakmai felügyelete mellett. Ugyanakkor a megfelelés érdekében szükségesnek tekinti az adatvédelmi tisztviselő alkalmazását az adatkezelőknél, hatásvizsgálatok lefolytatását.
Az érintetti jogok erősítése, köztük a saját adatok felletti hatékony ellenőrzés, az adatkezelések átláthatósága és a tájékoztatási kötelezettség, különösen a tájékozott hozzájárulás feltétele körében elsődleges fontosságú, az adatminimalizálás elvével összhangban. Az incidensek bejelentésének kötelezettsége, a digitális technológiához igazodó új jogosultságok, például az adathordozhatósághoz való jog kiemelt jelentőséget kapott.
A genetikai és biometrikus adatok fokozott védelmét is előirányozza, a jogorvoslati jogosultságok és az adatkezelők elszámoltathatóságának erősítésével párhuzamosan. Elismeri, összhangban a piaci igényekkel, az önszabályozási mechanizmusok és az alkalmazandó jog kérdéskörében felvetett igényeket és aggályokat, valamint az adminisztrációs terhek csökkentésére vonatkozó javaslatokat.

Az Európai Bizottság kritikusan megállapítja azt is, hogy „eltérések keletkeztek az irányelvet átültető nemzeti jogszabályok között, ami ellentétes a jogi aktus egyik legfontosabb célkitűzésével, vagyis a személyes adatok belső piacon való szabad áramlásának biztosításával.” Ugyanígy az alkalmazandó jogra vonatkozó aggályok már 2003. évben felmerültek.[87] A globális megközelítés tükrében a harmadik országba irányuló adattovábbítások vonatkozásában az Európai Bizottság elfogadta az egységesebb megközelítés szükségességét a megfelelőségi döntések kérdésében.

[86] E körben merül fel 2015. évben, hogy a tagállami hatóság hozhat-e döntést olyan adattovábbítás jogszerűségének kérdésében, amely esetében a harmadik ország tudottan nem biztosítja a személyes adatok védelmének megfelelő szintjét, de hatályban van egy, az Európai Bizottság által meghozott (megfelelőségi) határozat. Részletesen lásd a X. fejezet 2. pontjában.
[87] A Bizottság jelentése – Első jelentés az adatvédelmi irányelv (95/46/EK) végrehajtásáról (COM (2003) 265.)

DOI: 10.14750/ME.2019.022

Az akkori széttagolt szabályozási környezetben ugyanis az Európai Bizottság és egyes tagállamok is megállapíthatták egy harmadik ország megfelelőségét, eltérően is akár,[88] arra is tekintettel, hogy a közhatalmi szervek általi és hatósági adattovábbítások esetére nem rendelkezik az Adatvédelmi Irányelv.

Összességében az Európai Bizottság deklarálja, hogy az európai adatvédelmi szabályozásnak példaértékűnek kell lennie, a magas szintű adatvédelem sztenderdjét kell mintául mutatnia valamennyi harmadik ország számára, ezért 2011. évben javaslatot tett az adatvédelem jogi keretének felülvizsgálatára irányuló jogszabályra.

III.2. Hatásvizsgálat és tagállami javaslatok

III.2.1. Társadalmi véleményezés

2012. évben a Bizottság közzétette a jogszabály tervezetet kísérő hatásvizsgálati munkadokumentumot.[89] A hatásvizsgálat három nagy csoportban definiálja az adatvédelmi szabályozás problémaköreit: i) a széttagoltságból, jogbizonytalanságból és a következetlen jogalkalmazásból eredő nehézségek a gazdasági szereplők és a közfeladatot ellátó szervek oldalán ii) az érintettek személyes adataik feletti ellenőrzési nehézségei iii) a rendőrségi és büntető igazságszolgáltatási együttműködés során tapasztalt joghézagok és következetlenségek.

A harmadik országokba irányuló adattovábbítások kérdése és a BCR több aspektusban is valamennyi problémakörben megjelenik, a következőkben erre figyelemmel elemzem a munkadokumentumot.

[88] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A személyes adatok Európai Unión belüli védelmének átfogó megközelítése, COM(2010) 609 végleges, Brüsszel, 2010., 2.4.1. pont p. 16. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf [2017. október 15.]
[89] European Commission: Commission Staff Working Paper - Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf [2017. október 18.]

DOI: 10.14750/ME.2019.022

Az Adatvédelmi Irányelv eltérésekkel történő átültetése okán a harmadik országba irányuló adattovábbítás szabályai is különböznek, elsősorban a megfelelő védelmi szint kérdésében: az Egyesült Királyságban például az adatkezelő elvégezheti a megfelelőségi tesztet, Franciaországban az adatvédelmi hatóság jogosult dönteni róla. Természetesen az Európai Bizottság jogosult az adott harmadik országot megfelelő védelmi szintet biztosító országnak nyilvánítani határozatában. A megfelelő védelmi szint kérdése sok esetben diszkrecionális döntésen múlik, vagy az Európai Bizottság határozata nem hatályosul közvetlenül. A modell klauzulák körében kiemeli, hogy vannak tagállamok, amelyek a klauzulák alkalmazására tekintet nélkül megkövetelik az adatvédelmi hatóság előzetes jóváhagyását az adattovábbításokat megelőzően.

Azt azonban ki kell emelni, hogy a BCR-nek nem automatikus alternatívája a model klauzulák alkalmazása, és fordítva sem. Köztük ugyanis alapvető eltérések vannak, még ha végső céluk azonos is. A modell klauzulák tulajdonképpen egy szerződést testesítenek meg két jogi személy között, míg a BCR egy belső szabályzat. Így olyan adattovábbítás esetén, amely a jogi személy működési egységeinek keretein belül marad, a modell klauzulák nem alkalmazhatók. Nem alkalmasak továbbá bonyolult, nagyobb vállalati struktúrával rendelkező gazdasági szereplőknél vagy gyakori, nagy mennyiségű adattovábbítási munkafolyamatok során sem a nagy adminisztratív teher és időigényessége miatt. Nagy előnyük azonban, hogy előre elkésztíve rendelkezésre állnak, míg a BCR-t a vállalkozáscsoprotnak kell megalkotni. Az érintetti igényérvényesítés szempontjából a modell klauzulák hatékonyabbak lehetnek, hiszen az érintett ugyan nem fél a szerződésben, mégis felléphet a szerződés megszegése esetén, különösem, mivel a szerződő fél aláveti magát az uniós illetve tagállami joghatóságnak is. A BCR-esetén ilyen egyértelmű igényérvényesítési helyzetet nem tudunk azonosítani.[90]

[90] Részletesen lásd az V.1. részben.

DOI: 10.14750/ME.2019.022

Míg a modell klauzulákat jellemzően egyszerűen csak az alapul fekvő szerződéshez csatolják, addig a BCR-t vállalkozáscsoporti szinten kell érvényesíteni, és a szerződő harmadik személy például adatfeldolgozóként eljáró féllel újabb szerződést kell kötni úgy, hogy a BCR-t meg sem ismeri adott esetben. A BCR a vállalkozáscsoporton belül fejt ki hatást, míg a modell klauzulák a harmadik személlyekkel, a vállalkozáscsoproton kívüli jogviszonyokban alkalmazhatók, jellemzően egyedi adattovábbítások esetére. Összességében tehát a két jogi eszköz végső célja és funkciója azonos, a megfelelő védelmi szint biztosítása a harmadik országban eljáró félnél adattovábbítások esetén, azonban két teljesen eltérő jogi helyzetben alkalmazandók.

A hatásvizsgálati dokumentum külön értelmező rendelkezésben határozza meg a BCR fogalmát amellett, hogy számos negatívumát is kiemeli: nem minden tagállamban elismert jogalap a megfelelő védelmi szint igazolására, hosszú engedélyezési eljárás előzi meg alkalmazását, nem alkalmazható az adatfeldolgozókra, a vállalkozáscsoport mint fogalom hiányára tekintettel nem tisztázott az alkalmazás személyi köre. Ezek a gazdasági szereplőket leginkább akadályozó tényezők. Vitás helyzeteket szül a 2003 óta húzódó helyzet, amely a jogalkalmazás következetlenségét mutatja, ami a nemzeti hatóságok anyagi forrásai, eltérő hatáskörei és az összehangolt együttműködés hiánya következtében alakult ki. Megoldási javaslatként a hatásvizsgálat a harmadik országban működő adatkezelő és adatfeldolgozó tanúsítását adja, amely megfelelő szabványosítással, monitoringozással, a megfelelés ellenőrzésével és panaszkezelési eljárások alkalmazásával kiküszöbölheti a fenti aggályokat, akár szektorális, például munkahelyi (drog és alkoholtesztre vonatkozó), illetve egészségügyi (az érintettől történő adatgyűjtésre és a genetikai vizsgálat eredményeinek megismerésére vonatkozó) speciális szabályokkal.

DOI: 10.14750/ME.2019.022

A hatásvizsgálat rögzíti, hogy a szabályozás technológia-semleges, így nem volna indokolt e körben a módosítás – megjegyzem a harmadik országba irányuló adattovábbítások esetében nem a távolság vagy az alkalmazott módszer a kulcselem –, és a jól ismert C-101/01. számú Lindqvist[91] esetet idézi, amely már több mint egy évtizede elvi jelentőséggel mondta ki azt, hogy az internetes oldalra történő feltöltés nem minősül nemzetközi illetve harmadik országba irányuló adattovábbításnak, vagyis a harmadik országban lévő számítógépen megjelenő személyes adat nem feltétlenül jelenti azok az adatkezelő általi nemzetközi továbbítását.

Az adattovábbítás olyan tág értelmezése, amely azt a következtetést engedi, hogy minden internetes feltöltés egyben adattovábbítás is, mert azt bármely ország internet-hozzáféréssel rendelkező állampolgára elérheti, és így a megfelelő védelmi szint garanciája nem teljesülhet, nem egyeztethető össze az adatvédelem általános, és jogforrási speciális céljaival. Hiszen amennyiben a megfelelő védelmi szint nem biztosított, tagállami kötelezettség az adattovábbítást megakadályozni az irányelv rendelkezése és az ítélet 69. pontja szerint is, tehát a feltöltés helye szerinti tagállam köteles volna minden internetre történő feltöltést megakadályozni.

III.2.2. Tagállami javaslatok a BCR vonatkozásában

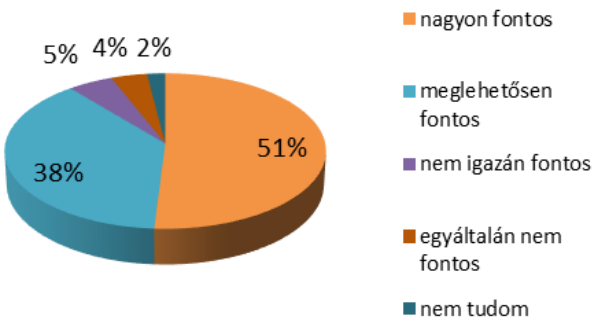
A hatásvizsgálat kiemeli, hogy a BCR jogintézményét anélkül fejlesztették ki, hogy a hatályos jogi környezet akárcsak hasonlót is explicite tartalmazott volna. Tehát saját interpretációm szerint a BCR olyan jogi eszköz, amelyet az adatkezelők saját elhatározásából és érdekéből, a jogalkotó erre az igényre reagáló normatív szabályalkotással hozott létre, így a jogintézmény elfogadottságát az adatkezelők körében mindez igazolja, de az érintettek jogvédelemét aligha támogatja.

[91] C-101/01. sz. Svédországban, Bodil Lindqvist ellen folytatott büntetőeljárás során előzetes döntéshozatali eljárásban a Bíróság 2003. november 6. napján meghozott ítélete, EBHT 2003., I- 12971. p ECLI:EU:C:2003:596

DOI: 10.14750/ME.2019.022

Azonban nem minden tagállam ismeri el, ahol pedig elismerik, ott hosszadalmas és költséges az engedélyezése, amely visszatartja a gazdasági szereplőket alkalmazásától, noha a modell klauzulákkal versenyképes jogi eszköz, amely képes reagálni a megváltozott digitális környezetre. Egyes válaszadók globális BCR- ek alkalmazására is javaslatot tettek.

A GDPR V. fejezetére, amely a harmadik országba irányuló adattovábbítást szabályozza, több tagállam számos további észrevételt[92] tett még a jogalkotási folyamat során több alkalommal is a tervezet különböző időállapotaiban,[93] amelyek közül számos[94] irányult közvetlenül a BCR szabályozásának átalakítására, pontosítására.



1. ábra Eurostat kördiagramm a joghatóságtól független jogvédelem fontosságáról

Feltett kérdés: Mennyire fontos Önnek az, hogy Önt ugyanazok a jogok illessék meg és személyes adatai azonos szintű védelemben részesüljenek, függetlenül attól, hogy melyik országban van az Önnek szolgáltatást kínáló gazdasági társaság vagy eljáró hatóság székhelye?

Az időbeli hatály és az alkalmazhatóság körében az az igény merült fel, hogy a *már engedélyezett BCR-k alkalmazhatók maradjanak a GDPR szerint is*.

[92] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Comments on Chapter V, Brussels, 12 December201, 6723/ 13 REV 5, 2012/0011 (COD)
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206723%202013%20REV%205
[2017. október 19.]

[93] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Comments on Chapter V, Brussels, 23 April 2014, 6723/ 13 REV 6, 2012/0011 (COD)
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206723%202013%20REV%206
[2017. október 19.]

[94] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Chapter V, Brussels, 28 April 2014, 8087/1/14 REV 1, 2012/0011 (COD)
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208087%202014%20REV%201
[2017. november 2.]

DOI: 10.14750/ME.2019.022

A BCR területi hatálya vonatkozásában javaslat érkezett arra vonatkozóan, hogy a BCR hatályát *a tagállamok közötti adattovábbításokra is ki kellene terjeszteni*. A harmonizált jogi környezetre tekintettel ennek csak csekély eredménye volna, megjegyzem, a javaslatot az uniós jogalkotó sem fogadta el.

A BCR személyi hatálya vonatkozásában alapvető hiányosság pótlására vonatkozó észrevételek érkeztek: a *vállalatcsoport* adatvédelmi jogi fogalmának szükségessége elvitathatatlannak látszik a BCR-t alkalmazni jogosultak körében. Felmerült a BCR alkalmazásának lehetősége a *közfeladatot ellátó szervek esetén*, azonban az Európai Tanács azt rögzíti, hogy nem lát olyan esetet, amikor ez megvalósulhatna. Az al-adatfeldolgozó és a munkavállalók automatikus a BCR hatálya alá rendelése is javaslatként fogalmazódott meg. A magyar javaslat[95] felveti, hogy BCR-t nemcsak profitorientált gazdasági társaságok, hanem nemzetközi szervezetek és más jogi személyek is alkalmazhatnának, amely látens módon[96] bele is került a magyar szabályozásba. Szektor-specifikus érvként érkezett, hogy a *BCR szektorális* kiterjesztése volna indokolt, különösen a légi fuvarozókra.

A BCR tárgyi hatályára és tartalmi elemeire vonatkozó szabályok tervezetei sem maradtak tagállami kritika nélkül. A BCR tartalmi elemeinek listája nem kerülhet kimerítő felsorolásként a GDPR szövegébe és több minimum tartalmi elemet helyesen „tartalmaz” (include) a BCR, de azok részletes leírása (description) nem a BCR tényleges tartalmi eleme.

Igény fogalmazódott meg arra, hogy a tartalmi elemek önállóan, esetenként meghatározott többlet elemekkel bővíthetők legyenek.

[95] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Partial General Approach on Chapter V, Brussels, 28 May 2014, 10349/14, 2012/0011 (COD)
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT
[2017. november 2.]
[96] Indokolás az V. fejezet 2. pontjában.

DOI: 10.14750/ME.2019.022

Az engedélyezési eljárás vonatkozásában javaslatok érkeztek olyan tartalommal, hogy az eljárási szabályok megalkotását nem a tagállamokra kellene delegálni, hanem az Európai Adatvédelmi Testület feladatául kellene tűzni az ott rendelkezésre álló szakmai tapasztalat és jó gyakorlat okán. Ugyanakkor mind az adatkezelői oldal mind a hatósági oldal az adminisztrációs terhek csökkentésének fontosságát helyezte előtérbe. Elvárásként fogalmazódott meg, hogy a vezető hatóság egyedüli hatásköre volna a BCR tárgyalások lebonyolítása és a társhatóságok jóváhagyásának megszerzése. Az egyesült királysági hatóság – már több tucat eljárás lefolytatását követően[97] – azon előzetes félelmét jelezte, hogy a hatóságokat elárasztathatják a BCR engedélyezések iránti kérelmek. Emiatt pedig az ellenkező hatás várható, vagyis az adatkezelők, a fennakadást elkerülendő a kivételekre alapítottan fognak eljárni az esetek többségében. Az engedélyezési eljárás egyébként is költségességes és hosszadalmas, ami további gátló tényezők az adatkezelők szempontjából.

Az országhatároktól független, azonos jogokat és védelmet biztosító jogi és technológiai környezet igénye nem csak a jogalkotó, hanem az egyének szintjén is megjelenik. Az Eurostat legfrissebb már 2015 tavaszán végzett felmérése[98] szerint *a megkérdezettek 89% százaléka tartja fontosnak,* hogy joghatóságtól függetlenül *ugyanazon jogok és védelem* illesse meg őket személyes adataik kezelése kapcsán. A GDPR megalkotása során különös jelentőséget kapott a Nemzetközi Vöröskereszt jogállása és adatkezelői minősége. E körben külön is nevesíteni kérte magát mint nemzetközi humanitárius szervezetet, amely harmadik országba irányuló adattovábbításait az érintett hozzájárulása nélkül, a létfontosságú érdekre hivatkozással végzi.[99]

[97] https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/ [2017. november 14.]
[98] A kördiagramm forrása: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf [2016. január 2.]
[99] http://data.consilium.europa.eu/doc/document/ST-8837-2015-INIT/en/pdf [2017. november 2.]

DOI: 10.14750/ME.2019.022

III.2.3. A GDPR reagál a megfogalmazott igényekre

Összességében a hatályos jogszabály szöveget vizsgálva – de még az első jogalkalmazási kérdések felvetődése és megoldása előtt – az rögzíthető, hogy a GDPR az előzetesen megfogalmazott társadalmi és állami igényekre, majd a tervezet egyes stádiumaiban tett javaslatokra reagál, többségében elfogadja azokat, erre – és a differenciált és szigorú szankciórendszerre is – tekintettel nagyfokú önkéntes jogkövetés várható, elméletileg.

A jogi környezet tagállami eltéréseire és a széttagoltságra a jogforrási szint megválasztásával adott egyértelmű választ az uniós jogalkotó.

Az érintettektől érkezett aggályokra válaszként új technológiákra reagáló új fogalmakat, jogokat és kötelezettségeket vezet be a GDPR, mint például a 4. cikk 4. pont szerinti profilalkotás, a 4. cikk 5. pont szerinti álnevesítés, a 20. cikk szerinti adathordozhatósághoz való jogot, a 32. cikk szerinti adatbiztonság szabályait, és a 33. cikk szerinti incidensjelentési kötelezettséget. Az érintett hozzájárulása körében egy régen várt jogalapot vezetett be a 6. cikk (1) bekezdés b) pontja, amely értelmében a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

A GDPR már kiemeli a genetikai és biometrikus adatokat, amelyek a személyes adatok ”különleges kategóriáját”[100] képezik.

A GDPR egészét áthatja egy új alapelvi szinten megfogalmazott szemlélet, amely szerint az *elszámoltathatóság elve* értelmében az adatkezelő felelős a megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására is.

[100] GDPR (51) preambulumbekezdés utolsó mondata

DOI: 10.14750/ME.2019.022

Ez az adatkezelőt is érdekeltté teszi a transzparens és pontos eljárásra. Az adatkezelők felvetésére reagálva a felelősség kérdésében is az eddigiektől merőben más szemléletet vezet be: az uralkodó elv, amely szerint az adatkezelő a felelős és viseli a bizonyítás terhét, megtörik, az adatkezelők és adatfeldolgozók számára is közel azonos felelősséget rögzít, így például a nyilvántartás vezetését, a felügyelő hatósággal kötelező együttműködést, az adatbiztonság biztosítását az incidens jelentése körében. A 28. cikk (2) bekezdése az al-adatfeldolgozó, a GDPR terminológiája szerint további adatfeldolgozó igénybe vételének feltételeként rögzíti az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazását és a (4) bekezdés a megbízó adatfeldolgozóra telepíti a felelősséget.

A GDPR, szintén az adatkezelők javaslatára, sok esetben meghagyja a cselekvési szabadságot az adatkezelő számára amikor akként rendelkezik, hogy az adatbiztonság körében a tudomány és technika állásának megfelelő intézkedések bevezetése szükséges. Ugyanígy a (64) preambulumbekezdés szerint „minden észszerű intézkedést megtesz a hozzáférést kérő érintett személyazonosságának megállapítására, különösen az online szolgáltatásokkal és az online azonosítókkal összefüggésben”, az elfeledtetéshez való jog online környezetben történő megerősítése érdekében is az „észszerű lépések” megtételét várja el. A Nemzetközi Vöröskereszt az elfogadott szövegben ugyan nevesítve nem jelenik meg, de az adatkezelés jogalapja a humanitárius okok fennállása esetén *természetes személy létfontosságú érdekeire* hivatkozással személyes adatkezelésre elvben sor kerülhet, ha más jogalap nincs. A *fontos közérdek* teremti meg az adatkezelés jogszerűségét akkor, ha a genfi egyezmények által előírt feladat elvégzése, illetve a nemzetközi humanitárius jog fegyveres konfliktus esetén alkalmazandó rendelkezéseinek történő megfelelés alapján valamely nemzetközi humanitárius szervezet számára olyan érintett személyes adatait továbbítják, akinek fizikailag vagy jogilag nem áll módjában a hozzájárulás megadása.

DOI: 10.14750/ME.2019.022

A konkrét tagállami javaslatokra tekintettel a BCR és a vállalkozáscsoport fogalma a 4. cikk fogalommeghatározásai körében deklarálásra került. Noha a szektorális BCR-ek nem is nyertek jogi elismerést, a 46. cikk a megfelelő garanciák alapján történő adattovábbítások körében a (2) bekezdés b) pontjaként deklarálja a BCR jogi elismerését és alkalmazhatóságát valamennyi tagállamban a harmadik országba irányuló adattovábbítások esetére. Ezzel a GDPR megszünteti az adattovábbításokat megelőző tagállami hatóság felé történő bejelentéssel illetve jóváhagyással - már amelyik tagállamban ilyenre szükség volt - járó adminisztrációs nehézségeket, és a szerződéses klauzulák a tömeges adattovábbítások esetére való alkalmazhatatlanságának problémájára is alternatívát biztosít. Noha arról még nincs egyértelmű álláspont, hogy a már jóváhagyott BCR-ek alkalmazhatók maradnak-e 2018. május 25. napját követően, az Európai Bizottság elfogadta azon tagállami javaslatokat, hogy csak a kötelező minimum tartalmi elemeket deklarálja a 47. cikk (2) bekezdése. Az engedélyezési eljárások tagállami hatáskörben maradtak, mind az anyagi jogi vizsgálat, mind az eljárásjogi kérdések, az adatkezelők és a felügyeleti hatóságok között folytatott információcsere módját a (3) bekezdés szerint mégis az Európai Bizottság határozhatja meg. Ezidáig ilyen végrehajtási jogi aktus nem készült. A 2014-es magyar javaslatra, amely az alkalmazás személyi körét érintette, nem született egyértelmű megoldás. Ezt a magyar jogalkotó úgy hidalta át, hogy álláspontom szerint *bizonytalan jogfogalmat alkotott a „kötelező szervezeti szabályozás" bevezetésével*.[101] A további adatfeldolgozó a BCR hatálya alá nem került be ex lege. Szerződéses kapcsolatban áll az adatfeldolgozóval, aki ugyancsak írásbeli szerződéses viszonyban áll az adatkezelővel. Ha a javaslat átment volna és a további adatfeldolgozó a BCR hatálya alá kerül, szerződéstani szempontból a vállalkozó alvállalkozóját kellett volna a megrendelő egyoldalú kötelezettségvállalása alanyává tenni. A jelen helyzet viszont az érintett számára hátrányos, hiszen így az adatok további feldolgozására nem terjed ki a BCR hatálya és az így biztosított garancia sem.

[101] Részletesen lásd az V. fejezetben.

DOI: 10.14750/ME.2019.022

III.3. Generáció- és paradigmaváltás

Meggyőződésem, hogy az adatvédelmi szabályozás következő, szándékosan nem számozom hányadik, generációja bevezetésének küszöbén állunk. Az alábbiakban csak röviden vázolom az eddigi korszakokat és arra törekszem, hogy bizonyítsam, valóban *új generáció van megszületőben* és bemutassam, hogy hogyan illik bele a paradigmaváltás körébe a BCR jogi elismerése.

III.3.1. A generációk egymásra épülő története

Az adatvédelmi pozitív jogi szabályozás története noha csak az 1970-es évekre nyúlik vissza, elvi megalapozását a szakirodalom elvitathatatlanul dedikálja Warren és Brandeis „The Rigth to Privacy"[102] című 1890-ben megjelent tanulmányának. A szerzők a bulvár sajtót és az abban közzétett pletykát valamint a korszakalkotó fotótechnikát[103] azonosították a magánszférát fenyegető legégetőbb veszélyként. Megfogalmazták a *magánszféravédelem filozofikus alapelvét,* amely szerint jogilag el kell ismerni, hogy az ember fizikai testén és dolgain túl jogi védelem illeti a magánszférát is, elkülönülve a szellemi alkotások és más személyiségi jogok jogi védelmétől, a rágalmazás vagy becsületsértés büntetőjogi szankcionálásától, azaz *jogunk van arra, hogy egyedül legyünk* (right to be let alone).

Ma ezt információs önrendelkezés forrásának neveznénk, azaz jogunk kell legyen ahhoz, hogy saját adataink felett rendelkezzünk, csak azt bocsássuk mások rendelkezésére, amelyről mi magunk döntünk ekként, és megismerhessük és meghatározhassuk adataink későbbi sorsát.

[102] WARREN – BRANDEIS (1890) p. 193-220.
[103] 1888-ban megszületett a Kodak név és a „Te csak nyomd meg a gombot – mi elvégezzük a többit" szlogen, amely új korszakot nyitott a fényképezés történetében: a pillanatfelvételek készítésének lehetőségét biztosította a cég legújabb kézi fényképezőgépe. Forrás: https://www.kodak.com/corp/aboutus/heritage/milestones/default.htm [2017. november 03.]

DOI: 10.14750/ME.2019.022

A tanulmány nyomán és a technológia rohamos fejlődésére tekintettel, a korábban jellemzően papíralapú adatkezelést számítógépes nyilvántartások váltották fel Európában, megszülettek az első, az állami nyilvántartások számítógépes kezelését szabályozó nemzeti jogszabályok[104] és a nemzetközi soft law jellegű jogforrások[105]. Elfogadott alapelvi álláspont lett az, hogy „kerüljék, hogy […] korlátokat szabnak a személyes adatok határokon átívelő áramlásának". Ezt valamennyi felosztás[106] *a szabályozás első generációjaként* határozza meg. A szabályozás célja a nagy állami, automatizált adatbázisok kialakításának, összekapcsolásának, elemzésének féken tartása és átlátható működtetésének megteremtése volt, még ha Warren és Brandeis alapvetően a magánjogi viszonyokból indult is ki és alkalmazta elméletét.[107]

Szőke[108] az első generáció öt fő jellemzőjét emeli ki, így a szabályozás:
- célja az állami adatbázisok átláthatóságának biztosítása;
- hatálya az automatizált adatkezelésekre terjedt ki;
- az érintettek számára csak néhány részjogosítvány biztosított (a betekintés és helyesbítés joga);
- érvényesüléséhez ombudsman jellegű vagy hatáskörökkel felruházott felügyelő hatóság szükséges;
- az adatkezelések nyilvántartásba való bejelentését írta elő.

Jóri[109] éppen azt emeli ki e vonatkozásban, hogy nem is tekinthetők adatvédelmi törvénynek az első generációs szabályok bizonyos értelemben, mivel „tárgyuk elsősorban a nyilvántartást szolgáló technológia volt."

[104] Például 1973-ban Svédországban, 1978-ban Dániában.
[105] Gazdasági Együttműködési és Fejlesztési Szervezet: Áttekintés OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, 2003 http://www.oecd.org/sti/ieconomy/15590228.pdf [2017. november 02.] és az Európa Tanács az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény, amelyet hazánk a 1998. évi VI. törvénnyel hirdetett ki.
[106] A generációk felosztásában, számozásában több elmélet ismert, például a magyar jogirodalomban első Majtényi, őt követi Jóri, és ismert a Mayer-Schönberger-féle, valamint Bodenschatz és Hegedűs Bulcsú korszakolása is. Én Majtényi felosztását követem a korszakok számozásban.
[107] SZŐKE (2015) p. 28.
[108] i.m. p. 35.
[109] Jóri (2009) p. 29.

DOI: 10.14750/ME.2019.022

Közvetlen céljuk nem az adatvédelem volt, hanem a végrehajtó hatalom információs túlsúlyának visszaszorítása. A szabályozás egészen addig volt megfelelő, míg a ’80-90-es évekre a technológiai fejlődése és az internet megjelenése okán meghaladottá nem vált. Innentől válik differenciálttá a korszakolás az egyes szerzőknél, én Majtényi felosztását[110] követem. A második generációs szabályozás Majtényi szerint már technológiasemleges, nemcsak az automatizált adatkezelésekre terjed ki.

Majtényi korszakolásában a harmadik, mikor 1995. évben az Európai Uniós jogalkotó, már látva a korábbi hiányosságokat, a 95/46/EK irányelvben rögzíti az adatvédelmi szabályozás főbb irányait és az átültetendő szabályokat, amely hatálya kiterjedt a személyes adatok részben vagy egészben automatizált módon történő feldolgozásra, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni. Azt azonban nem lehetett figyelmen kívül hagyni, hogy két alapvető érdek került szembe egymással: a személyes adatok gyűjtése és hatékony felhasználása a gazdasági integráció, a globális gazdaság és a kialakuló információs társadalom záloga és motorja, viszont az érintettek magánszférája egyre inkább védtelen marad, az információs önrendelkezési jog gyakorolhatósága egyre nehezebb, olykor esélytelen. Történik mindez egy olyan időszakban, amikor megszületett a Német Szövetségi Alkotmánybíróság ún. népszámlálás-ítélete 1983. évben, amely jól illett az érintetti jogok erősítésére törekvő európai tendenciába.[111]

Mindezzel párhuzamosan Európában a nemzeti jogalkotások is adatvédelmi törvények sorát készítik el, nemcsak a jogharmonizációra köteles (tag)államok: hazánk és Csehszlovákia 1992-ben, Lengyelország 1997-ben.

[110] Majtényi (2003) p. 577-635
[111] SZŐKE (2015) p. 43.

DOI: 10.14750/ME.2019.022

A szabályozás hatályát már nemcsak az állami, hanem *a piaci szereplők adatkezelési tevékenységére is kiterjeszti* a jogalkotó.

Szőke[112] a második és harmadik generáció tíz fő jellemzőjét emeli ki, amelyek szerint a szabályozás:
- kiterjed az állami adatéhséggel vetekedő piaci szereplők adatkezelésére is;
- technológiasemleges, a számítógépes és a manuális adatkezelés is hatálya alá tartozik;
- alapjogi minőséget nyert, különösen az Alapjogi Charta 2000. évi aláírásával, amelyben a 7. cikk a magán- és a családi élet tiszteletben tartását, a 8. cikk a személyes adatok védelmét deklarálja;
- az érintett szerepét és rendelkezési jogosítványait helyezi előtérbe, bízva abban, hogy a jogosítványokkal élni fog és így aktív közreműködője lesz az adatkezelési eljárásoknak;
- erős paternalista szemléletű korlátozásokat tartalmaz az adatkezelőkre nézve;
- jellemzője, hogy megjelennek a szektorális szabályok;[113]
- jellemzője, hogy hangsúlyos az érintett hozzájárulása, mint az adatkezelés jogalapja, és megjelennek más jogalapok is;
- erősíti a felügyelő hatóságok szerepét;
- egyszerűsíti a nyilvántartásba vételi kötelezettséggel járó terheket;
- megteremti a megfelelő védelmi szint fogalmi körét és harmonizálja a harmadik országba irányuló adattovábbítások szabályrendszerét.

Székely[114] érzékletesen jellemzi ezt az időszakot, mikor megfogalmazza, hogy a technológiai fejlődés következtében a magánélet hagyományos határai folyamatosan erodálódnak. A szabályozás igyekezett reagálni a technológiai fejlődésre, a szabályozás kiterjedt a piaci szereplőkre is, a középpontba az érintetti kontroll került. Hamar rá kellett jönni azonban, hogy *a személyes adatok védelme kevéssé biztosítható az érintetti kontroll gyakorlásával*.

[112] SZŐKE (2015) p. 49.
[113] Megjegyzem, Majtényi ezt a jellemzőt a harmadik generációhoz kapcsolja.
[114] SZÉKELY – BALOGH – JÓRI – FÖLDES (2004) p. 49.

DOI: 10.14750/ME.2019.022

Az online világban az adatkezelések *átláthatatlanná* váltak, és az érintettek csak akkor gyakoroltak tényleges kontrollt – utólag, gyakran hatástalanul és a reparáció esélye nélkül, ha pénzben mérhető kár érte őket. Elterjedt az „internet nem felejt" jelmondat, ami az esetek többségében igaznak bizonyult. Az érintett *hozzájárulásának megszerzése az adatkezelő erőfölényéből adódóan aligha minősíthető önkéntesnek*, pedig az adatkezelések jogalapját szinte mindig erre az aktusra alapítják. A WEB2.0 elterjedésével az érintett egyszemélyben adatalany és adatkezelő, a tartalom szolgáltatója is. A felhőszolgáltatók, az okos eszközök és a dolgok internete, a drónok reptetése, a profilozás és a viselkedés alapú marketing mindennapossá vált.

III.3.2. Paradigmaváltás, az új generáció igazolása

Szőke számos társadalmi, technológiai és gazdasági hatás nyomán rögzíti, hogy a szabályozás alapjainak újragondolására, újgenerációs adatvédelmi szabályozásra van szükség.[115] A fejlesztési irányok között kiemeli az *elszámoltathatóság elvének rögzítését*. A GDPR 5. cikk (2) bekezdésében elismerést nyert alapelv értelmében az adatkezelő felelős a megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. Szőke szerint az elv lényege, hogy a „szervezet felelősségét komolyan véve" kell kialakítani a belső irányítási struktúrát, eljárásrendeket és szervezeti kultúrát, amellyel elérhető a megfelelés. Az elvnek azonban van egy további vetülete, a megfelelés igazolása. Vagyis az adatkezelőnek képesnek kell lennie utóbb meg is mutatni, bizonyítani, azaz igazolni, hogy a tevékenysége valóban jogszerű volt. A GDPR hatályos szövegében ez több szabályban megjelenik.

Először a (76) preambulumbekezdés rögzíti, hogy „ahhoz, hogy az adatkezelő igazolni tudja az e rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik […] az adatvédelem elveit.

[115] SZŐKE (2015) p. 81.

DOI: 10.14750/ME.2019.022

Igazolási kötelezettség jelenik meg explicite továbbá az érintett hozzájárulásának megadása körében a 7. cikk szerint, az adatkezelő és adatfeldolgozó közötti jogviszonyban a rendelkezésre bocsátandó információk körében, amelyek a kötelezettségek teljesítésének igazolásához szükségesek a 28. cikk szerint. Az adatvédelmi hatásvizsgálat is kiterjed a kockázatok kezelését célzó intézkedések bemutatására, amelyek a GDPR-ral való összhang igazolását szolgálják.

Az elv megvalósításához a BCR akként illeszkedik, hogy abban illetve annak alkalmazásával valóban kialakul egy belső intézményi szervezeti rend, szabályozási koncepció és konkrét végrehajtható előírások, panaszkezelési mechanizmus illetve felelősség telepítés.

Ezek az elszámoltathatóság alapvető kellékei. Ezen túl az utólagos igazolás sem kérdéses a BCR hatósági jóváhagyása és nyilvánossága okán. Jóri[116] is kiemeli, hogy a szabályozás hiányosságait, azaz az állami szabályozást kiegészítheti az ön- illetve társszabályozás, amely valójában az állami szabályozás kivédésére, elhárítására szolgál, amerikai mintára.[117] Szőke[118] a paradigmaváltást egyenesen az önszabályozás, az audit és a tanúsítás körében azonosítja. A BCR-t a *belső szabályozások* kategóriájába sorolja.

Összességében három, a kutatási téma fókuszába tartozó szabályozási tendenciát azonosítok az alábbiak szerint.

Az *első szabályozási tendencia*, hogy a GDPR ez eddigi szabályozáshoz képest számos előnyt biztosít a magatartási kódexeket, a tanúsítást, az ön- és társszabályozási módszereket alkalmazó adatkezelők számára.

[116] JÓRI (2009) p. 285.
[117] Részletesebben az amerikai mintáról lásd a X fejezetben.
[118] SZŐKE (2015) p. 118-145.

DOI: 10.14750/ME.2019.022

A szabályozások sikere mindig a konkrét rendelkezések természetén, a megvalósíthatóság hatékonyságán és a megfelelési hajlandóságon múlik. Mivel joghézagok adódhatnak és az alkalmazási nehézségek a gyakorlatban mutatkoznak meg, így a jogi szabályozás kiegészítésére lehet szükség, amelynek egyik módja lehet az ön- és társszabályozás, amely nem helyettesítheti, csupán kiegészíti a jogi szabályozást.[119] Az önként létre hozott szabályokat olyannyira rugalmasra és gyorsan adaptálhatóra szabják, hogy a változó technológiai, gazdasági és sturkturális viszonyokra alkalmazni tudják annak érdekében, hogy a cégek erősítsék ügyfeleik bizalmát.
A társszabályozás azt jelenti, hogy a piaci szereplő és az állami szervekkel együtt dolgozza ki a szabályokat, míg az önszabályozás esetében klasszikusan a gazdasági szektor szervezetei, például kamarák és érdekképviseleti szervek alkotnak szabályokat és tartatják azokat be a cégekkel.

Ebben a tekintetben a BCR a társszabályozás és az önszabályozás egy új, hibrid, kevert válfaja, ugyanis a szabályokat maga a cég alkotja akként, hogy annak megfelelőségét a nemzeti hatóságok megvizsgálják, adott esetben módosíttatják, és engedélyezik.

A *második szabályozási tendencia*, hogy a GDPR számos esetben kötelezővé teszi az adatvédelmi hatásvizsgálatok és auditok elvégzését a megelőzés jegyében, és inkább prevenciós mint szankcionáló céllal bevezeti az incidensjelentési kötelezettséget, amely a növekvő adatkezelői és adatfeldolgozói tudatosság elvárását példázza, csakúgy mint a beépített védelem és az alapértelmezett adatvédelem.

A szabályozási generáció váltást támasztja alá az is, hogy megjelentek a személyes adatot – amerikai mintára – a tulajdonjog tárgyaként azonosító szabályok is.[120]

[119] CASTRO (2011) p. 1-3.
[120] PURTOVA (2017)

DOI: 10.14750/ME.2019.022

Ilyen az adathordozhatósághoz való jog, amely bevezetésének célja az volt, hogy egyrészt az érintett valódi kontrollt gyakoroljon adatai sorsa felett, másrészt aktív szereplője lehessen azoknak a gazdasági folyamatoknak, amelyeknek a személyes adatai is a motorját képezik.[121]

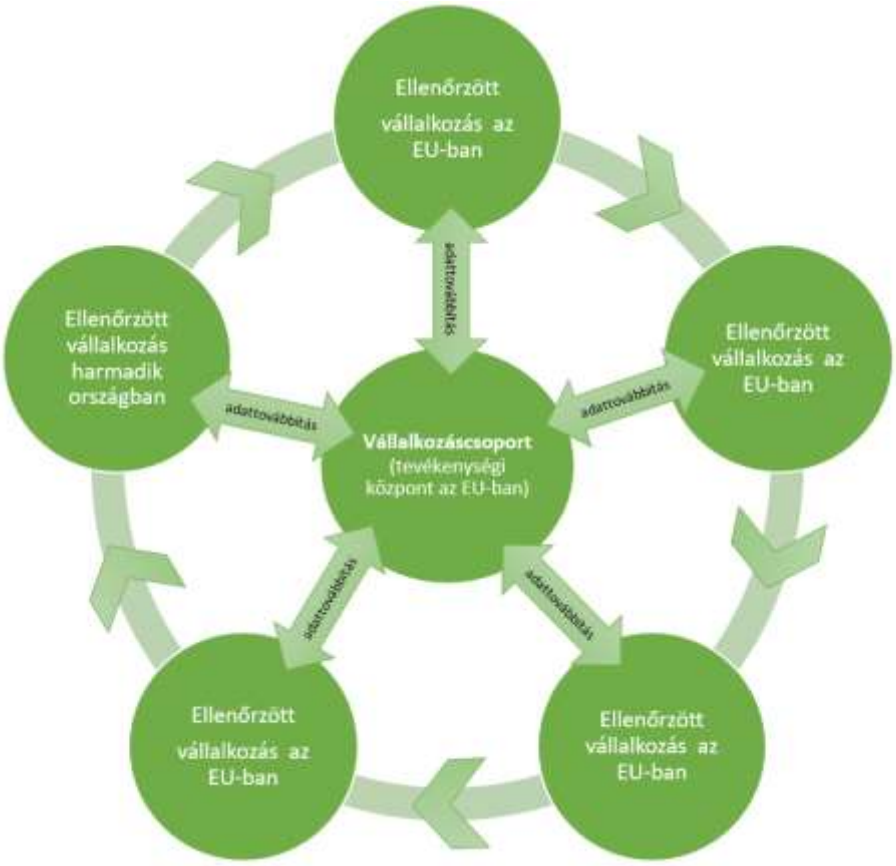
A *harmadik*, hogy a harmadik országokba irányuló adattovábbítás szabályozását a korábbiaktól sokkal részletgazdagabban, több megfelelőségi módot biztosítva szabályozza, igazodva a gazdasági szereplők elvárásaihoz, olykor az érintettek hátrányára. Ebben a szabályozási körben pedig eddig nem tapasztalt módon követeli meg a nemzetközi együttműködést a nemzeti felügyelő hatóságok egymás közötti és az adatkezelő gazdasági szereplőkkel való ügyintézések során.

[121] Article 29 Working Party, 'Guidelines on the right to data portability', 5 April 2017, 16/EN WP 242 rev.01., 4, fn 1

DOI: 10.14750/ME.2019.022

IV. FEJEZET
A HARMADIK ORSZÁGOKBA IRÁNYULÓ ADATTOVÁBBÍTÁS SZABÁLYOZÁSI KÖRNYEZETE

A személyes adatok továbbításának napjainkban már nem a távolság vagy az országhatárok szabnak gátat, hanem az eltérő jogrendszerek előírta korlátozások. Nem újszerű az olyan multinacionális cégstruktúra, amely esetében a vállalkozáscsoport egyes tagjainak az Európai Unió valamely tagállamában van a tevékenységi központja, másoknak harmadik országokban, és a vállalkozáscsoporton belül belső személyes adatokat továbbítanak, például adminisztratív célból vagy az ügyfelek illetve az alkalmazottak személyes adatainak a kezelését más-más vállalkozási tag látja el.



1. ábra: Vállalkozáscsoport struktúra minta[122]

[122] Az ábra KUNER (2003) p. 169. ábrája alapul vételével készült.

DOI: 10.14750/ME.2019.022

A fentebb vázolt struktúrát tekintve az adattovábbítások szempontjából komplex jogi helyzet előtt állhat az az adatkezelő, aki nem tudatosan jár el az adatvédelmi szabályozás egyre inkább adatkezelő-központú útvesztőjében.

A személyes adatok továbbítására vonatkozó általános elvek nem különböznek, ha a vállalkozáscsoporton belüli továbbítások címzettje harmadik országban található tag, viszont a tételes jogi szabályozás reformja kellett ahhoz, hogy feloldható legyen számos nehézkes gyakorlat. Ha a fenti – igencsak leegyszerűsített – struktúrára tekintünk még a GDPR alkalmazását megelőzően, akkor 28, a harmonizált jogi környezet ellenére is különböző EU tagállami szabályozás valamint az Adatvédelmi Irányelv szabályai határozzák meg az EU-n belüli tagok közötti adatáramlás valamennyi részletét, főszabályként a harmadik országba irányuló továbbítás szabályait és az Adatvédelmi Irányelv extraterritorriális hatására[123] tekintettel a harmadik országokban történő adatkezelés illetve adatfeldolgozás lehetőségeit is. A területiség elve, amely a joghatóság kérdésének sarok köve, az államhatárok és a hatósági illetékesség kérdései az adatvédelem európai uniós és nemzetközi szabályozásában eltűnni látszik, mivel az új jogi eszközök és előírások formálisan a területiség és a joghatóság elvére épülnek, azonban hatással vannak a harmadik országbeli adatkezelőkre és adatfeldolgozókra.[124]

A továbbiakban a harmadik országba irányuló adattovábbítás Adatvédelmi Irányelvi és a GDPR szerinti szabályainak változását - és azonosságait - vizsgálom, kitekintve hazánk szabályozására, kiemelve a BCR jogi elismerésének indokoltságát és már látható valamint várható hatásait.

[123] KUNER (2015) p. 1-18.
[124] RYNGAERT (2015) p. 221.

DOI: 10.14750/ME.2019.022

IV.1. A megfelelés nehézségei az alkalmazandó jog szempontjából

A harmadik országba irányuló vállalkozáscsoporton belüli adattovábbítások folyamatának adatvédelmi szabályanyagát az 1. sz. ábra segítségével az alábbiak szerint azonosíthatjuk:

- Amennyiben az Európai Unió tagállamának területén történő adatkezelést az adatkezelő vállalkozáscsoporti tag végzi és az Európai Unió tagállamának területén adatkezelést végző tagnak továbbít személyes adatokat, úgy az alkalmazandó jog az Adatvédelmi Irányelv szabályai, valamint a küldő és a címzett tagállam nemzeti joga volt; 2018. május 25. napjától irányadó a GDPR annak 3. cikk (1) bekezdése első fordulata alapján és azon szabályok vonatkozásában a küldő és a fogadó tagállam joga, amelyek megalkotását a GDPR tagállami hatáskörbe utalja.

- Amennyiben az Európai Unió tagállamának területén történő adatkezelést az adatkezelő vállalkozáscsoporti tag végzi és harmadik ország területén adatkezelést végző tagnak továbbít személyes adatokat, úgy alkalmazandó jog az Adatvédelmi Irányelv szabályai voltak a küldő adatkezelő vonatkozásában, bizonyos esetekben az Adatvédelmi Irányelv 4. cikk c) pontja alapján az adattovábbítás címzettje vonatkozásában is, és a címzettre irányadó nemzeti jog is alkalmazandó volt a címzett adatkezelő vonatkozásában; 2018. május 25. napjától a küldő adatkezelőre alkalmazandó a GDPR, és az érintett személyétől illetve tartózkodási helyétől függően a GDPR 3. cikk (2) bekezdése alapján a fogadó harmadik országbeli adatkezelőre is irányadó lehet. Érdekes helyzetet teremt, amikor egy harmadik országban letelepedett adatkezelő és egy harmadik országbeli állampolgár személyes adatának kezelésére az uniós jog, a GDPR lesz az irányadó, mivel a „rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Európai Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére” is, ha áruknak vagy szolgáltatásoknak az Unióban

DOI: 10.14750/ME.2019.022

tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell- e azokért; vagy az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó. Tehát egy olyan jogviszonyban kell majd alkalmazni a GDPR szabályait, amelynek egyik alanya sem áll az uniós jog hatálya alatt. Ilyen eset például olyan weboldal üzemeltetője, amely harmadik országban székhellyel rendelkező cég, és uniós tagállam területén igénybe vehető szolgáltatást kínál – például ingatlan rövid távú bérbe adása, városnéző séta szervezése – és online regisztrációhoz valamint személyes adatok kötelező szolgáltatásához köti a szolgáltatás igénybevételét a harmadik országbeli turisták számára. A GDPR területi hatálya tehát erős extraterritorriális jelleget mutat, erős alapjogvédelmi szemlélettel.

- Külön kiemelést érdemel az USA-ba irányuló adattovábbítások jogi megítélése a post-Schrems[125] időszakban, mivel a megfelelő védelmi szint biztosítására az adatkezelőknek egyéni és egyedi megoldást kellett találniuk. A 2016. július 12. napján elfogadott Adatvédelmi Pajzs azon cégek számára jelent csak megoldást, amelyek megfelelési nyilatkozatukkal vállalják a keretrendszer alapelveinek és szabályainak való megfelelést, ez azonban nem biztosítja valamennyi, az USA-ba történő adattovábbítás vonatkozásában a megfelelő védelmi szintet.

A GDPR alkalmazásának kezdeti bizonytalanságait a tagállami jogalkotások is eltérően közelítették meg.

[125] A szakirodalom a C-362/14. sz. ügyben (A Bíróság ítélete (nagytanács), 2015. október 6., Maximillian Schrems kontra Data Protection Commissioner; ECLI:EU:C:2015:650) meghozott ítéletet követő időszakra utal így, t.i. az ítélet megállapította a 2000/520 határozat érvénytelenségét, amely alapján a Safe Harbor rendszerhez önként csatlakozó cégek USA-ba irányuló adattovábbításának jogszerűségét biztosította a megfelelő védelmi szint vonatkozásában.

DOI: 10.14750/ME.2019.022

Míg Németországban már 2017 tavaszán[126] megtettek minden szükséges jogalkotási lépést a GDPR alkalmazása kapcsán és 2018 februárjában a tagállamok többségében már volt benyújtott törvénymódosítási javaslat[127] – hazánkban ekkor még nem volt –, 2018 májusára Németországon túl mindössze további 10 tagállamban hirdették ki a nemzeti szabályokat.[128]

Tekintettel arra, hogy hazánkban a jogalkotás nem reagált a GDPR alkalmazására 2018. május 25. napjáig érdemben, a NAIH a jogkövetést segítő közleményt[129] adott ki az alkalmazandó szabályokról. Az Infotv. 2018. júliusi módosítása azonban az alapvető kérdésekre választ adott. Az Infotv. 2. § (2) valamint (4) bekezdése taxatív módon sorolja fel azon rendelkezéseket, amelyek a GDPR hatály alá tartozó jogviszonyok esetében alkalmazandók a GDPR mellett.

Az alkalmazandó jog körében bonyolítja a helyzetet, ha a vállalkozáscsoport központja a harmadik országban van és uniós polgárok személyes adatainak kezelését, továbbítását végzi. Ugyanis a GDPR szabályai alkalmazandó ezen cégre is, ha az Európai Unióban tartózkodó polgárok adatainak kezelését végzi vagy az Unión belüli magatartásuk megfigyelésére vonatkozik. Kuner[130] egyik lehetséges jó megoldásként javasolja, és fontos előnyöket irányoz elő a fenti helyezetekre akként, hogy a vállalkozáscsoporton belüli adattovábbításokra magatartási kódexek létrehozását tartotta támogathatónak, már 2003-ban. Mára az alkalmazandó jog megállapításának nehézségei nem változtak, viszont nagy hangsúlyt kapott az adatvédelmi önszabályozás és a magatartási kódexek, a BCR is ismert megoldási lehetőségként vehető igénybe.

[126] 2017. július 5. napján jelent meg a német hivatalos lapban a törvény.
[127] https://www.lw.com/admin/Upload/Documents/LW-FINAL-GDPR-National-Implementation-Tracker-Feb2018.pdf [2018. márciusz12.]
[128] Ausztriában, Belgiumban, Horvátországban, Dániában, Franciaországban, Írországban, Olaszországban, Hollandiában, Svédországban és az Egyesült Királyságban.
[129] A személyes adatok védelmére vonatkozóan alkalmazandó előírások http://naih.hu/files/2018-05-25-GDPR-koezlemeny.pdf [2018. május 25.]
[130] KUNER (2003) p. 174.

DOI: 10.14750/ME.2019.022

Hazánk a jogalkotás során azt az álláspontot képviselte, hogy a GPDR szabályait „elsősorban a tagállami jogrendszerek közötti különbséget kihasználó multinacionális gazdasági társaságok ellen fellépve szükséges alkalmazni”.[131] Nem volt ismeretlen az a *fórum shopping* típusú jelenség, hogy egyes cégek a székhelyüket, szerverüket olyan tagállamban telepítették, ahol a tevékenységeik szempontjából a számukra legkedvezőbb szabályokat érvényesítő országokban végezzék az adatkezelési tevékenységüket.

Kiemelendő ugyanakkor, hogy az Adatvédelmi Irányelv vonatkozásában megfogalmazott, az alkalmazandó joggal kapcsolatos kérdések miatt a GDPR elvi szinten változtatja meg az alkalmazandó jogra vonatkozó szabályokat, különösen a harmadik országba irányuló adattovábbítások esetében, amely szabályok körében a 29. cikk szerinti adatvédelmi munkacsoport 8/2010. számú véleményében foglaltakat figyelembe véve döntő kritériumként az EU-s adatalany személye és adatai lesznek.

Kiemelt szerepet kap a tagállami képviselő kijelölése is. Megjegyzem, az Európai Unió Bírósága[132] már 2015. évben kimondta, hogy „egy külföldi államban regisztrált cég tevékenységére is alkalmazható a magyar jog, amennyiben tevékenysége magyarországi felhasználókra irányul […], a formális letelepedés nem nehezítheti meg az adatalanyok jogainak érvényesítését.”[133] Így a GDPR már a kialakult bírói gyakorlat szerint határozza meg területi és személyi hatályát.

[131] Iromány száma: T/335. Parlex azonosító: W838KPW50003, Általános Indokolás
[132] C-230/14. ECLI:EU:C:2015:639
[133] A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye az Európai Unió Bíróságának a Weltimmo-ügyben hozott ítéletéről https://www.naih.hu/files/2015-10-03-Kozlemeny---Weltimmo-itelet.pdf

DOI: 10.14750/ME.2019.022

Olyan esetekben tehát, amelyekben adattovábbítás történik harmadik országban letelepedett adatkezelő részére, az érintettek személyes adatainak védelme kiemelt jelentőséget kap a jogellenesség megelőzése és a jogérvényesítés lehetőségének biztosítása érdekében. Ugyanakkor az adatkezelők és adatfeldolgozók is nehéz helyzetben vannak, mivel adott esetben az uniós jogon túl több (tag)állam szabályainak és hatóságainak is meg kell felelniük, amely jogbizonytalanságot - és valószínűsíthetően további adminisztratív és működési költséget - okoz számukra. Mindez pedig elvezet a joghatóság kérdéskörének vizsgálatához, azaz azon olyan kérdésekre kell választ találni, hogy melyik tagállam hatósága lesz jogosult eljárni egy, a fenti struktúra szerinti vállalkozáscsoport esetében.

IV.2. Az eljáró hatóság meghatározása

A GDPR 2018. május 25. napjától kötelező és közvetlen alkalmazására tekintettel a legtöbb nemzeti hatóság, így a NAIH is kiadta iránymutatását,[134] amely 12 lépésben foglalja össze a legfontosabb teendőket.

Ezek között szerepel az adatvédelmi felügyeleti hatóság illetékességének vizsgálata is, amely bonyolultságát igazolja, hogy számos további praktikus kérdés várt értelmezésre és magyarázatra, amelyek vonatkozásában a 29. cikk szerinti Adatvédelmi Munkacsoport iránymutatása[135] világított rá. A *fő felügyeleti hatóság kiválasztásának szempontjait* azonban csak a határokon átnyúló adattovábbítások esetén alkalmazható, mert a harmadik országba irányuló adattovábbítások esetén alkalmazandó BCR jóváhagyására a WP 107 határoz meg szempontokat.

[134] NAIH: Felkészülés az Adatvédelmi Rendelet alkalmazására 12 lépésben http://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html [2017. december 18.]
[135] A 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás az adatkezelő vagy az adatfeldolgozó fő felügyeleti hatóságának meghatározásához, WP 244 rev.01, 2017. április 5., https://naih.hu/files/Iranymutatas-az-adatkezel--vagy-az-adatfeldolgozo-f--feluegyeleti-hatosaganak-meghatarozasahoz.pdf [2018. február 04.]

DOI: 10.14750/ME.2019.022

Az Infotv. hatálya egyben megalapozza a NAIH illetékességi területét is, ugyanakkor a határokon átnyúló adatkezelések esetén egy fő felügyeleti hatóság lesz jogosult eljárni, amely az érintett többi felügyeleti hatósággal információcserét folytat és együttműködik, valamint hatáskört ruházhat át. A *személyes adatok határokon átnyúló adatkezelésének* fogalmát a GDPR 4. cikk 23. pontja határozza meg, azonban az kizárólag az *Európai Unió több különböző tagállamában végzett tevékenység* besorolására szolgál alapul. Itt felhívom a figyelmet arra, hogy az adattovábbítás fogalma harmadik országokba, harmadik országon belüli területekre és meghatározott ágazatoknak vagy nemzetközi szervezetek részére történő adattovábbítást jelent, így nem tartozhat ezen fogalmi körbe. A joghatósági kérdések vizsgálatának elméleti és elvi célja, hogy meghatározza azt, hogy melyik az az állam és hatóságai, amelyek jogosultak eljárni egy adott ügyben. Az adatvédelmi ügyekben elsősorban nem az államok léptek fel joghatóságuk megállapítása érdekében, hanem az adatkezelők fejezték ki aggályukat az iránt, hogy *extraterritorriális hatású* jognak kell megfelelniük.

Egy hazai vonatkozású eset[136] már az Adatvédelmi Irányelv vonatkozásában is joghatósági kérdéseket vetett fel, amely körében az Európai Unió Bírósága[137] kimondta, hogy „egy külföldi államban regisztrált cég tevékenységére is alkalmazható a magyar jog, amennyiben tevékenysége magyarországi felhasználókra irányul […], a formális letelepedés nem nehezítheti meg az adatalanyok jogainak érvényesítését.” Az azonban elismerhető, hogy a joghatóság kérdésén túl számos további, mélyebb tartalom húzódik meg a fenti kérdéskör fölött, mint például a terrorizmus elleni harc és a nemzetközi, digitális kereskedelmi folyamatok zavartalansága. A joghatóság pusztán az államhatáron vagy a nemzeti jogon alapuló kérdése azonnal nemzetközi vetületet kapott, amikor az adattovábbítások megítélése a feladat.

[136] NAIH-510-6/2012/H
[137] C-230/14. ECLI:EU:C:2015:639

DOI: 10.14750/ME.2019.022

Az adatvédelem körében az a már-már gyakorlattá vált megoldás látszott megvalósulni, hogy a külföldi személyekre a nemzeti illetve uniós adatvédelmi jogot csak bizonyos arányossági követelményeket figyelembe véve alkalmazták.[138] Erre a Safe Harbor mechanizmus kiváló példa, és látjuk, hogy meg is bukott. Így a GDPR minden eddigi mintától eltérően kiterjesztő hatálya és alkalmazási köre egyértelműbb helyzetet teremt majd, azonban a végrehajtás és a kikényszerítés, amennyiben az adott cégnek nincs az Európai Unión belül tevékenységi helye, ugyanúgy nehézkes marad.

Míg Kuner a fenti arányosság elvén nyugvó, a joghatóságok tágító extraterritorriális hatású megoldást támogatja - beismerve ugyanakkor, hogy ez a nemzeti jogok konfliktusát és jogérvényesítési nehézségeket eredményezhet -,[139] addig Svantesson[140] sokkal inkább egy letisztultabb és szűkítő joghatósági megoldást várna el, szerinte a GDPR hatályára vonatkozó szabály alkalmazhatatlan lesz – a pénznem alapján eldönthető-e például, hogy a szolgáltatást kinek kínálja az adatkezelő. Az extraterritorrális adatvédelmi szabályozás alapját abban látja, hogy az államnak eleget kell tennie alapjogvédelmi kötelezettségének. Azonban szerinte ésszerűtlen minden ilyen természetű jogon alapuló igény, hiszen ez alapján bármilyen internetes oldal a világ minden államának jogi környezetének meg kellene, hogy feleljen, hiszen az Internet mindenki számára kínál szolgáltatást. Svantessson ezen megállapítása nem helytálló.

Egyrészt, az informatikai megoldások lehetővé teszik azt, hogy földrajzi alapon – és így a nemzeti jogot figyelembe véve – olyan korlátozásokat építsenek be a weboldal elérésének mechanizmusába, hogy bizonyos országok felhasználói egyáltalán ne, vagy csak korlátozottan férjenek hozzá.

[138] RYNGAERT (2015) p. 223.
[139] KUNER (2015) p. 7.
[140] SVANTESSON (2012) p. 88-96.

DOI: 10.14750/ME.2019.022

Másrészt, az uniós joggyakorlat[141] már – egyébként nem túl meggyőző érveléssel – kimondta, hogy az internetre feltöltés nem minősül harmadik országba irányuló adattovábbításnak. Még ha nem is fogadjuk el az Európai Unió Bírósága által hozott ítélet megfelelőségét, Svantesson érvelése sem meggyőző. Poullet további megkülönböztetést tesz, amikor elválasztja az extraterritorriális hatást és az extraterritorriális hatálytól,[142] amely álláspontom szerint jogilag helyes, gyakorlatilag nincs különbség sem az érintetti, sem az adatkezelői oldalon, a jogalkalmazás eljárási jogosultságai, adott esetben az államok viszonosság alapján történő eljárása már nemzetközi közjogi kérdés.

IV.3. Az uniós jogalkotó indokolása

Az Adatvédelmi Irányelv megalkotásakor az uniós jogalkotó a harmadik országba irányuló adattovábbítások szabályozásának szükségességét leginkább abban látta, hogy a személyes adatok határokon átnyúló áramlására szükség van a nemzetközi kereskedelem bővüléséhez.[143]

Kiemelt indok, hogy az egyének garantált védelme nem áll útjában a személyes adatok továbbításának olyan harmadik országokba, amelyek megfelelő szintű védelmet biztosítanak, azonban *egyértelmű a tilalom* a megfelelő védelmi szintet biztosítani nem tudó harmadik országokba irányuló továbbítások vonatkozásában. Ez a személyes adatok védelmének egyik alapvető követelménye. Az Adatvédelmi Irányelv [144] is előre jelezte már, hogy különleges intézkedéseket lehet hozni a valamely harmadik országban tapasztalható védelem hiányának orvoslására olyan esetekben, amikor az adatkezelő megfelelő biztosítékokat nyújt, például megfelelő jogi garanciák, magatartási kódex formájában.

[141] C-101/01. sz. Svédországban, Bodil Lindqvist ellen folytatott büntetőeljárás során előzetes döntéshozatali eljárásban a Bíróság 2003. november 6. napján meghozott ítélete, EBHT 2003., I-12971. p ECLI:EU:C:2003:596
[142] POULLET (2007)
[143] Adatvédelmi Irányelv (56)
[144] Adatvédelmi Irányelv (59) preambulumbekezdés

DOI: 10.14750/ME.2019.022

A GDPR jogalkotói indokolása[145] a fenti szabályozás eredményeit alapállásnak tekintve már azt rögzíti, hogy a technológia egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét. Ma már nem is kérdés, hogy az adattovábbítás a digitális közegben, tulajdonképpen mennyiségi, távolsági, időbeni, technikai vagy technológiai korlátozás nélkül megtörténhet. Ugyanakkor, helyesen, fenntartja a tilalmat a megfelelő védelmi szintet nem biztosító címzetteknek történő adattovábbítások esetére azzal, hogy differenciál az adott harmadik ország, a harmadik ország valamely területe vagy meghatározott ágazata, illetve valamely nemzetközi szervezet, mind fogadó célország, illetve fogadó adatkezelő között.

A differenciálás indokoltságát alátámasztandó egy adatbiztonsági szolgáltatásokat kínáló cég[146] 2016. évi statisztikája szerint[147] az adatvédelmi incidensek aránya gazdasági szektoronként eltérő. Az összes adatlopás és jogellenes felhasználás például 1,9 %-a az egészségügyben, 0,9 %-a a pénzügyi szektorban, és mindössze 30,26%-a történt a szórakoztatóiparban.

A magatartási kódexek fontosságát és az adatkezelői tudatosságot hangsúlyozza a jogalkotói indokolás azzal, hogy jogfejlesztő célzattal kiemeli, hogy az adatkezelő vagy az adatfeldolgozó olyan megoldásokhoz folyamodhat, amelyek az érintettek számára olyan tényleges és érvényesíthető jogokat garantálnak, amelyek igénybevételével az érintettek az adattovábbítást követően is élvezhetik az őket megillető alapvető jogokat és garanciákat akkor is, ha az Európai Bizottság az adott harmadik ország viszonylatában nem

[145] GDPR (6) preambulumbekezdés
[146] A cég szlogenje szerint már nem az a kérdés, hogy egy hálózatot feltörtek-e már, hanem az, hogy mikor tették és mikor fogják legközelebb.
[147] Gemalto: DATA BREACH STATISTICS, 2016, http://breachlevelindex.com/ [2017. december 10.]

DOI: 10.14750/ME.2019.022

hozott határozatot a harmadik ország adatvédelmi szintjéről.[148] Hangsúlyosan emeli ki e körből a BCR-t mint megfelelő garanciát nyújtó jogi eszközt az adattovábbítások megfelelő garanciájául.[149]

IV.4. A tételes jogi összehasonlítás

A személyes adatok harmadik országba irányuló továbbításának uniós szabályozása részletszabályokkal és számos új lehetőségbiztosításával gazdagodott: a piaci igényekhez igazodva bővítette szabályozási spektrumát miközben a főszabály azonos maradt.

Az Adatvédelmi Irányelv három jól azonosítható részben – az adatvédelmi felügyelő hatóság részére történő előzetes bejelentési kötelezettséget a 19. cikk (1) bekezdés e) pont szerint, a főszabályt a 25. cikk szerint és a kivételes jogcímeket a 26. cikkben szabályozta a harmadik országba irányuló adattovábbítás kérdését.

A *GDPR strukturáltabb* szabályozási rendet követ. A 30. cikk előírja az adatkezelő részére az adatkezelési tevékenységekről szóló *nyilvántartás vezetését,* amelynek kötelező tartalmi eleme többek között a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása. A 44. cikkben rögzítésre kerül az adattovábbításra vonatkozó *általános elv,* a 45. cikk rendezi a *főszabályként* elterjedt megfelelőségi határozat kérdését, ezt követően a 46. cikk listázza a *megfelelő garanciák* alapján történő adattovábbítások egyes eseteit, a 47. cikk részletezi a *BCR általános tartalmi minimum előírásait* és az eljárási szabályokat mint a megfelelő garanciák

[148] GDPR (114)
[149] GDPR (107)

DOI: 10.14750/ME.2019.022

egyik típusát, a 48. cikk az uniós jog által nem engedélyezett továbbítás és közlés főszabályát határozza meg, majd a 49. cikk szabályozza a *különös helyzetekben biztosított eltérési lehetőségeket*, végül az Európai Bizottság és a felügyeleti hatóságok nemzetközi *együttműködésének* érdekében deklarál az 50. cikk előírásokat.

Szembetűnő a szabályozás volumenének növekedése és differenciáltsága, amelynek legfőbb indoka a gyakorlatban feltárt hiányosságok.

A köztudatban Lindqvist - ügyként ismertté vált C-101/1. számú eset,[150] amelyben az ítélet deklarálja, hogy a harmadik országba történő adattovábbítás nincs definiálva, és a személyes adatok internetes oldalra történő feltöltése esetén nem lehet megállapítani a harmadik országba történő adattovábbítást, nem tudta megválaszolni a szabályozás hiányosságából fakadó, a mindennapossá váló tömeges adattovábbítások következtében kialakult jogértelmezési kérdéseket.

Az Adatvédelmi Irányelvben előírt előzetes értesítési kötelezettséget a GDPR megszünteti, amelynek indoka, hogy az igazgatási és pénzügyi terhekkel járt, azonban nem minden esetben járult hozzá a személyes adatok védelmének javításához.[151] A felügyeleti hatóság előzetes értesítésének kötelezettségét a jövőben azon adatkezelések vonatkozásában kell megtenni, amelyek magas kockázattal járnak az érintett szempontjából, új technológiákat alkalmaznak, illetve amelyek új fajtájúak, és amelyek esetében az adatkezelő még nem végezte el az adatvédelmi hatásvizsgálatot, vagy amelyek esetében az adatvédelmi hatásvizsgálat az első adatkezelés óta eltelt időre tekintettel vált szükségessé.[152]

[150] C-101/01. sz. Svédországban, Bodil Lindqvist ellen folytatott büntetőeljárás során előzetes döntéshozatali eljárásban a Bíróság 2003. november 6. napján meghozott ítélete, EBHT 2003., I- 12971. p ECLI:EU:C:2003:596
[151] GDPR (89) preambulumbekezdés
[152] GDPR (89) preambulumbekezdés utolsó fordulata

DOI: 10.14750/ME.2019.022

Az értesítési kötelezettség a tagállami jogalkotás szintjére helyeződött azokban az esetben, amikor megfelelőségi határozat hiányában az uniós jog vagy a tagállami jog fontos közérdekből kifejezetten korlátozza bizonyos kategóriába tartozó adatoknak valamely harmadik országba vagy nemzetközi szervezet részére történő továbbítását. A tagállamok az ilyen rendelkezésekről a Bizottságot értesítik.[153]

A szabályozás újdonsága, hogy a *vállalkozáscsoport adatvédelmi jogi fogalmát* rögzíti a GDPR 4. cikk 19. pontja. A fogalom megalkotásának szükségessége elvitathatatlannak látszott, mivel az igény a cégek oldaláról már a jogalkotási eljárás során megmutatkozott.[154]

Ugyancsak tételes jogi előzmény nélkül, de számos soft law jellegű iránymutatás[155] és a piaci igényekre alapozottan kapott kiemelt szerepet a *BCR jogintézménye* a GDPR 47. cikkeként, amely az Adatvédelmi Irányelvben csak implicite jelent meg az adatkezelő által teremtett megfelelő garanciák fogalmi ernyője alá besorolva.

A GDPR *négy egységből álló szabályozási koncepciót* alkalmaz. *Főszabályként* rendezi a megfelelőségi határozat (GDPR 44. cikk első egység) valamint a megfelelő garanciák (GDPR 46. cikk (2) bekezdés szerinti második egység) eseteit, majd a *különleges helyzetekben biztosított eltérések alkalmazhatóságát szabályozza* (GDPR 49. cikk szerinti harmadik egység). Ezek hiányában a harmadik országba történő adattovábbítás csak akkor történhet meg (GDPR 49. cikk (1) bekezdés utolsó három mondata szerinti

[153] GDPR (112) preambulumbekezdés és GDPR 49. cikk (5) bekezdés
[154] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Chapter V, Brussels, 28 April 2014, 8087/1/14 REV 1, 2012/0011 (COD)
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208087%202014%20REV%201
[2017. november 02.]
[155] A 29. cikk szerinti Adatvédelmi Munkacsoport vonatkozó magyarázó dokumentumai: WP 74, WP 108, WP 153, WP 154, WP 155, WP 176, WP 195, WP 204 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [2018. június 23.]

DOI: 10.14750/ME.2019.022

negyedik egység), ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik, az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, illetve az adatkezelő az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében.

A negyedik koncepció szerint az adatkezelőnek tájékoztatnia kell a felügyeleti hatóságot az adattovábbításról és adatkezelő az általános tájékoztatási kötelezettségen túl az érintettet az adattovábbításról, valamint az adatkezelő kényszerítő erejű jogos érdekéről is tájékoztatnia kell.

IV.4.1. Főszabály

Az Adatvédelmi Irányelv 25. cikk (1) bekezdése főszabályként rögzítette, hogy személyes adatok csak akkor továbbíthatók harmadik országba, ha az adott harmadik ország megfelelő védelmi szintet tud biztosítani.

A GDPR megőrzi a szabályozás elvi és tartalmi alapját úgy, hogy a továbbítás csak a rendelet teljes betartása mellett hajtható végre, azaz valamennyi rendelkezést alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára a rendeletben garantált védelem szintje ne sérüljön, deklarálja a 44. cikk. A megfelelő védelmi szint fogalma a 45. cikkben a megfelelőségi határozatok vonatkozásában jelenik meg először a GDPR szövegében, amely szerint harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha az Európai Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít.

DOI: 10.14750/ME.2019.022

Rendszeres, legalább *négyévente elvégzendő felülvizsgálatot* ír elő a GDPR 45. cikk (3) bekezdés, amely megelőzheti a Schrems-ügy következtében kialakult helyzeteket.

Az Adatvédelmi Irányelv felülvizsgálati kötelezettséget nem írt elő, így következhetett be az a helyzet is, amely a Safe Harbor mechanizmus érvénytelenítéséhez vezetett, ti. az Európai Bizottság ugyan nem azt állapította meg, hogy USA mint harmadik ország megfelelő védelmi szintet biztosít, hanem egy, az USA-beli cégeknek szóló önkéntes vállaláson alapuló rendszert hozott létre az adattovábbítások jogszerűségének biztosítására, azonban sem a rendszert, sem az USA szövetségi és tagállami jogi környezetét, sem pedig a cégek tevékenységét nem vizsgálták érdemben.

Mind az Adatvédelmi Irányelv,[156] mind a GDPR az Európai Bizottság jogkörébe utalja a megfelelőségi határozat meghozatalát.[157] További novumot azonosíthatunk *a harmadik ország valamely területe illetve ágazata* vonatkozásában. Ez a GDPR- beli distinkció éppen arra az általános alapállásra reagál, amely a szektorális ön- illetve társszabályozás koncepcióját támogatja, azaz ha a harmadik ország egésze nem is, annak egy területe, például önálló jogalkotással bíró területi egysége, vagy gazdasági vagy nonprofit ágazata biztosíthat megfelelő védelmi szintet, például a területi jogalkotással vagy magatartási kódexek alkalmazásával. Az Európai Bizottság közzéteszi az olyan harmadik országok, harmadik országon belüli területek és meghatározott ágazatok, valamint nemzetközi szervezetek jegyzékét, amelyek esetében úgy ítélte meg, hogy biztosítják, vagy többé nem biztosítják a megfelelő védelmi szintet.[158]

[156] Adatvédelmi Irányelv 31. cikk (2) bekezdés
[157] A megfelelő védelmi szintet biztosító országok listáját lásd: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (2017.12.08.)
[158] GDPR 45. cikk (8) bekezdés

DOI: 10.14750/ME.2019.022

A GDPR újszerű szabályozási megoldása, hogy külön nevesíti a harmadik országba vagy nemzetközi szervezet részére történő továbbításokat, miközben azonos szabályokat rendel alkalmazni rájuk. A Nemzetközi Vöröskereszt például külön kérte, hogy mint nemzetközi humanitárius szervezetet nevezze meg a GPDR, amely vonatkozásában a harmadik országba irányuló adattovábbítások az érintett hozzájárulása nélkül, a létfontosságú érdekre hivatkozással végezhetők.[159]

A megfelelő védelmi szint kérdése fogalmi szinten sem volt tisztázott, hiszen „tagállami hatáskör" a harmadik országba történő adattovábbítás feltételéről történő rendelkezés és a megfelelő védelmi szint biztosításáról való intézkedések végrehajtása az Adatvédelmi Irányelv 25. cikke értelmében. Az Adatvédelmi Irányelv 25. cikk (2) bekezdése iránymutatásul szolgált a megítélési szempontok vonatozásában: a védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni. Így különös figyelmet kell fordítani az adatok jellegére, a tervezett adatfeldolgozási művelet vagy műveletek céljára és időtartamára, a kiindulási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre. Ugyanakkor a tényleges felülvizsgálat - mivel a gyakorlatban ennek teljes hiánya volt tapasztalható - nem érte el a kívánt hatást, amely tényt a fentebb idézett Schrems-ügyben is egyértelműen rögzített a bíróság. *A GPDR ugyanakkor a jogalkalmazás precedensértékű megállapításaira jogfejlesztő értelmezéssel válaszolt:* figyelembe kell venni azt, hogy az adott harmadik országban mennyire tartják tiszteletben a jogállamiságot, az igazságszolgáltatáshoz való jogot, valamint a nemzetközi emberi jogi normákat és előírásokat, valamint vizsgálat alá kell vonni az adott ország általános és ágazati jogszabályait, ideértve a közbiztonságra, a védelemre és a

[159] http://data.consilium.europa.eu/doc/document/ST-8837-2015-INIT/en/pdf [2017. november 2.]

DOI: 10.14750/ME.2019.022

nemzetbiztonságra vonatkozó jogszabályait, valamint közrendjét és büntetőjogát is. Rögzíti, hogy a megfelelőségi határozat elfogadásakor olyan egyértelmű és objektív szempontokat szükséges figyelembe venni, mint például a konkrét adatkezelési tevékenységek, továbbá a harmadik országban alkalmazandó jogi normák és jogszabályok hatálya. Kiemeli a személyes adatok gépi feldolgozása során a természetes személyek védelméről szóló, 1981. január 28-i Európa tanácsi egyezményhez való csatlakozás tényének fontosságát a vizsgálat szempontjából.

A GDPR a Schrems-ügyben hozott ítélettel összhangban rögzíti a főbb szempontokat: a harmadik országnak olyan kötelezettséget kell vállalnia, amelyek megfelelő – az Unión belül biztosítottal lényegében megegyező – védelmi szintet biztosít, különösen gondoskodnia kell a tényleges, független adatvédelmi felügyeletről és tagállami adatvédelmi hatóságokkal való együttműködési mechanizmusairól, továbbá biztosítania kell, hogy az érintettek tényleges és érvényesíthető jogokkal, valamint hatékony közigazgatási és bírósági jogorvoslati lehetőségekkel rendelkezzenek.

A megfelelő védelmi szint tehát olyan jogokkal és garanciákkal ellátott jogi környezetet feltételez az adatalany szempontjából, amely hatálya alatt személyes adatainak kezelése és feldolgozása során az érintett uniós polgár státusa szerinti védelem illeti meg.

A 29. cikk szerinti Adatvédelmi Munkacsoport[160] már 1998. évben foglalkozott a megfelelő védelmi szint fogalmával és értelmezésével, amelyet 2017. évben, a GDPR elfogadásra tekintettel részben felülvizsgált. Egyértelműen rögzíti a jelentés, hogy a megfelelő védelmi szint nem az uniós jogszabály tükörfordításával biztosítható csupán.

[160] 29. cikk szerinti adatvédelmi munkacsoport: Megfelelőségi jelentés, WP 254.

DOI: 10.14750/ME.2019.022

Akkor megfelelő a személyes adatok védelmének szintje a harmadik országban, ha egy olyan, az érintettek jogaiból és az adatkezelők és adatfeldolgozók kötelezettségeiből valamint a független felügyelő hatóságra vonatkozó szabályanyagból álló jogi környezet van hatályban, amely a gyakorlatban ténylegesen alkalmazható rendelkezéseket tartalmaz és amelyek betartása kikényszerítő.

Az Európai Bizottságnak két alapvető jellemzőt kell vizsgálnia e körben: az alkalmazandó jog szabályait és azok alkalmazására vonatkozó eszközöket.

Az adatvédelmet érintő vagy az arra csak általánosságban vonatkozó szabályok nem tekinthetők kielégítőnek. Az Európai Bizottság határozatának meghozatalában kulcsszerepet fog játszani a GDPR szerinti Európai Adatvédelmi Testület, amely véleményével, adott esetben a harmadik országbeli jog módosítására tett javaslatával fogja segíteni a vizsgálatot, ugyancsak a négyéves felülvizsgálatokat.

A megfelelő védelmi szint megállapíthatóságához a javaslat szerint szükséges:
- alapvető adatvédelmi fogalmaknak kell hatályban lenniük;
- előírás legyen, hogy az adatkezelésnek jogszerűnek, igazságosnak és jogszerű célhoz kötöttnek kell lennie;
- a célhoz kötöttség, az adatminőség elve és az arányosság elve előírás legyen;
- az adatmegőrzés tilalma és az adatkezelés időtartamának szabályozása legyen rögzítve;
- a nyíltság elve, az érintett tájékoztatásának kötelezettsége előírás legyen;
- a hozzáférés, a helyesbítés, a töröltetés és a tiltakozás joga biztosítva legyen;
- korlátozott legyen az adattovábbítás.

DOI: 10.14750/ME.2019.022

Vizsgálati szempont a szektoriális adatkezelések szabályozása valamint az eljárásjogi és a kikényszerítésre vonatkozó szabályanyag:
- a hatáskörrel rendelkező felügyeleti hatóság, amely teljes függetlenséggel és pártatlansággal végzi feladatait;
- a megfelelés magas szintjét biztosítsa az adatvédelmi rendszer, elszámoltatható és tudatos adatkezelői eljárások révén;
- az érintetteket segítő és támogató adatvédelmi rendszer működjön.

Kulcselem a nemzeti jog és a nemzeti hatóságok jogköreinek befolyása, különösen a biztonságpolitikai vonatkozások, amely körében négy szempontot emel ki a javaslat:
- világos, pontos és megismerhető jogi alapon történhet megfigyelés;
- a szükségesség – arányosság teszt elvégzése a jogos cél igazolására;
- a független felülvizsgálat lehetősége legyen biztosítva;
- az érintettek számára rendelkezésre álljon hatékony jogorvoslati lehetőség.

IV.4.2. Kivételes jogcímek

Az Adatvédelmi Irányelv 26. cikke és a GDPR 49. cikke is számos kivételes jogcímet biztosít arra az esetre, ha a megfelelő védelmi szint nem biztosított, mégis megtörténhet az adattovábbítás a harmadik országba.

Az Adatvédelmi Irányelv és a GDPR szabályai szerint *azonos kivételes jogcímek* az alábbiak:

- az érintett hozzájárulása; míg az irányelv az „egyértelmű” jelzőt használja, amelynek tartalma, hogy a hozzájárulás kérésére, illetve adására irányuló eljárás kétséget kizáróan igazolja az egyén hozzájárulási szándékát,[161] addig a

[161] A 29. cikk alapján létrehozott adatvédelmi munkacsoport: 15/2011. számú vélemény a hozzájárulás fogalommeghatározásáról, WP 187, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_hu.pdf [2018. január 18.]

DOI: 10.14750/ME.2019.022

GDPR számos további követelményt ír elő: a hozzájárulás „kifejezett” és előzetes tájékoztatás történt az adattovábbításból eredő esetleges kockázatokról. A kifejezettség esszenciája, hogy az „tartalmazza az adatfeldolgozás pontos célját” valamint „egyértelműen és pontosan utalnia kell az adatfeldolgozás hatókörére és következményeire.”[162] A fokozott tájékoztatási kötelezettség teljesítése vonatkozásában szükséges utalni az elszámoltathatóság alapelvére, azaz az adatkezelőnek igazolnia kell tudni, hogy a tájékoztatás megtörtént.

- az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;

- az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;

- az adattovábbítás fontos közérdekből szükséges;

- az adattovábbítás jogi igények – az irányelvben követelések – előterjesztése, érvényesítése és védelme miatt szükséges;

- az érintett létfontosságú érdekeinek védelme miatt szükséges, itt a GPDR más személy esetén is lehetővé teszi azzal a konjunktív feltétellel, hogy az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;

- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló

[162] i.m.

DOI: 10.14750/ME.2019.022

bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

Az Adatvédelmi Irányelv 26. cikk (1) bekezdés d) pont utolsó fordulata egyetlen *további lehetőséget* biztosít még: ha jogszabály írja elő az adattovábbítást.

Megállapítható, hogy a kivételes jogcímek nem változtak.

Az Adatvédelmi Irányelv 26. cikk (2) bekezdése szerint a tagállamok engedélyezhetik a személyes adatok olyan harmadik országba irányuló továbbítását, amely nem biztosít megfelelő szintű védelmet, amennyiben az adatkezelő megfelelő garanciákat teremt. Ezt a szabályt az Adatvédelmi Irányelv az Európai Bizottság által elfogadott általános szerződési feltételek[163] körében azonosítja és magatartási és eljárási szabályzatok megalkotásának ösztönzése körében zárja le, míg a GDPR 46. cikk (2) bekezdése explicite és taxatív módon állapítja meg a hat különböző garancia típust, amelyek lehetnek közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszközök, a BCR, a Bizottság által elfogadott általános adatvédelmi kikötések, a felügyeleti hatóság által elfogadott általános adatvédelmi kikötések vagy a felügyeleti hatóság által engedélyezett általános szerződési feltételek alkalmazása, tanúsítási mechanizmusok illetve jóváhagyott magatartási kódexek az adatkezelő kötelező erejű és kikényszeríthető kötelezettségvállalásával.

A jogalkotói indokolás szerint a garanciák különösen a személyes adatok kezelésre vonatkozó általános elveknek, valamint a beépített és alapértelmezett adatvédelem elveinek való megfelelésre vonatkoznak, noha

[163] 2001/497/EK határozat (HL L 181., 2001.7.4., 19—31. o.) és 2004/915/EK határozat (HL L 385., 2004.12.29., 74—84. o.)

DOI: 10.14750/ME.2019.022

számos olyan objektív és praktikus részletről is rendelkezniük kell az adatkezelőknek, amelyek a tényleges jogérvényesítés, például a tájékoztatáshoz való jog gyakorlását vagy a panaszkezelési mechanizmusok működését mutatja be és biztosítja.

Az Adatvédelmi Irányelv 25. cikk (3) bekezdés értelmében a tagállamok és az Európai Bizottság értesítik egymást azokról az esetekről, amelyekben úgy vélik, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet. Ezen túl a tagállamoknak meg kell tenniük a megfelelő intézkedéseket a szóban forgó harmadik országba irányuló továbbításának megakadályozására, amennyiben a Bizottság megállapítja, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet. Hasonló, de következetesebb felülvizsgálati mechanizmust vezet be a GDPR 45. cikk (5) bekezdés utolsó fordulata akként, hogy a Bizottságnak azonnal alkalmazandó végrehajtási jogi aktusokat kell elfogadnia azokban a kellően indokolt, rendkívül sürgős esetekben, ha a rendelkezésre álló bizonyítékokból az derül ki, hogy a célország már nem biztosít megfelelő védelmi szintet. Ez egyértelműen a Schrems-ügy hozadéka az USA védelmi szintjének tényleges felülvizsgálata – illetve annak hiánya – vonatkozásában.

A GDPR 49. cikke rendelkezik egy különös kivételi szabályról, amely szerint a megfelelő védelmi szint hiányában, ha az eltérések egyike sem alkalmazható csak akkor történhet adattovábbítás, ha az nem ismétlődő, csak korlátozott számú érintettre vonatkozik, az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és az adatkezelő az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében. A kivétel igen részletes vizsgálatot és igazolási kötelezettséget ró az adatkezelőre, így csak ritka esetekben szolgál majd jogalapként.

DOI: 10.14750/ME.2019.022

A 29. cikk szerinti Adatvédelmi Munkacsoport már közzétette iránymutatását a 49. cikk szerinti kivételes jogalapok megítéléséről. Azt leszögezi, hogy ezen kivételek alkalmazása során is meg kell felelni a GDPR többi rendelkezésének, különösen az 5. cikk szerinti alapelveknek és a 6. cikkben foglalt jogalapoknak. Az adattovábbítások megfelelőségének biztosítása körében kétlépcsős vizsgálatot ír elő: első lépésben meg kell vizsgálni, hogy az adatkezelés jogalapja megfelel-e a GDRP többi vonatkozó rendelkezésének, a második lépésben pedig biztosítani kell a GDPR V. fejezete szerinti szabályokkal való összhangot. Kiemeli továbbá, hogy a kivételeket megszorítóan kell értelmezni és csak különleges esetekben lehet alkalmazni, ahogy arra a cikk címe is utal „Különös helyzetekben biztosított eltérések". Tekintettel arra, hogy a kivételek esetén a megfelelő védelmi szint nincs biztosítva és az adattovábbítások semmilyen előzetes hatósági jóváhagyására sincs szükség, ezek az adattovábbítások jelentősen növelik az érintettek jogaira és szabadságaira vonatkozó kockázatokat.

A GDPR 49. cikk (1) bekezdésében foglalt „nem ismétlődő" kifejezés körében rögzíti, hogy történhet több adattovábbítás, de azok nem lehetnek szokásosak, csak véletlen, előre nem ismert körülmények között előre nem meghatározható időintervallumon belül.

Kiemelendő, hogy a 111. preambulumbekezdés megkülönbözteti az egyes kivételes jogalapokat egymástól. A 49. cikk (1) bekezdés b) és c) (szerződéses jogalapok) valamint az e) (jogi igényhez kötött jogalap) pontján alapuló adattovábbítás csak alkalomszerűen történhet, míg az a) (az érintett kifejezett hozzájárulása), a d) (fontos közérdek), f) (létfontosságú érdekeinek védelme) és a g) (nyilvántartásból származó adatok) pont esetére ezt a követelményt nem írja elő. Ugyanígy, a szükségesség teszt lefolytatása is csak a b), c), d), e) és f) pont esetén szükséges.

DOI: 10.14750/ME.2019.022

Az érintett kifejezet hozzájárulása körében a hozzájárulás általános követelményein[164] (önkéntes, konkrét, megfelelő tájékoztatáson alapuló, egyértelmű kinyilvánítás, félreérthetetlenül kifejező cselekedet) túl további kritériumoknak kell eleget tenni a 49. cikk (1) bekezdés a) pont szerinti adattovábbítások esetére. Az egyik ilyen többletkövetelmény a „kifejezett" hozzájárulás. Megjegyzem, az Infotv. is ezzel a többletkövetelménnyel operál. Szükséges, hogy a hozzájárulás az adott adattovábbítási műveletre vonatkozzon, így gyakran felmerül az az eset, hogy az adatok gyűjtésekor ilyen hozzájárulást érvényesen nem lehet megszerezni, hiszen ekkor az alapul szolgáló körülmények sem láthatók még előre. Így ez a típusú hozzájárulás szükségszerűen külön, az adattovábbítás megtörténte előtt szerezhető csak be, de fontos, hogy még a művelet elvégzését megelőzően megtörténjen az érintett beleegyezése. A tájékozott beleegyezés követelménye akként változik, hogy az adattovábbítás valamennyi részletén túl külön is tájékoztatást kell adni a megnövekedett kockázatokról és arról, hogy azok fennállnak, mert az adattovábbítás címzettje - akár a célország, akár az adott adatkezelő - nem biztosítja a megfelelő védelmi szintet. Az Adatvédelmi Munkacsoport hangsúlyozza, hogy ez a jogalap – a hozzájárulás visszavonásának lehetőségére is figyelemmel – nem biztosít hosszú távon megfelelő megoldást.

[164] 29. cikk szerinti munkacsoport: Guidelines on Consent under Regulation 2016/679 WP 259

DOI: 10.14750/ME.2019.022

IV.4.3. A magyar szabályozás

A GDPR közvetlen alkalmazását megelőzően az Infotv. egyedi megoldást alkalmazott[165] a „külföldre irányuló adattovábbítások" szabályozására a 8. § rendelkezéseiben. Az Infotv. értelmében „külföld" a nem EGT tagállamok körét fedte.[166] A 8. § (4) bekezdése szerint az adattovábbítást ezen országokba úgy kellett tekinteni, mintha Magyarország területén belüli adattovábbításra került volna sor, tehát nem kellett vizsgálni a megfelelő védelmi szint követelményét.

Az Infotv. 8. § (1)-(2) bekezdése alapján harmadik országban letelepedett adatkezelőnek illetve adatfeldolgozónak történő adattovábbításra három lehetőség állt fenn:

a) főszabályként amennyiben az érintett az adattovábbításhoz kifejezetten hozzájárult. Az érintett hozzájárulása tekintetében az Infotv. 3. § 7. pontja előírta, hogy az önkéntesség, az akarat határozott kinyilvánítása, a megfelelő tájékoztatás és a félreérthetetlen informált beleegyezés kritériumának eleget kell tennie az érintett akaratnyilatkozatának. A harmadik országba történő adattovábbítás esetén külön ismertetni volt szükséges, ha a megfelelő védelmi szintet a célország nem garantálja. E körben szükséges volt, hogy az érintett egyértelműen kinyilvánítsa, hogy megértette a harmadik országba történő adattovábbítással járó fokozott kockázatot és ennek tudatában egyezik be az adattovábbításba.[167]

b) az érintett kifejezett hozzájárulásának hiányában, ha az alábbi két konjunktív feltétel esetén:
ba) az Infotv. hatálya alá tartozó adatkezelő az Infotv. által elismert jogalappal rendelkezett az adatkezeléshez, és

[165] Eltérő hivatkozás hiányában az Infotv. idézett szakaszai alatt jelen alfejezetben a 2018. július 25. napi időállapot szerinti jogszabályszöveget értem.
[166] EGT tagállamok: valamennyi EU tagállam, Izland, Liechtenstein és Norvégia.
[167] NAIH állásfoglalás http://naih.hu/files/2223-2-2013-v.pdf [2018. február01.]

DOI: 10.14750/ME.2019.022

bb) a harmadik országban a személyes adatok megfelelő szintű védelme biztosított volt, amelyet az Európai Unió kötelező jogi aktusa megállapított vagy nemzetközi szerződés rendelkezik a garanciákról,

c) az Infotv. 6. § (2) bekezdésén alapuló kivételes adattovábbítás esetén nem kellett vizsgálni azt, hogy a harmadik ország a személyes adatok megfelelő szintű védelmet biztosítja-e vagy sem. Az adattovábbítás fogalmának értelmezése körében rejlő visszásságot tárt fel Jóri és Soós,[168] mikor az adatfeldolgozó részére történő adattovábbítást nem minősítették az Infotv. fogalma szerint adattovábbításnak, így az adatfeldolgozási célú adattovábbításhoz az érintett hozzájárulása nem követelhető meg, összhangban a NAIH álláspontjával.[169] Megjegyzem, sem az Adatvédelmi Irányelv, sem a GDPR nem rendezi az adatfeldolgozás fogalmát, a GDPR az adatfeldolgozó fogalmában is az „adatot kezel" fordulatot használja.

A megfelelő védelmi szint három módon volt biztosítható:

a) az Európai Unió kötelező jogi aktusa azt megállapította;

b) a harmadik ország és Magyarország között az érintettek jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés volt hatályban;

c) az adatkezelés, illetve az adatfeldolgozás BCR szabályainak megfelelően történt. Ez utóbbi jogalap a törvénymódosítás indokolása és a közzétett hatásvizsgálat szerint a piaci igényekre reagálva 2015. október 1. napján lépett hatályba.

[168] JÓRI –SOÓS (2016) p. 183.
[169] NAIH állásfoglalás, Ügyszám: NAIH-2223-2/2013/V, https://www.naih.hu/files/2223-2-2013-v.pdf [2018. január 21.]

DOI: 10.14750/ME.2019.022

Megítélésem szerint azonban *volt a BCR-hez hasonló, de nem ugyanolyan lehetőség* a megfelelő védelmi szint biztosítására ezt megelőzően is. Állításom igazolását megelőzően azonban meg kell jegyezni, hogy mivel hazánkban a harmadik országba történő adattovábbítás nem engedélyköteles illetve előzetes jóváhagyáshoz, bejelentéshez sem kötött és nem is volt az, így BCR vagy BCR-szerű szabályozás létrehozása hazai vállalkozáscsoporti tag számára valós előnyt nem jelentett volna. A 1992. évi LXIII. törvény 9. § (2) bekezdés c) pontja biztosította, hogy amennyiben harmadik országbeli adatkezelő illetve adatfeldolgozó az *adatkezelés és az adattovábbítás szabályainak ismertetésével igazolta*, hogy a személyes adatok megfelelő védelmi szintje, az érintettek jogai és jogérvényesítési lehetőségei garantáltak, különösen akkor, ha tevékenységét az Európai Unió Bizottsága külön törvényben meghatározott jogi aktusának megfelelően végezte, akkor a személyes adatok védelmi szintje *biztosítottnak volt tekinthető*. Mindez annak az előfeltétele volt, hogy a 9. § (1) bekezdés b) pontja szerint személyes adat harmadik országban adatkezelést folytató adatkezelő illetve adatfeldolgozó részére továbbítható lehessen. A szabályozás tartalma tehát arra utal, hogy egy BCR-szerű megoldással biztosítható volt a megfelelő védelmi szint.

A részletszabályok kidolgozása, azaz hogy mikor - az adatkezelés megkezdése előtt, alatt, után, csak jogsérelem esetén vagy az érintett kérelmére -, mely hatóság előtt – azaz az érintett nemzeti hatósága vagy a harmadik országban lévő adatkezelő nemzeti hatósága, ha ilyen egyáltalán működik -, hogyan történhetett ilyen igazolás és mikor volt ez kötelező vagy szükséges, elmaradt, így nem is vált elterjedté ez a módszer. Az Adatvédelmi Irányelv 26. cikk (2) bekezdése rögzített hasonló megoldást, a garanciák elsősorban szerződéses klauzulák formájában biztosíthatók, a további szabályozást tagállami hatáskörbe utalja, ami a fentiek szerint hazánkban elmaradt.

DOI: 10.14750/ME.2019.022

IV.5. A magyar szabályozás módosításáról

A külföldi adattovábbítás hazai szabályozása többször módosult, mire kialakult mai rendszere. A GDPR 2018. május 25. napi alkalmazásától azonban a közvetlen hatállyal bíró jogforrásban biztosított valamennyi jogi eszköz és módozat használatára lehetősége nyílik az adatkezelőknek, amelyre a hazai - elsősorban hatósági - jogalkalmazásnak is készen kell állnia. A GDPR-ban biztosított eszközök alkalmazásának lehetőségén túl arra is figyelmet kell fordítani, hogy az Infotv. 8. § (1) bekezdés a) pontja szerinti jogalapot, azaz az érintett kifejezett *hozzájárulását a GDPR 49. cikke különös esetekben biztosítja* arra az esetre, ha sem megfelelőségi határozat, sem pedig a 46. cikk szerinti garanciák nem állnak rendelkezésre. A GDPR fenntartja az információs önrendelkezés szabályozási filozófiai alapjait, noha számos törvényes adatkezelési jogcímet állít fel. Az utóbbiaknál értelemszerűen nincs, vagy csak közvetetten létezik hozzájárulás, például egy szerződés megkötésekor a szerződési szabadság és akarat talaján nyugvó önrendelkezés. Ebben a megközelítésben az önrendelkezés nem kivétel, hanem alapjogcím és (az egyik) alapja a jogcímeknek. Azonban az adatkezelő szempontjából az érintett hozzájárulása noha alapjogcím, egyben a bizonytalanságot is magában hordozza, hiszen a hozzájárulás bármikor visszavonható, és másik jogcím hiányában az adat nem kezelhető tovább.

A BCR jogi elismerésének folyamata egyértelműen pozitív hozzáállást mutat a jogalkotó részéről: míg az Adatvédelmi Irányelvben csak rejtett, implicite megoldás, addig a magyar jogalkotó megelőzve a GDPR közvetlen alkalmazásának időpontját, léptette hatályba a jogintézményt, a GDPR- ban pedig egyértelműen támogatott jogintézmény a megfelelő védelmi szint biztosítására. A BCR tehát a megfelelő védelmi szint biztosításának csupán egyik, legkésőbb törvénybe iktatott módja.

DOI: 10.14750/ME.2019.022

A GDPR „teljes körű végrehajtásához, illetve a bűnügyi Adatvédelmi Irányelv teljes körű átültetéséhez szükséges módosítására és további, e célból szükséges jogalkotási intézkedésekre még nem került sor„ – írta közleményében 2018. május 25. napján a NAIH.[170] A GDPR és a 2016/680/EU irányelv miatt szükséges módosítások vonatkozásában az Infotv. módosításáról szóló törvénymódosítást (a továbbiakban: módosítás) 2018. július 25. napján hirdették ki. Az alapállás, amelyre tekintettel a módosítás vizsgálandó, az, hogy az Infotv. csak akkor alkalmazandó, ha az adatkezelés a 2016/680/EU irányelv hatálya alá tartozik, valamint azon részletszabályok körében, amelyeket a GDRP nem rendez és a tagállamok alkothatnak további részletszabályokat, azaz az Infotv. 2. § (2) és (4) bekezdésében taxatívan felsorolt szakaszok. Minden más esetben közvetlenül a GDPR alkalmazandó. Tekintettel arra, hogy jelen értekezés nemcsak a BCR-t vizsgálja, hanem az adattovábbítások jogi szabályozását is, indokoltnak találom a módosítás vonatkozó szakaszainak elemzését.

A módosítás két új fogalmat vezet be a külföldi adattovábbítások körében, azonban egyiket sem kell alkalmazni a GDPR hatálya alá tartozó jogviszonyok esetében.[171]

Az egyik a nemzetközi szervezet fogalma, amely – az értelmet meg nem változtató – kötőszavak kivételével azonos a GDPR-beli fogalommal.

A másik a *közvetett adattovábbítás* fogalma.

[170] http://naih.hu/files/2018-05-25-GDPR-koezlemeny.pdf [2018. május 25.]
[171] A GDPR 4. cikk 26. pontja is meghatározza a nemetközi szervezet fogalmát, tartalmilag azonosan.

DOI: 10.14750/ME.2019.022

Kiemelendő, hogy a GDPR nem tartalmazza sem az adattovábbítás fogalmát, sem a közvetett adattovábbítás fogalmát. A módosítás szerint a közvetett adattovábbítás:

> *„személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása”*

A fogalom bevezetésével az Inftov. hatálya alá tartozó adatkezelések esetén a közvetett adattovábbítás *elkülönül* a külföldi adattovábbítástól. Míg a külföldi adattovábbítás esetén Magyarországról vagy EGT tagállamból indul az adattovábbítás harmadik országba, addig a közvetett adattovábbítás esetén *a harmadik országból egy másik harmadik országba történik továbbítás*. A bevezetés célja az lehet, hogy a megfelelő védelmi szintet akkor is garantálni szükséges, ha az EGT-beli adatkezelő által harmadik országba továbbított személyes adatokat a célországban működő adatkezelő egy másik harmadik országbeli adatkezelőnek vagy adatfeldolgozónak továbbítja. A fogalom pedig azáltal nyert majd jelentőséget, hogy a felelősség-kiterjesztő rendelkezések útján nem lehet majd kijátszani a szabályokat pusztán azzal, hogy további al-adatfeldolgozót vesz igénybe az adatfeldolgozó. Az EGT-beli első továbbítónak garantálnia kell az adattovábbítási láncolaton végig a megfelelő védelmi szintet.

DOI: 10.14750/ME.2019.022

A fogalom bevezetése alapvetően hasznos és erős garanciális jelleget mutat. Ugyanakkor nem pontos a megfogalmazása, amely a fogalom alkalmazhatóságát vonja kétségbe. A „más harmadik országban" kifejezés használatával nem minősül közvetett adattovábbításnak az, ha a harmadik országban lévő adatkezelő vagy adatfeldolgozó a letelepedése szerinti és nem másik harmadik országban működő adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbít személyes adatot. A „más (harmadik országban vagy) nemzetközi szervezet keretében" fordulat is hasonló következményekkel járna: nem tekinthető közvetett adattovábbításnak az, ha ugyanazon nemzetközi szervezet egyes szervezetei egy adott harmadik országban egymás között továbbítanak személyes adatot, csak az, ha másik nemzetközi szervezet az adattovábbítás címzettje. A jogalkotó célja bizonyára nem ez volt.

Javaslatom, hogy a fogalomból *el kellene hagyni az „adatkezelést folytató"* kifejezést, mivel az adatkezelő - és gyakorlatilag az adatfeldolgozó is - egyértelműen adatkezelést folytat, így nincs jelentősége. A *„más harmadik országban" kifejezést pedig ki kellene egészíteni* azzal, hogy „vagy ugyanazon harmadik országban, vagy ugyanazon nemzetközi szervezet ugyanazon vagy más harmadik országban működő szervezete részére" fordulattal. Így a fogalom magában foglalná azon adattovábbítási műveleteket is, amelyek egyazon harmadik országban vagy ugyanazon nemzetközi szervezet keretein belül történnek.

A módosítás az Infotv. 8. § *teljes szerkezetét és volumenét megváltoztatta*, azt azonban hangsúlyozni kell, hogy bizonyos szabályait a 2016/680/EU irányelv implementálása eredményeként kellett bevezetni, az új 13. § (2) bekezdését pedig GDPR vonatkozó szabályának kiegészítéseként kell alkalmazni az adattovábbítási folyamatokra.

DOI: 10.14750/ME.2019.022

A módosítás az Infotv. 6. alcímét - „Adattovábbítás külföldre” - is módosította, „Az adattovábbítás feltételei” címre. Álláspontom szerint egyik cím sem pontos. Az Inftov. fejezetcíme a *külföld* szót tartalmazta, amely a szó köznapi használatában minden olyan államot jelentette, amely nem Magyarország. Tekintettel azonban arra, hogy a 8. § (4) bekezdése értelmében az EGT-államba irányuló adattovábbítást úgy kellett tekinteni, mintha Magyarország területén belüli adattovábbításra került volna sor, a szabályok ténylegesen azokra az adattovábbításokra vonatkoznak, amelyek címzettjei nem EGT-államban működnek. Így a külföld e körben indokolatlanul tág fogalom volt. A módosítás szerinti cím, azaz „Az adattovábbítás feltételei” az adattovábbítás Infotv. 3. § 11. pont szerinti fogalmából[172] kiindulva nem érzékelteti megfelelően, hogy a szabályok ténylegesen olyan adattovábbításokra vonatkoznak, amelyek átnyúlnak az országhatárokon. Tekintettel arra, hogy a GDPR bevezeti a személyes adatok határokon átnyúló adatkezelésére vonatkozó fogalmat a tagállamok közötti adattovábbításokra és az V. fejezetben a harmadik országokba illetve nemzetközi szervezetek részére történő továbbításról rendelkezik, az Infotv–nek is *hasonló terminológiát kellene alkalmaznia*. Erősíti ezt a megállapítást azt is, hogy a módosítás a 10. § szakasz vonatkozásában következetesen a nemzetközi adattovábbítás kifejezést használja. E körben megfelelőbbnek találom a GDPR mintájára a „*harmadik országokba vagy nemzetközi szervezetek részére történő adattovábbítás*” cím megfogalmazását.

Főszabályként a 13. § (1) bekezdésében deklarálja, hogy az EGT-államba, valamint az Európai Unió működéséről szóló szerződés V. címének 4. és 5. fejezete szerint létrehozott ügynökségek, hivatalok és szervek részére irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

[172] *adattovábbítás:* az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele

DOI: 10.14750/ME.2019.022

A módosítás itt nem hoz újdonságot, megjegyzem a GDPR hatálya alá tartozó jogviszonyokban a rendelkezés nem alkalmazandó.

A 10. § rendezi az alapesetet, amely értelmében személyes adat akkor továbbítható, ideértve a közvetett adattovábbítást is, ha
a) a nemzetközi adattovábbításhoz az érintett kifejezetten hozzájárult, vagy
b) a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, valamint
ba) annak során az adatkezelésnek az adatkezelés az Infotv. 5. § szakaszában rendezett jogalapjára vonatkozó feltételei teljesülnek, és
bb) a harmadik országban, illetve a nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó tekintetében a továbbított személyes adatok megfelelő szintű védelme biztosított, vagy
c) a nemzetközi adattovábbítás a 11. §-ban meghatározott kivételes esetekben szükséges.

E körben érdekes különbség, hogy míg a GDRP az érintett kifejezett hozzájárulását a 49. cikkben a különleges helyzetekre vonatkozó eltérések közötti jogalapok körében rögzíti, addig az Inftov. még mindig főszabályként rendeli alkalmazni, noha a GDPR is fenntartja az érintett önrendelkezésének elsőbbségét. Érdekes megfogalmazásbeli eltérés, hogy az adatkezelés céljának eléréséhez köti az adattovábbítás jogszerűségét. Azért nevezem ezt megfogalmazásbelinek, mert a célhoz kötöttség elvének megtartása az adatkezelés jogalapját is befolyásolja, így az Infotv. jelenlegi szabályától tulajdonképpen nincs jelentésbeli eltérés.

A GDPR rendelkezéseivel összhangban megjelenik a nemzetközi szervezet is, mint az adattovábbítás címzettje.

DOI: 10.14750/ME.2019.022

A (4) bekezdés egy *vélelmet* állít fel, amely értelmében a megfelelő szintű védelmet – az ellenkező bizonyításáig – *biztosítottnak kell tekinteni,* ha:
a) az Európai Unió kötelező jogi aktusa, azaz a megfelelőségi határozat azt megállapítja,
b) ennek hiányában az érintetteknek a 14. §-ban, 22. §-ban és 23. §-ban foglalt jogai érvényesítésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés alkalmazandó Magyarország és azon harmadik ország, illetve nemzetközi szervezet között, amelynek joghatósága kiterjed a nemzetközi adattovábbítás címzettjére, vagy a fentiek hiányában
c) nemzetközi adattovábbítást megelőzően az adatkezelő a személyes adatok továbbításának valamennyi körülményét megvizsgálta és megállapította, hogy a személyes adatok megfelelő szintű védelme tekintetében megfelelő garanciák állnak fenn.

Ez a rendelkezés a GDPR 49. cikk (1) bekezdés szerinti kivételes esetek a negyedik koncepciója szerinti szabállyal mutat hasonlóságot, - kvázi a kivétel alól al-kivétel -, azzal a különbséggel, hogy a módosítás elhagyja a „nem ismétlődő, csak korlátozott számú érintettre vonatkozik, az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai” többlet feltételt. Az érintettek szempontjából nem támogatható megoldás, tekintettel arra, hogy az *ismétlődést kizáró garanciális szabályt elhagyja* és kizárólag az adatkezelő vizsgálatára bízza a megfelelő védelmi szint megítélését.

Az első ilyen nemzetközi adattovábbítást követően haladéktalanul tájékoztatni kell a NAIH-t a nemzetközi adattovábbítás céljáról, a továbbított adatok címzettjéről és köréről, valamint a nemzetközi adattovábbítás rendszerességéről, a GDPR vonatkozó szabályával összhangban.

DOI: 10.14750/ME.2019.022

E körben tehát hatósági *bejelentési kötelezettséget vezetett be a* módosítás. Eddig ilyen kötelezettség nem volt, a GDPR ilyen kötelezettség előírását lehetővé teszi. Ez az adatkezelőkre jelentős adminisztrációs terhet fog róni.

A 11. § rendezi a kivételes jogcímeket azokra az esetekre, ha nem vélelmezhető a megfelelő védelmi szint. E körben négy lehetőséget biztosít az Infotv.:

a) az érintett vagy más létfontosságú érdekeinek védelme érdekében,

b) valamely EGT-állam vagy harmadik ország közbiztonságát közvetlenül és súlyosan fenyegető veszély elhárítása érdekében,

c) egyedi ügyben, eseti jelleggel az adatkezelő által végzett vizsgálatok vagy eljárások hatékony és eredményes lefolytatása érdekében és az nem jár az érintett alapvető jogainak aránytalan korlátozásával, vagy

d) egyedi ügyben, eseti jelleggel az érintett vagy más jogi igényeinek előterjesztése, érvényesítése, illetve védelme érdekében és az nem jár az érintett alapvető jogainak aránytalan korlátozásával.

A módosítás eredményeként a 12. § egy további nyilvántartás vezetési kötelezettséget is előír ezen esetekre. Az adatkezelőnek dokumentálnia kell a nemzetközi adattovábbítás körülményeit, így különösen az (1) bekezdésben meghatározott, a hatósági bejelentés adatait, továbbá a nemzetközi adattovábbítás időpontját, a továbbított személyes adatokat, valamint az adatkezelő által vizsgált és megfelelően azonosított garanciák megnevezését. A dokumentációt 10 évig meg kell őrizni és azt a Hatóság kérésére rendelkezésére bocsátani.

DOI: 10.14750/ME.2019.022

A 13. § utaló szabálya szerint a GDPR 96. cikke szerinti adattovábbítások, amelyek a tagállamok által a 2016. május 24. előtt kötött nemzetközi megállapodások alapján történnek, és amelyek megfelelnek az említett dátum előtt alkalmazandó uniós jognak, módosításukig, felváltásukig vagy visszavonásukig változatlanul hatályban maradnak és az Infotv. szerinti feltételek hiányában megalapozzák a jogszerű adattovábbítást.

A GDPR 46. cikk (2) bekezdés szerinti garanciák közvetlenül alkalmazandók lesznek, ezeket helyesen a módosítást követően az Infotv. nem tartalmazza.

Az adatminőség elvére tekintettel a módosítást követően az Infotv. előírja, hogy az adatok pontosságát, teljességét és naprakészségét az adattovábbítást megelőzően meg kell vizsgálni. Pontatlan, hiányos vagy már nem naprakész adatokat kizárólag abban az esetben továbbítható, ha az adattovábbítás céljának megvalósulásához elengedhetetlenül szükséges, és az adatkezelő az adattovábbítással egyidejűleg tájékoztatja a címzettet az adatok pontosságával, teljességével és naprakészségével összefüggésben rendelkezésére álló információkról. Előírja, hogy a címzettet tájékoztatni szükséges arról, ha utóbb kiderül, hogy az adattovábbítás feltételei nem álltak fenn.

DOI: 10.14750/ME.2019.022

IV.6. Ellenpont: az adatok helyhez kötöttsége

Az angol nyelvű szakirodalomban *data localization* néven ismert jogfogalom lényege, hogy a nemzeti jog előírja, hogy személyes adatokat csak az adatok forrásával azonos országban - fizikailag is ott található adattárolón és adatkezelő illetve adatfeldolgozó személlyel - lehet tárolni, kezelni, feldolgozni. A tilalom módszere lehet teljes vagy szektorális, így például az egészségügyi vagy pénzügyi helyzetre vonatkozó személyes adatokra vonatkozó tiltás. Érzékletes kritika, hogy mennyiben jobb az a védelmi szint, ha egy iskolában a rendszergazda asztala alatti számítógépen tárolják a diákok adatait, mint ha biztonságos módon egy harmadik országban működő adatbankba továbbítják azokat.[173]

A szabályozás *előnye*, hogy az adatok mindvégig a forrásuk szerinti ország joghatósága alatt maradnak, nem alkalmazandó más ország, például a szerver helye szerinti állam joga. Védelmet nyújthat az online szolgáltatók visszaélése és jogellenes támadások ellen,[174] továbbá a nemzeti hatóság az adatok tárolásának felügyeletére hatáskörrel és illetékességgel rendelkezik. *Hátránya*, hogy az internetes kommunikációból és adattovábbítási lehetőségekből eredő előnyöket nem veszi figyelembe. Az ilyen szabályozás egyes szerzők szerint a gazdasági növekedés gátja, az internet „balkanizálódásának”[175] illetve nemzeti fragmentálódásának[176] előfutára. Az adatok helyhez kötöttségét elutasítja a legtöbb gazdasági szereplő is, mert az nemcsak a közösségi médiát használók magatartására van hatással, hanem minden gazdasági szereplőt is érint, amely az internet segítségével végzi gazdasági tevékenységét, intézi pénzügyeit, fizeti a munkabért vagy az adókat.

[173] PFEIFLE (2017)
[174] Technopedia: Data Localization https://www.techopedia.com/definition/32506/data-localization [2017. november 21.]
[175] FRASER (2016)
[176] BAUER-LEE-MAKIYAMA-Erik VAN DER MAREL-Bert VERSCHELDE (2014) P. 11.

DOI: 10.14750/ME.2019.022

Jelenleg nagyságrendileg három tucat olyan jogrendszer van – köztük Kína, Indonézia, Oroszország és Vietnám –, amely előírja az adatexport és az adattárolás határon kívüli tilalmát,[177] amely az információs technológiák – nemcsak a felhő alapú szolgáltatások, hanem a Big Data és az IoT újdonságaiban rejlő lehetőségek – előnyeinek kiaknázására is hátrányos.[178] Kínában[179] például kevésbé a megfigyelés lehetősége, sokkal inkább a személyiség lopások és a jogellenes adattovábbítások növekvő száma, valamint politikai szempontok indukálták a szigorítást, amely értelmében tilos minden olyan külföldi adattovábbítás, amelyre vonatkozóan az adatkezelő nem rendelkezik az érintett kifejezett hozzájárulásával, kormány engedéllyel vagy más kifejezett jogi felhatalmazással. A People's Bank of China kibocsátott egy állásfoglalást arról, hogy tilos a pénzügyi helyzetre vonatkozó személyes adatok országon kívüli tárolása, feldolgozása vagy elemzése. Az állásfoglalás nem kötelező erejű ugyan, de a gyakorlatban minimumelvárásként értelmezik. Hasonló, a pénzügyi helyzetre vonatkozó személyes adatokra vonatkozó szabályozás Dél-Koreában is. Indiában 2014-ben vezették be azt, hogy minden indiai felhasználó kommunikációjára vonatkozó adatokat Indiában kell tárolni. Egyes szerzők ezzel *párhuzamba vonják a GDPR vonatkozó szabályozását is*, mert olyan országokba, amelyekben a megfelelő védelmi szintet nem biztosítják, tilalmazott az adattovábbítás, amely így de facto az adatok helyhez kötöttségét fogja eredményezni.[180] Megjegyzem, az a főszabály az Adatvédelmi Irányelvben is hatályos volt, mégsem eredményezte az adatok helyhez kötöttségét. Felmerül azonban a kérdés, hogy a nemzeti gazdaságoknak jelent-e akkora előnyt, mint amennyi veszteséget eredményez az adatok helyhez kötöttsége.

[177] PFEIFLE 2017. i.m.
[178] CHANDER-Lê (2014)
[179] LIVINGSTON-GREENLEAF (2016)
[180] BAUER - LEE-MAKIYAMA - VAN DER MAREL – VERSCHELDE (2014) p. 11.

DOI: 10.14750/ME.2019.022

Az bizonyos, hogy már megjelent az a trend, hogy az érintett országokban helyi adat központokat hoztak létre – praktikusan szervereket telepítettek – egyes cégek.[181] Ez összességében a fórum shopping jelenségét illetve a székhely vagy tevékenységi hely áthelyezések számának növekedését is eredményezheti. Az Európai Bizottság is elkötelezett minden ilyen jellegű vagy hatású tagállami intézkedés megszüntetése mellett,[182] de az adatok szabad áramlását csak a tagállamok körében biztosítaná hatósági felügyelet mellett. Az Európai Bizottság a szerzői joghoz hasonló szabályozási rendet látna szívesen, amelyben az adat létrehozója (helyesen az adatkezelő, aki az adatgyűjtést végzi) szabadon rendelkezne az általa létrehozott nem-személyes „nyers" adatok, például belépési adatok halmaza felett.

[181] FRASER (2016)
[182] European Commission: Communication on Building a European Data Economy https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy [2017. november 3]

DOI: 10.14750/ME.2019.022

IV.7. Összegező gondolatok

A harmadik országba irányuló adattovábbítás – csakúgy mint a teljes uniós adatvédelmi szabályanyag – átfogó reformra szorult. A GDPR ugyan az Adatvédelmi Irányelv által lefektetett alapállásból indul ki, mégis jellemzi az újszerűség és a piaci igényekre való reakcióra törekvés. Felismerve a szabályozás modernizálásának szükségességét új jogintézményeket vezet be, reagál a globális gazdaság megkívánta elvárásokra, amelyek magukkal vonják a személyes adatok határokon átnyúló korlátozásmentes áramlásának elvárását. Ugyanakkor az érintettek jogainak védelme a digitális viszonyokra tekintettel új kihívások és megnövekedett kockázatokkal szemben is kell, hogy érvényesüljön. Az érintettek tudatossága növelése mellett az adatkezelőket is érdekeltté kell tenni a megfelelésre, nemcsak a szankciók szigorításával. Így a szabályanyagban hangsúlyt kap az önszabályozás és a BCR, amely látszólag az új adatvédelmi rezsim úttörő jelensége lehet.

Mindezek mellett az európai adatvédelmi standard földrajzi kiterjesztése látszik érvényesülni, például a hatály kérdésében vagy a harmadik országban működő adatkezelő illetve adatfeldolgozó tevékenységére vonatkozó elvárások mint az adattovábbítások előfeltételeként történő rögzítésével. Tekintettel pedig arra, hogy a harmadik országbeli vállalkozáscsoporti tag eljárásáért egy Európai Unióban tevékenységi hellyel rendelkező tag vállal felelősséget a jogellenesség esetére, a kiszabható hatósági bírság összegének jelentős megemelésére tekintettel a megfelelés prioritásként kerül előtérbe a cégek mindennapi működése során.

DOI: 10.14750/ME.2019.022

V. FEJEZET
A BCR FOGALMI ELEMZÉSE

A BCR olyan *szabályzat*, amely deklarálja, hogy egy multinacionális vállalkozáscsoport milyen adatvédelmi politikát folytat, továbbá szabályozza az adatkezelés, az adatfeldolgozás és a vállalkozáscsoporton belüli adattovábbítás részleteit, rögzíti az érintettek jogait. Olyan harmadik országokban működő cégek esetén fontos a BCR alkalmazása, amelyek letelepedése szerinti harmadik országokban a személyes adatok védelmi szintje elmarad a GDPR által meghatározott európai szinttől.

A BCR tekinthető a vállalkozáscsoport tagjai és az érintett közötti magánjogi szerződésnek, kvázi *általános szerződési feltételeknek*, ugyanakkor minősíthető *egyoldalú nyilatkozatnak* is. Hatósági jóváhagyása, amely egyes tagállamokban alkalmazhatóságának kötelező előfeltétele is, garantálja azt, hogy a BCR rendelkezéseinek betartásával a vállalkozáscsoport az adattovábbítás célországában letelepedett tagja biztosítja a személyes adatok megfelelő védelmének szintjét.

A BCR azonban nem általános adatvédelmi garanciát nyújt a harmadik országban, hanem csupán az adott vállalkozáscsoport adott tagjának adatkezelési illetve adatfeldolgozási tevékenysége során határozza meg és biztosítja az előírt megfelelő védelmi szintet, amely például egy további (al-)adatfeldolgozó bevonásával már adott esetben teljes funkcióvesztést is eredményezhet. Megjegyzem, a megbízó adatfeldolgozóra történő felelősség telepítés a GDPR 28. cikk (4) alapján bizakodásra ad okot.

DOI: 10.14750/ME.2019.022

A BCR olyan *magatartási kódex-szerű* szabályok alkalmazásának lehetőségét vezeti be, amely lehetővé teszi multinacionális gazdasági társaságok számára, hogy *a* vállalkozáscsoporton belüli személyes adatok – például HR adatbázisok, munkavállalók, vásárlók és ügyfelek adatai – harmadik országba történő továbbítása és ottani kezelése és feldolgozása megfeleljen a GDRP és az érintett Európai Uniós tagállamok részletező vagy megszorító rendelkezéseinek. Ebben a fejezetben a BCR GDPR és Infotv. szerinti fogalmának elemeit vizsgálom.

V.1. Fogalmi megalapozás

A BCR *elsődleges célja*, hogy egységes szabályrendszert hozzon létre, mivel a vállalkozáscsoport egyes tagjai más-más államban végzik adatkezelő tevékenységüket, így eltérő joghatóság alá tartoznak, továbbá eltérő adatvédelmi gyakorlatot folytathatnak, mint *magatartási kódex jellegű keretrendszer* iránymutatást és konkrét szabályokat biztosít az egységesítéshez. Általa az európai uniós adatvédelmi politika exportja globális szinten is megvalósulhat a vállalkozáscsoport tagjai körében, hiszen a harmadik országban működő adatkezelőhöz továbbított adatok védelmi szintjét ez Európai Unió szabályai által előírt szinten kell biztosítani.

A BCR révén az adatvédelmi politika alapelvi és gyakorlati szintű átültetése történhet meg olyan országokban működő cégek esetén, ahol kevésbé kidolgozott az adatvédelem dogmatikai és védelmi szintje. E körben azonban szem előtt tartandó, hogy a BCR kizárólag a gazdasági társaság saját biztosítéka, nem a jogszabályból eredő garancia, és amíg az igényérvényesítés módja és hatékonysága bizonytalan, addig ez a tulajdonsága egyben gyengesége is.

DOI: 10.14750/ME.2019.022

Minden vállalkozáscsoport kötelezettsége, hogy a lehető legszélesebb nyilvánosság elé tárja adatvédelmi politikájának rendszerét, transzparenssé tegye az adatkezelésre alkalmazandó szabályait.

A BCR alkalmazása persze nem feltétlenül jelenti majd, hogy általa valóban átláthatóbb lesz az adattovábbítás gyakorlata. Az azonban kétségtelen, hogy mivel az adattovábbítás a gazdasági társaság működésének és profitjának motorja lehet, üzletpolitikájának szerves részét fogja képezni a GDPR-megfelelés is, így pedig hasonlóan kiemelt figyelmet kap, mint bármely más beruházás. A BCR-rel a vállalkozáscsoport a jogszabályi előírásoknak úgy tehet eleget, hogy mindeközben olyan szabályrendszer szerint jár el, amely *beépül a vállalkozáscsoport struktúrájába*.

A Magyar Közlöny 2015. évi 102. számában megjelent a Infotv. módosítása, amely 2015. október 1. napján léptet hatályba és egy, a magyar jogrendszerben új jogintézményt iktatott be. A törvénymódosítás indokolása és a közzétett hatásvizsgálat utalt arra, hogy a BCR bevezetését a hatályos uniós szabályozás és a tagállami adatkezelők gyakorlata indokolta, továbbá a piaci szféra régóta jelzett igényére is reagált. A GDPR felhatalmazó rendelkezései arra ösztönzik a tagállami adminisztrációkat, hogy a helyes végrehajtás érdekében, amelyet a szubszidiaritás elvére figyelemmel tagállami szinten kell megvalósítani, eljárási szabályokat alkossanak különösen a harmadik országokba történő adattovábbítások esetére. Az Infotv. a BCR tekintetében két részben módosult szignifikánsan. Az egyik jelentős módosítás az *új fogalom* bevezetése, a másik pedig a részben szubsztantív, részben procedurális jellegű szabályok beillesztése a NAIH-ra vonatkozó *hatásköri és eljárási szabályok közé*.

DOI: 10.14750/ME.2019.022

A BCR az Infotv. 3. § 25. pontjában az értelmező rendelkezések között *fogalommagyarázó* módon került rögzítésre.

> *kötelező szervezeti szabályozás:*
> *több országban, de köztük legalább egy EGT-államban is tevékenységet folytató*
> *adatkezelő vagy adatkezelők csoportja által elfogadott és a*
> *Nemzeti Adatvédelmi és Információszabadság Hatóság által jóváhagyott,*
> *az adatkezelőre vagy adatkezelők csoportjára nézve kötelező belső adatvédelmi szabályzat, amely a harmadik országba történő adattovábbítás esetén a személyes adatok védelmét az adatkezelő vagy adatkezelők csoportjának*
> *egyoldalú kötelezettségvállalása útján biztosítja*

Korábban a 29. cikk szerinti Adatvédelmi Munkacsoport vonatkozó Magyarázó dokumentumai soft law jellegű jogforrásként nyújtottak iránymutatást a fogalom tartalmi elemei vonatkozásában a tagállami jogalkotónak.

A GDPR (110) preamubulumbekezdése kiemeli, hogy vállalkozások ugyanazon csoportjai számára *lehetővé kell tenni*, hogy a vállalkozáscsoporton belüli, de harmadik országba irányuló adattovábbítások során BCR-t alkalmazhassanak, ha az minden olyan alapvető elvet és érvényesíthető jogot magában foglal, *„amelyek megfelelő garanciát nyújtanak a személyes adatoknak vagy azok bizonyos kategóriáinak a továbbítására vonatkozóan.”*

DOI: 10.14750/ME.2019.022

A GDPR 4. cikk Fogalommeghatározások 20. pontja deklarálja a BCR fogalmát:

> *„a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ”*

Ebben a fejezetben arra teszek kísérletet, hogy értékeljem a dereguláció szükségességét az Infotv. BCR-re vonatkozó szabályai körében a közvetlenül alkalmazandó GDRP szabályainak tükrében. Azon túl ugyanis, hogy a GDPR közvetlen hatállyal bír, az Infotv. módosítását az egyébként vitatható rendelkezések is indokolták. A BCR fogalmát a 2018. július 25. napján hatályos Infotv-ben foglaltak szerint veszem alapul, tekintettel arra, hogy azt 2018. július 26. napjával hatályon kívül helyezték. Álláspontom szerint a hatályon kívül helyezett Infotv. szerinti fogalomnak több olyen eleme is volt, amely a GDPR szerinti fogalomnak nem része, viszont a jogintézmény jogi jellegében iránymutatást adott, ezért az elemzés körében hasznos azok felelevenítése is.

V.2. A kötelező erejű szervezeti szabályozás mint elnevezés

Az Infotv. 3. § 25. pont értelmező rendelkezése a „kötelező szervezeti szabályozás” terminológiát használta az uniós magyarázó dokumentumok, szakértők és a GDPR magyar nyelvű dokumentumaiban használatos „kötelező erejű vállalati szabályok” elnevezés helyett.

DOI: 10.14750/ME.2019.022

Véleményem szerint nem volt szerencsés egyrészt az, hogy nem vette át a hazai jogalkotó az uniós terminológiát, amely az Infotv. 2015. évi módosításának idején már a GDPR utolsó olvasatban lévő szövegében is elérhető volt. Így azt is gondolhatnánk, hogy nem volt egyértelmű, hogy az akkor bevezetni kívánt jogintézmény azonos-e a GDPR-beli BCR-rel. Másrészt az is aggályos - vagy szándékosan bizonytalan eredménnyel zárult -, hogy az Infotv. fogalma nyitva hagyta a fogalom félárnyékával operáló lehetőségek körét. Az Infotv-ben szereplő „*szervezeti"* elnevezés, amely elnevezésbeli elem eltér az uniós soft law jellegű jogforrásokban bevett terminológiától („vállalati"), vitára adhat okot. A *szervezeti jelző* a hazai irodalomban gyakran utal azokra a jogi személyekre, amelyek körébe beletartoznak az egyesületek, alapítványok, köztestületek és kamarák, esetenként tisztán közjogi intézmények is. A Nemzetközi Vöröskereszt például a magyar szabályok szerint alkalmazhatna BCR-t a harmadik országba irányuló adattovábbítása esetén.

Érdemes figyelemmel lenni arra is, hogy a GDPR angol nyelvi változata „undertakings", a német pedig az „unternehmen" szavakat tartalmazza, amelyek a magyar *gazdasági társaság, cég, gazdasági szereplő* terminológiával azonosítható. A GDPR kizárólag, de legalábbis elsősorban tehát a gazdasági folyamatokban részt vevő jogi személyek részére szánta az eszközt. Ezt erősíti az is, hogy a vállalkozáscsoport fogalmát is rendezi a GDPR 4. cikk 19. pontjában, amelyet ismét a *vállalkozás* terminológiával határoztak meg. Ugyanezt az alapállást támasztotta alá az Infotv. 2015. évi törvénymódosításhoz kapcsolódó hatásvizsgálat is, amely I.1. pontjában a piaci szféra igényeire hivatkozik a módosítás szükségességének indokolásaként. A I.1.1. pontban kifejezetten a vállalkozásokat említi a hatásvizsgálat, és nem például egyesületek vagy alapítványok adatkezelését.

DOI: 10.14750/ME.2019.022

Álláspontom szerint tehát a jogbiztonságot erősítendő érdemes lett volna *átvenni az uniós terminológiákat: a vállalkozáscsoport és a kötelező erejű vállalati szabályok elnevezéseket.* Ha azokat elvetették, akkor jó lehetett volna például a „*vállalkozáscsoporti adatvédelmi kódex*" kifejezés bevezetése, még ha nem is az angol kifejezés tükörfordítása. Utal a szabályok kötelezően alkalmazandó rendszerére mint kódex, kijelöli alkalmazásának személyi hatályát, tehát a vállalatcsoport tagjait, és beazonosítja a szabályozás tárgyát, azaz a személyes adatok védelmének garanciáját az adatokkal végzett minden vállalati tevékenység során.

Megjegyzem *a kötelező jelző félrevezető az uniós elnevezésben is*, tekintettel arra, hogy önkéntesen alkalmazható jogi eszközt jelöl, a kötelező jellege csak akkor áll be, ha a vállalkozáscsoport az alkalmazása mellett dönt, a megfelelési kötelezettség pedig jellemzően vállalkozáscsoporton belüli önkéntes hajlandóságon alapul, kevéssé a külső imperatív kényszeren.

V.3. Fogalmi elemek

A BCR a GDPR alapján az alábbi tartalmi elemekre bonthatók:

a) a személyes adatok védelmére vonatkozó szabályzat
b) az Unió valamely tagállamának területén tevékenységi hellyel rendelkező
c) adatkezelő vagy adatfeldolgozó ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belül követi
d) egy vagy több harmadik országban működő adatkezelő vagy adatfeldolgozó részéről történő adattovábbítás vagy ilyen továbbítások sorozata tekintetében követendő

DOI: 10.14750/ME.2019.022

Az Infotv. szerinti fogalom tartalmi elemei a fentiektől eltérően határozták meg a jogintézményt az alábbiak szerint:

a) több országban, de köztük legalább egy EGT-államban is tevékenységet folytató
b) adatkezelő vagy adatkezelők csoportja által elfogadott
c) a NAIH által jóváhagyott
d) adatkezelőre vagy adatkezelők csoportjára nézve kötelező
e) belső adatvédelmi szabályzat
f) harmadik országba történő adattovábbítás esetén
g) személyes adatok védelmét egyoldalú kötelezettségvállalás útján biztosítja.

Az egyes fogalmi elemek részletes áttekintésére az alábbiakban a 29. cikk szerinti Adatvédelmi Munkacsoport vonatkozó munkadokumentumai alapján teszek kísérletet, párhuzamba állítva a GDPR szerinti és az Infotv. szerinti – már hatályon kívül helyezett - tartalmi elemeket.

GDPR	**Infotv.**
a) a személyes adatok védelmére vonatkozó szabályzat	e) belső adatvédelmi szabályzat

A BCR olyan önkéntesen elfogadott „adatvédelmi szabálycsomag,”[183] amely az érintett által ténylegesen érvényesíthető jogokat tartalmazó megfelelő adatvédelmi és adatbiztonsági intézkedések, alapelvek és kötelezettségek rendszere. A GDPR (110) preamubulum-bekezdése szerint minden olyan alapvető elvet és érvényesíthető jogot magukban foglalnak, amelyek megfelelő garanciát nyújtanak a személyes adatoknak vagy azok bizonyos kategóriáinak továbbítására vonatkozóan. Tehát elvek és jogok összessége.

[183] Európai Bizottság: Milyen előnyökkel jár az uniós adatvédelmi reform az európai vállalkozások számára?http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_hu.pdf (letöltés dátuma: 2015. július 1.)

DOI: 10.14750/ME.2019.022

A fogalommeghatározás a személyes adatok védelmére vonatkozó szabályzatként határozza meg a BCR-t. A belső jelző utalt a vállalkozáscsoport tagjaira mint a BCR személyi hatálya alá tartozó jogalanyokra.

GDPR	**Infotv.**
b) az Unió valamely tagállamának területén tevékenységi hellyel rendelkező	a) több országban, de köztük legalább egy EGT-államban is tevékenységet folytató

A kiindulási ország meghatározásának fogalmi eleme a külföldi adattovábbítás egyik esszenciális feltétele. Pontos volt a kijelölés az Infotv-ben, hiszen az *EGT tagállamok köre tágabb*, mint az Európai Unió tagállamai.

2012-ben az Európai Unió, kiemelten az Európai Bizottság a személyes adatok védelmét rendező uniós aktusok reformjáról határoztak, mivel a tagállamok eltérően implementálták az Adatvédelmi Irányelvet, így több különbség is kialakult a jogalkalmazás során.[184] A személyes adatok védelmének magas szintjét és állandóságát az adattovábbításra vonatkozó szabályok egyszerűsítése mellett szükséges biztosítani. Mindezt úgy kívánta elérni az Európai Bizottság, hogy uniós aktusok alkalmazhatóságát szorgalmazta nem uniós tagállamokban székhellyel rendelkező jogalanyokra,[185] amelynek egyik eszköze - a GDPR extraterritorriális hatályát meghatározó rendelkezések mellett - a BCR lehet.

[184] Európai Bizottság: Commission proposes a comprehensive reform of the data protection rules , 2012. január 25. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (letöltés dátuma: 2012. november 10.)
[185] Miben fogja az uniós adatvédelmi reform megkönnyíteni a nemzetközi együttműködést? – Európai Bizottság, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_hu.pdf (letöltés dátuma: 2012. november 10.)

DOI: 10.14750/ME.2019.022

A GDPR kifejezetten az Európai Unió tagállamát határozza meg, szűkítve a fogalom földrajzi hatályát. Valószínűleg a gyakorlat ad arra a kérdésre választ, hogy a „tevékenységi hellyel rendelkező” kifejezés mit jelent e körben.

GDPR	**Infotv.**
c) adatkezelő vagy adatfeldolgozó ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belül követi	b) adatkezelő vagy adatkezelők csoportja által elfogadott

A többes szám az Infotv-ben arra utalt, hogy a BCR olyan, jellemzően multinacionális vállalkozáscsoportok által alkalmazott eszköz, melyek harmadik országban működő leányvállalatainak, ellenőrzött vállalkozásainak továbbítanak személyes adatokat. Az, hogy egyetlen adatkezelő fogadjon el BCR-t, fogalmilag kizárt, annak jogi jellegéből adódóan.
A GDPR egyértelmű e tekintetben, hiszen alaklmazza az új fogalomként deklarált vállalkozáscsoport fogalmát is.

A BCR alkalmas *bármilyen struktúra szerint kialakított vállalatok* számára, a külön jogi személyként működő leányvállalatok esetére is. A gyakorlat azt mutatja, hogy azon vállalkozáscsoportok tudják előnyösen kihasználni, amelyek nagy mennyiségű adatot, rendszeresen továbbítanak harmadik országban működő ellenőrzött vállalkozásaik számára és nem tudják hatékonyan működtetni a modell klauzulák alkalmazását illetve a harmadik ország nem rendelkezik megfelelőségi határozattal.

Érdekes fejlemény lesz az Egyesült Királyság kilépése az Európai Unióból, amely következtében harmadik országként kell minősíteni mint adattovábbítási célországot. Mivel az adatvédelmi jogi környezete az uniós jogharmonizáción már keresztül ment, valószínűsíthető, hogy a megfelelőségi

DOI: 10.14750/ME.2019.022

határozatot meg fogja kapni. Addig is alternatív megoldásokra lesz szükség, amelyeket korlátozott számban, de az Adatvédelmi Irányelvhez képest szélesebb körben biztosít a GDPR.

Kiemelendő ismét, hogy BCR alkalmazása kizárólag a vállalkozáscsoporton belüli adattovábbítás lehetőségét és jogszerűségét alapozza meg, a vállalkozáscsoporton kívüli címzett részére történő továbbításra hatálya nem terjedhet ki. A BCR jogi természetéből adódik az is, hogy az a vállalkozáscsoport adatkezelése vonatkozásában biztosítja a védelmi szintet, *nem a célország vonatkozásában*.

GDPR	**Infotv.**
d) egy vagy több harmadik országban működő adatkezelő vagy adatfeldolgozó részéről történő adattovábbítás vagy ilyen továbbítások sorozata tekintetében követendő	f) harmadik országba történő adattovábbítás esetén

A BCR jogi természetéből adódóan a külföldi adattovábbítási műveletek esetén értelmezhető és alkalmazandó eszköz. Funkcióját azon esetekben nyeri el, amelyekben olyan harmadik országokban működő többnyire leányvállalatokhoz, fióktelepekre történik az adattovábbítás, ahol *a személyes adatok védelmi szintje nem megfelelő* és az adott állam nem rendelkezik megfelelőségi határozattal. A harmadik ország az Infotv-ben egyértelműen az EGT-államokon kívüli országokat jelölte. Az adattovábbítás Infotv-beli fogalma a 8. § szerinti külföldi jelzővel kiegészülve megfelelően határolta a BCR alkalmazási körét. Noha a GDPR nem tartalmazza sem a harmadik ország fogalmát, sem az adattovábbítás fogalmát, a BCR alkalmazási köre reálisan azonosnak tekinthető.

DOI: 10.14750/ME.2019.022

GDPR	Infotv.
nincs ilyen fogalmi elem	c) a Hatóság által jóváhagyott

Egyes tagállamokban a harmadik országba történő adattovábbítás előzetes, a nemzeti adatvédelmi hatóság általi *engedélyeztetésének kötelezettségét* írja elő. Hazánkban a külföldi adattovábbítás nem volt engedélyköteles és előzetes bejelentéshez sem volt kötött, kizárólag az adatvédelmi nyilvántartás egyik tartalmi eleme volt. Tehát azok az adatkezelők, akik nem voltak kötelesek bejelentkezni az adatvédelmi nyilvántartásba a NAIH tudomása nélkül is továbbíthattak személyes adatot harmadik országba. Az Infotv. 2018. júliusi módosítása – igaz nem a GDPR alá tartozó jogviszonyokra - rendelkezik a hatósági bejelentésről. Amennyiben az adattovábbítás jogszerűségéhez megkövetelt megfelelő védelmi szint azon a vélelmen alapul, hogy az adatkezelő által megvizsgált körülmények és feltételek körében fennállnak a megfelelő garanciák, akkor az adatkezelő az első alkalommal történő nemzetközi adattovábbítást követően haladéktalanul tájékoztatni köteles a NAIH-t a nemzetközi adattovábbítás céljáról, a továbbított adatok címzettjéről és köréről, valamint a nemzetközi adattovábbítás rendszerességéről. A BCR jelentősége éppen az, hogy ha annak szabályait a hatóságok jóváhagyták, utóbb az egyes tranzakciók alkalmával nem kell újra a hatóságokhoz fordulni.

A GPDR sem ír elő semmilyen előzetes bejelentési vagy jóváhagyási kötelezettséget az egyes tranzakciók esetére, azonban a 46. cikk (2) bekezdése szerinti megfelelő garanciák az a) pontban foglalt *közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz* kivételével hatósági vagy az Európai Bizottság jóváhagyásához kötött jogi eszközök. Ennek következtében ha nem is az egyes tranzakciók, de valamennyi adattovábbítási gyakorlat illetve módszer, pontosabban ezek rögzítésére alkalmas jogi eszközök előzetesen átesnek majd nemzeti hatósági vagy Európai Bizottság általi vizsgálaton.

DOI: 10.14750/ME.2019.022

A BCR nemzeti hatóság általi jóváhagyása mint érvényességi kelléke tekinthető a hatálya alatt végrehajtott összes jövőbeni külföldi adattovábbítás előzetes engedélyezésének is. Noha a GDPR szerinti fogalomban explicit nem is szerepel ez a feltétel, a 47. cikk (1) bekezdésének helyes értelmezése szerint az illetékes felügyeleti hatóságnak jóvá kell hagynia a BCR-t.

A NAIH mint tagállami adatvédelmi hatóság egyik *új hatásköre* már 2015 októberétől[186] a BCR-ek jóváhagyása.[187] A NAIH honlapján közzétette az eljárására vonatkozó részletes leírásait illetve a szükséges formanyomtatványt. A hatósági jóváhagyás a BCR ön- illetve társszabályozási jellegét erősíti. Megjelenik ugyanis az a jellemző, hogy a vállalkozáscsoport saját, a jogi előírásokkal összhangban álló szabályait a nemzeti hatóságokkal együttműködve alakítja ki. *Önszabályozási jellege*[188] ott mutatkozik meg, hogy a vállalkozáscsoport olyan magatartás-szabályokat alkot meg, amelyben a saját tagjait szabályozza, az általuk megalkotott előírásokat saját magukra nézve kötelezőnek ismerik el, azok érvényesülését maguk ellenőrzik belső panaszkezelési és monitoring rendszereik útját. *Társszabályozási jellegét* akként nyeri el, hogy a „felülről jövő" jogi szabályozás „eredője (a célok és a keretek meghatározója) az állam, amely viszont teret enged az önszabályozásnak a keretek rugalmas kitöltésére."[189] *A BCR-re azonban tisztán egyik jellemző sem maradéktalanul igaz.*

A BCR szabályai valóban a jogi szabályozásból indulnak ki, amelyek nemcsak célokat és kereteket határoznak meg, hanem konkrét elvárásokat, kötelezettségeket s jogokat is. Ugyanakkor a BCR-ben teret kapnak azok a praktikus megoldások, amelyeket az adott vállalkozáscsoport saját tevékenységére, struktúrájára, adatkezelési műveleteire alapozottan alakít ki.

[186] A NAIH-2223-2/2013/V ügyszámú állásfoglalása 2.2. pontjában rögzítette, hogy az együttműködési eljárásban nemzeti hatóságunk 2015 októbere előtt is részt vehetett.
[187] A jóváhagyási eljárásról részéletesen lásd a VI. fejezetben.
[188] CSINK-MAYER (2012) p. 35.
[189] im. 61.

DOI: 10.14750/ME.2019.022

Az állam általi beavatkozási pontok a saját szabályok jóváhagyásakor és a felülvizsgálatok során, adott esetben jogsérelem esetén a jogalkalmazáskor és a jogi és a saját szabályok érvényesülésének ellenőrzésekor keletkeznek.

GDPR	**Infotv.**
nincs ilyen fogalmi elem	d) adatkezelőre vagy adatkezelők csoportjára nézve kötelező

Az adatkezelő és az adatfeldolgozó elkülönítése a szabályozás során végig eltérően alakult. Az Adatvédelmi Irányelv nem alkalmazta az adatkezelés elnevezést, helyette az adatfeldolgozást használta, amely valójában adatkezelést jelent. Ismerte az adatkezelő fogalmát és használta az adatfeldolgozó kifejezést is, noha ez utóbbit nem definiálta.

Az Infotv. deklarálta mind az adatkezelő és az adatfeldolgozó, mind pedig az adatkezelés és az adatfeldolgozás fogalmakat is. A GDPR noha az adatfeldolgozás fogalmát nem definiálja, operál az adatfeldolgozó fogalmával, és meghatározza az adatkezelés és az adatkezelő pontos definícióját. Az elkülönítés több szempontból is fontos, különösen a felelősségvállalás és a bizonyítási teher szempontjából, de a GDRP az éles különbségeket e körben tompítja azzal, hogy az adatfeldolgozóra is számos kötelezettséget ró és felelősségtelepítő rendelkezéseket is bevezet.

Az Infotv. szerinti BCR definícióban kizárólag az adatkezelő vagy az adatkezelők csoportja jelent meg. Az Infotv. 8. § (2) bekezdés c) pontja a BCR vonatkozásában azonban azt rögzítette, hogy az adatfeldolgozás vonatkozásában is alkalmazhatók szabályai. A fogalmi meghatározás azonban nem szól az adatfeldolgozóról.

DOI: 10.14750/ME.2019.022

A procedurális jellegű szabályokban – az Infotv. 64/A § (1) bekezdése szerint[190] - a BCR engedélyezésének kezdeményezésére is kizárólag az adatkezelő volt jogosult. Indokolhatja ezt az, hogy az adatkezelő az, aki főszabály szerint felelősséget vállal az adatkezelési eljárások során. Indoka lehet továbbá az is, hogy az adatfeldolgozó jellemzően nem tagja a vállalkozáscsoportnak, például egy vállalkozási szerződésben felkért bérszámfejtő cég adatfeldolgozó, amely főszabály szerint nem tartozik az adatkezelő vállalkozáscsoportnál hatályos BCR hatálya alá.

A GDPR szerinti BCR fogalom azonban a BCR-t létrehozó vállalkozás az Európai Unió valamelyik tagállamában letelepedett adatkezelő vagy adatfeldolgozó is lehet. Tekintettel arra, hogy adatfeldolgozók is hozhatnak létre BCR-t, indokolatlan és következetlen volt a magyar szabályozásban megjelenő kettősség. A GDPR bevezeti a vállalkozáscsoport[191] fogalmát is, amely egyértelműen lehatárolja a BCR-t alkalmazni jogosultak alanyi körét.

A WP108 rendelkezik arról is, hogy a jóváhagyásra irányuló kérelemben meg kell jelölni, hogy az al-adatfeldolgozó - aki nem a vállalkozáscsoport tagja, hanem annak például szerződéses partnere - milyen alapon tartozik a BCR betartásáért felelősséggel és milyen alapon történik számára a továbbítás.

Az Infotv. 10. § (2) bekezdése[192] deklarálta az al-adatfeldolgozó igénybevételének lehetőségét. Az adatfeldolgozási szerződéshez csatolni kellett a BCR dokumentumot, mely alapján az az adatfeldolgozó is a megfelelő adatvédelmi szint garanciájaként szolgáló BCR szerint volt köteles eljárni, így az adatkezelés, az adattovábbítás és az adatfeldolgozás jogszerűsége, „gyakorlatias és valószerű”[193] jellege érvényre juthatott.

[190] 2018. július 26. előtti időállapot szerint.
[191] GDPR 4. cikk 19. pont: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások
[192] 2018. július 26. előtti időállapot szerint.
[193] Adatfeldolgozói BCR esetére: WP 204 3. pont 3.1. alpontja 14.p.

DOI: 10.14750/ME.2019.022

A NAIH is vizsgálja a jóváhagyási eljárásban, hogy az adatfeldolgozó vonatkozásában hogyan biztosított a megfelelő védelmi szint. Arra a kétséges helyzetre, ha az adatfeldolgozó további al-adatfeldolgozót venne igénybe és így próbálna az európai standard alól kibújni, az Infotv. 2018. júliusi módosítása bevezette a közvetett adattovábbítás fogalmát,[194] amelynek célja, hogy a teljes adattovábbítási lánc során a megfelelő védelmi szint biztosított legyen, de nem alkalmazandó a GDPR hatálya alá tartozó jogviszonyokra.

Vitára adhat okot, hogy a gyakorlatban egyrészt a vállalkozáscsoport bármely jogsértő tagjáért egy kijelölt tag tartozik felelősséggel. Másrészt a nemzeti jog kiegészítő szabályai alkalmazandók a BCR rendelkezései mellett, így a kijelölt tag végső soron egy másik állam szabályrendszerének betartásáért is felelősséget vállal. Megjegyzendő azonban, hogy a harmadik ország adatvédelmi szintje valószínűleg elmarad az uniós standardtól, ezért szükséges a BCR alkalmazása, így nem valószínű, hogy szigorúbb nemzeti szabályok betartásának elmulasztása miatt kellene felelnie a kijelölt tagnak.

A BCR *kötelező jellege* a befelé irányuló, azaz a megfelelési kötelezettség, és a kifelé irányuló, tehát a többnyire bírói úton történő kikényszeríthetőség oldaláról alapvető fontosságú és egyben érvényességi kelléke is.

A NAIH által közzétett, a jóváhagyási eljárás mellékleteként benyújtandó formanyomtatvány II. rész A) pontja ezen jellemző részletes bemutatását kívánja meg. A kikényszeríthetőség - kifelé irányuló kötelező erő - vonatkozásában a BCR dokumentumban az adatalanyt, mint „kedvezményezett harmadik személyt” kell feltüntetni, mely nyomán jogosult bírói illetve hatósági jogérvényesítésre jogsérelem esetén.
A vállalkozáscsoport az Európai Unióban székhellyel rendelkező, illetve a központi ügyvitel helye szerint uniós tagja vállalja, hogy az esetleges harmadik országban elkövetett jogsértéseket követően az adott Európai Unión

[194] A közvetett adattovábbítás fogalmáról részletesen lásd a IV. fejezet 6.1. pontjában.

DOI: 10.14750/ME.2019.022

kívüli tag magatartásáért felel akként, hogy kártérítés megfizetését illetve egyéb jogorvoslat végrehajtását vállalja. Esetről esetre is történhet a felelős tag kiválasztása, azonban ez az adatalany jogérvényesítése szempontjából nem lehet kedvezőtlen. A bizonyítási teher a felelős tag adatkezelőn nyugszik. Kimentéses a bizonyítás, azaz a felelősséget vállaló tag bizonyítja, hogy a harmadik országbeli tag nem követett el jogsértést illetve nem tartozik felelősséggel. Akkor mentesülhet, ha bizonyítja az elháríthatatlan, adatkezelésén kívüli ok fennállását valamint a kár és a károsult szándékos vagy súlyosan gondatlan magatartása közti okozatosságot. A jogsérelemmel érintett adatalany tényleges jogérvényesítési jogosultsága ezzel azonban még nincs biztosítva, hiszen *ez a felelősséget viselő tag vagyoni viszonyait nem vizsgálja a hatóság a kijelöléskor*, amely adott esetben a kártérítés vagy sérelemdíj megfizetésekor jelentőséggel bírhat. Ezért a BCR kötelező tartalmi elemei között ugyan nem, de a jóváhagyási eljárásban a NAIH által közzétett formanyomtatványának II. rész B) pontjában „meg kell erősíteni”, hogy a felelősséget vállaló tagnak van vagyona vagy vagyontárgya, amelyből fedezni tudja az esetleges kártérítésre marasztalásokat.

A megfelelési kötelezettség - a befelé irányuló kötelező erő –, azaz hogy a vállalkozáscsoport munkavállalói és valamennyi tagja önként betartsa a szabályokat ugyancsak fontos jellemzője a BCR-nek. Az önszabályozási jellegéből adódóan a vállalkozásnál nagyobb hajlandóság mutatkozik - vagy kellene, hogy mutatkozzon - a saját maguk által megalkotott szabályok betartására. A befelé irányuló kötelező erő lényege, hogy a szabályok a vállalkozáscsoporton illetve a szervezeten belüli betartásának elmulasztása esetére belső szankciókat is alkalmazni kell. A szabályok kikényszeríthetősége lehet munkaköri, egyedi munkaszerződésből eredő vagy kollektív szerződésből eredő kötelezettség is, amelynek megszegése esetére a BCR belső mechanizmust és joghátrányt kell, hogy tartalmazzon.

DOI: 10.14750/ME.2019.022

GDPR	Inftov.
nincs ilyen fogalmi elem	e) személyes adatok védelmét egyoldalú kötelezettségvállalás útján biztosítja

A BCR - belső - szabályzat jellegére tekintettel, a vállalkozáscsoport adatvédelmi politikájába illeszkedő jogszabályi kivonat és bizonyos, jellemzően gyakorlati részletszabályokat meghatározó sajátos rendelkezések összessége, amelyet a harmadik országokba történő külföldi adattovábbítás során magára nézve *önkéntes kötelezettségvállalás módjára teljesít*. Mind egyoldalú kötelezettségvállalás, mind általános szerződési feltételek nézőpontból tekintve kötelezővé válik azon adatkezelő számára, akit harmadik országbeli törvényei nem kötnek az Európai Unió tagállamaiban elvárt megfelelő szintű adatvédelem megvalósításához.

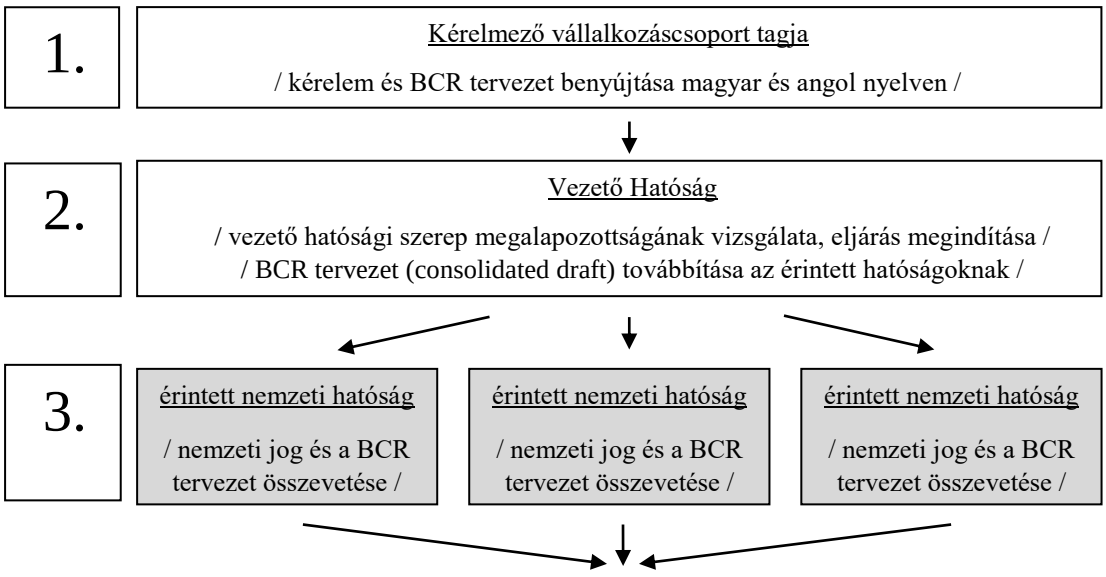
Felvetődik több kérdés a BCR jogi jellegét illetően, elsősorban az érintetti igényérvényesítés oldaláról. Lehet-e hatósági vagy bírói úton kikényszeríthető kötelező jellege egy - belső - szabályzatnak, ha a BCR-t akként azonosítjuk? A belső szabályzat hatálya alá kerülhet-e az az érintett, aki a vállalkozáscsoport egy tagjával áll kötelmi viszonyban? A vállalkozáscsoport munkavállalói esetén ennél egyértelműbb a helyzet, hiszen a munkaszerződés ezt a kapcsolatot megteremti. Ha általános szerződési feltételként (a továbbiakban: ÁSZF) értelmeznénk a BCR-t, akkor mindig kell egy alapul fekvő jogviszony és szerződés, amelyhez kapcsolódhat és a szerződéses közös akarategység. Ez alapján könnyebben elfogadható a kötelező és kikényszeríthető jellege is, azonban kérdés, hogy minősülhet-e egyáltalán ÁSZF-nek az a szabályzat, amely kizárólag az egyik fél magatartására határoz meg szabályokat és a szerződéses akarat létrehozását a felek nem kívánják, sőt a jogi eszköz érvényessége sem követeli azt meg. Álláspontom szerint is az egyoldalú kötelezettségvállaláshoz áll a legközelebb a BCR jogi jellege, a fenti kérdésekre a jogalkalmazás fog végső választ adni.

DOI: 10.14750/ME.2019.022

VI. FEJEZET
A BCR JÓVÁHAGYÁSÁRA VONATKOZÓ ELJÁRÁS

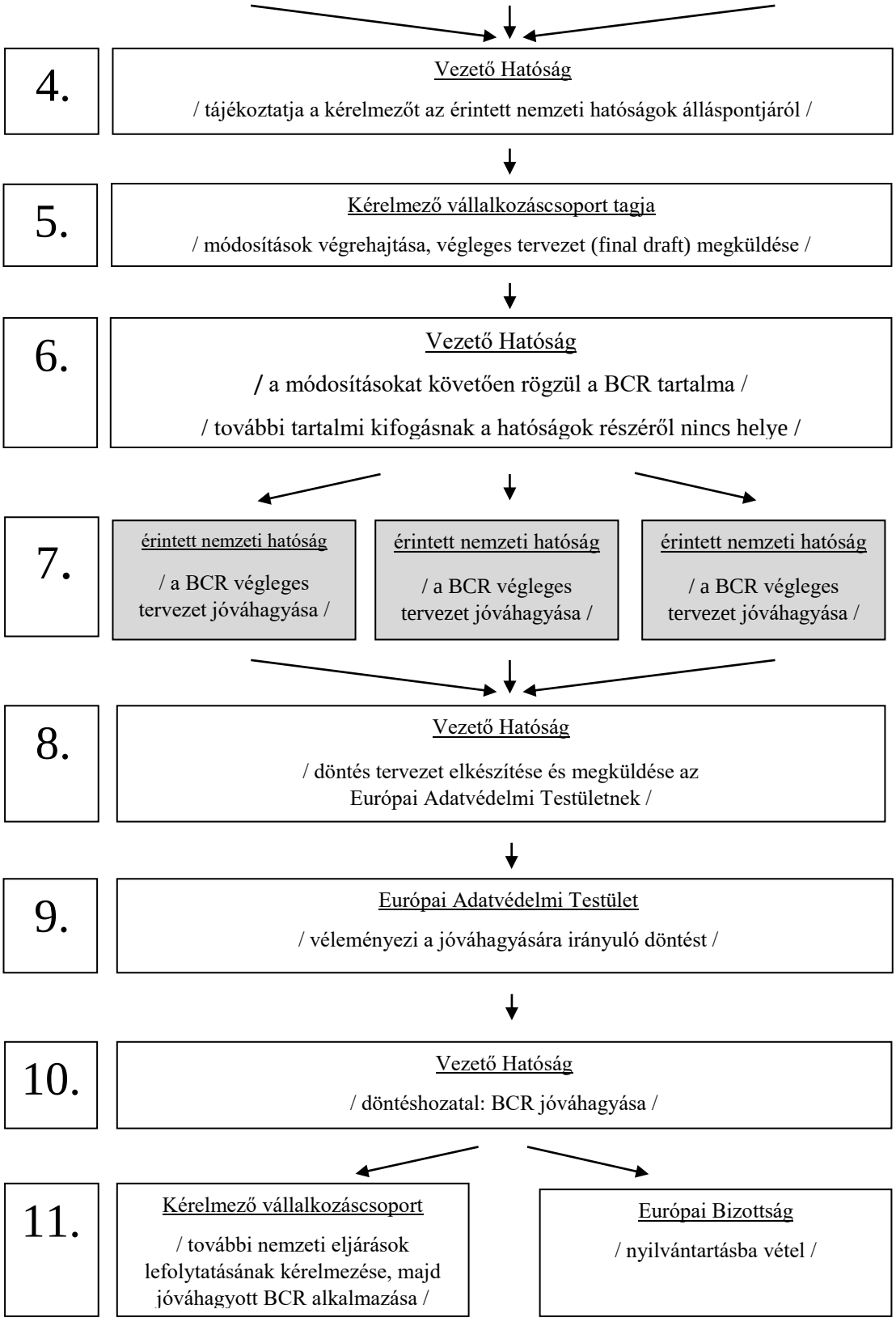
A BCR előzetes hatósági jóváhagyása érvényességi kelléke, egyben fogalmi eleme is a jogintézménynek. Tekintettel arra, hogy a hatósági jóváhagyását az eljárási cselekmények szakterületi újszerűsége, az eljárásban résztvevő tagállami nemzeti hatóságok együttműködési kötelezettsége és az eljárás komplexitása jellemzi, ebben a fejezetben arra teszek kísérletet, hogy ezt a hazánkban előzmény nélküli sajátos eljárásrendet elemezzem. Egyidejűleg a hipotetikus eljárási sémát felvázolva azzal a meggyőződéssel és előfeltevéssel teszek javaslatot a jogalkotásra, hogy az általános közigazgatási rendtartás számos szektorális részletszabállyal kell, hogy kiegészüljön a hatékonyság és jogszerűség érdekében. A hazai szakirodalom csekély számú elemét, a NAIH saját eljárásrendjét a külföldi gyakorlattal együtt vizsgálom. Kiemelem, hogy a NAIH a mai napig vezető hatóságként még nem járt el BCR engedélyeztetés tárgyában, így hazai gyakorlat tulajdonképpen még nem létezik.

A BCR jóváhagyására irányuló eljárás az alábbi *sematikus folyamatábrában* vázoltak szerint történik:[195]



[195] A folyamatábra a WP-k, a NAIH által közzétett saját eljárásrendi szabályok és a brit adatvédelmi hatóság (ICO) https://ico.org.uk/for-organisations/binding-corporate-rules/ [2015. július 10.] gyakorlatának elemzésével készült.

DOI: 10.14750/ME.2019.022



DOI: 10.14750/ME.2019.022

A sematikus folyamatábra egy olyan eljárást vázol, amely valamennyi tagállamban hasonlóan kell, hogy lefolytatásra kerüljön, kisebb-nagyobb, a nemzeti eljárásjog által megkövetelt különbségekkel egy még jóvá nem hagyott BCR vonatkozásában:

1. A vállalkozáscsoport tagja az általa meghatározott vezető hatóságnál kérelmezi a BCR jóváhagyását.

2. A hatóság elbírálja, hogy ténylegesen eljárhat-e vezető hatóság minőségben - e körben megvizsgálja a kérelemben foglalt indokokat és az alátámasztó információkat a WP107 iránymutatását alapul véve -, vezető hatóságként megindítja az eljárást. E körben azon túl, hogy megvizsgálja a kérelmet, a BCR tervezetét és valamennyi benyújtott mellékletet, megkeresi az összes érintett hatóságot annak érdekében, hogy a BCR tervezetét (consolidated draft) a nemzeti jognak való megfelelés körében értékeljék.

3. Az érintett nemzeti hatóságok észrevételeket, módosítási javaslatokat, kifogásokat tehetnek a nemzeti jogukkal való összhang megteremtése érdekében, amelyeket a vezető hatóságnak továbbítanak. Kiemelem, hogy sem a 29. cikk szerinti adatvédelmi munkacsoport által kiadott WP-k, sem az Infotv. nem rögzítik, hogy a vezető hatóság illetve az érintett hatóságok milyen jogi formában jelzik a nemmegfelelőséget a kérelmező számára. A WP107 annyit rögzít, hogy párbeszéd (discussion) folyik a vezető hatóság és a kérelmező között, az érintett hatóságok pedig megjegyzéseket (comment) tehetnek. *Javaslatom, hogy mind a vezető hatóság, mind az érintett hatóságok jogosultak legyenek különböző jogi formában közölni álláspontjukat. Javaslatom szerint akként tipizálhatók az hatóságok álláspontjai, hogy a BCR szövegén kötelező-e változtatni. Ennek nyomán a hatóságok emelhetnek kifogást vagy javasolhatnak módosítást, amelyeket kötelező volna átvezetni, és amelyek figyelmen kívül hagyása a kérelem elutasítását eredményezné, illetve tehetnek észrevételt, amely a megfelelőségen túl a BCR „finomhangolását”, könnyebb alkalmazhatóságát, az értelmezési nehézségek tisztázását eredményezné, de a jóváhagyást nem befolyásolná.*

DOI: 10.14750/ME.2019.022

4. Az érintett nemzeti hatóságok észrevételeit, módosítási javaslatait, kifogásait a vezető hatóság közli a kérelmezővel.

A 3-4. eljárási cselekménysort - elvben - annyiszor kell megismételni amíg a BCR végleges szövege meg nem felel a vezető hatóság és valamennyi érintett hatóság elvárásának és a nemzeti jogoknak. Azonban, de lege ferenda javaslatom[196] mintájára, és ahogy azt az Infotv. módosítására vonatkozó előterjesztés is tartalmazza, a nemzeti jog ezen kvázi hiánypótlási körök számát - elvárt és támogatandó szellemben – maximalizálhatja. A GDPR rendelkezéseihez képest a nemzeti jogok írhatnak elő ugyan bizonyos kérdésekben szigorúbb vagy részletesebb rendelkezéseket, de nem lesznek és nem is lehetnek olyan lényeges eltérések, mint amilyenek az Adatvédelmi Irányelv hatálya alatt lettek volna. Így a BCR szövegének valamennyi érintett nemzeti joggal való harmonizálása alapvető, de egyúttal teljesíthető, a kérelmező adatkezelő oldalán keletkező követelmény is.

5. A kérelmező a jóváhagyás érdekében a szükséges módosításokat végre hajtja a BCR tervezetében és kialakul a BCR végleges tervezete (final draft).

6. A BCR végleges tervezetét a kérelmező ismételten megküldi a vezető hatóságnak, aki továbbítja azt az érintett hatóságoknak.

7. Amint a végleges szöveg megfelelősége megállapítható, az érintett hatóságok jóváhagyásukkal erősítik meg a vezető hatóság döntés tervezetét.

8. A vezető hatóság a GDPR 64. cikk (1) bekezdés f) pontja alapján döntésének tervezetét megküldi az Európai Adatvédelmi Testületnek (a továbbiakban: EAT) véleményezésre.

9. Az EAT véleményt bocsát ki az elé terjesztett ügyről, amelyet a vezető hatóság a lehető legnagyobb mértékben köteles figyelembe venni. A GDPR 64. § (3) bekezdés bevezeti a hallgatás szabályát, azaz amennyiben az EAT kifogást nem támaszt, a döntéstervezetben foglalt döntést a vezető hatóság meghozhatja.

[196] MAKSÓ (2015) p. 152.

DOI: 10.14750/ME.2019.022

10. A vezető hatóság az EAT támogató véleményének birtokában - vagy a vélemény kibocsátására irányadó határidő elteltével - dönt arról, hogy a BCR-t jóváhagyja.

11. A vezető hatóság a döntését közli a kérelmezővel és értesíti az Európai Bizottságot, amely nyilvántartásba veszi és online közzéteszi a vállalkozáscsoport nevét, mint BCR-t alkalmazó adatkezelő vállalkozáscsoportot. Főszabály szerint valamennyi tagállamban, ahol a vállalkozáscsoport a BCR-re hivatkozással kíván adattovábbítást végezni, a már jóváhagyott BCR vonatkozásában is kérelmezni kell a nemzeti hatóság jóváhagyását, kivéve, ha az érintett hatóság részes állama a WP107 szerinti kölcsönös elismerési eljárásnak. Ebben az esetben az adott állam a vezető hatóság a BCR érvényessége vonatkozásában meghozott jóváhagyó döntését saját államában saját nemzeti joga szerint is érvényesnek köteles elfogadni.

A nemzeti eljárások lefolytatásának kötelezettségét alapjaiban módosítandó, sőt végső soron elvetendő szabályozásnak tartom. Ennek indoka *egyrészt* az, hogy ha a BCR jóváhagyása során már a nemzeti hatóság megvizsgálja azt, akkor miért szükséges egy újabb – formális – nemzeti eljárást lefolytatni. A nemzeti eljárásban egy olyan BCR szöveget kell a nemzeti hatóságnak jóváhagynia, amelyet azt megelőzően már megvizsgált, a BCR-ben tartalmi változtatást – hacsak a jogszabályi környezet időközbeni változása miatt elengedhetetlen – nem írhat elő. Az adminisztratív tájékoztatás illetve az eljárási költség más módon rendezhető a nemzeti hatóságok vonatkozásában. *Másrészt* az uniós tagállamok hatóságainak együttműködését kellene fejleszteni, összehangolni, hogy a nemzeti eljárásra utólag, külön már ne legyen szükség. *Harmadrészt*, és talán a lefontosabb érv, hogy napjainkban a digitális európai gazdaság nem tud különbséget tenni állampolgárság és állampolgárság között, az államhatárok sem szabnak gátat az adatgyűjtésnek, adattovábbításnak[197] - ha mégis, az a gazdaság gátját jelenti -, így okszerűtlen, ha a BCR-t csak bizonyos tagállami hatóságok ellenőrzik.

[197] A határokon átnyúló adatkezelések és a harmadik országokba irányuló alkalmazandó jog kérdéséről lásd részletesen a IV. fejezet 2. pontjában foglaltakat.

DOI: 10.14750/ME.2019.022

Javaslatom, hogy a jóváhagyásra irányuló eljárásban vegyen részt valamennyi tagállami nemzeti hatóság. A fentiek alátámasztására a következőkben teszek kísérletet.

A BCR jóváhagyása körében a WP107 alapján zajló *kölcsönös elismerési eljárás* mint hazánkban ez idáig nem alkalmazott jogtechnikai megoldás szükségtelenné tehetné a nemzeti eljárások lefolytatására vonatkozó kötelezettséget. A kölcsönös elismerési eljárásban jelenleg 21 állam vesz rész.[198] Az eljárás célja, hogy rövidítse és gyorsítsa a jóváhagyás folyamatát, ezáltal elősegítse a mielőbbi döntéshozatalt. A kölcsönös elismerési eljárás lényege, hogy amennyiben egy részes állam nemzeti hatósága úgy ítéli meg, hogy az előtte folyó eljárás tárgyát képező BCR megfelel a jogszabályi követelményeknek, akkor valamennyi részes állam hatósága is megfelelőnek tekinti azt, de legalábbis támogató döntéssel segíti a kérelmet befogadó nemzeti hatóságot. Hazánk és így a NAIH, bár a kölcsönös elismerési eljárásnak nem részese, a WP108 szerinti együttműködési eljárásban részt vesz, amely során érintett hatóságként eljár - és eljárt a BCR 2015. évi bevezetése előtt is[199] - a jóváhagyási eljárásokban. Mivel ha hazánkban a vállalkozáscsoport alkalmazni kívánja a BCR-t, az Infotv. előírja a nemzeti jóváhagyási eljárást is, amely a már lezárult együttműködési eljárást követi. Így a kölcsönös elismerési eljárásban való részvétel nem jelentene előrelépést a vállalkozáscsoport szempontjából, hiszen akkor is a NAIH-hoz kellene fordulni a nemzeti jóváhagyási kérelemmel. A NAIH gyakorlata szerint az együttműködési eljárás és a kölcsönös elismerési eljárás lényegében két különböző elnevezésű együttes vizsgálati-véleményezési eljárás, tartalmi szempontból azonos, csak a BCR érvényességére vonatkozóan az előbbi nem jár együtt a nemzeti jóváhagyás nemzeti eljárás nélküli automatizmusával.

[198] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm
[2018. március 29.]
[199] NAIH-2223-2/2013/V állásfoglalás 2.2. pontja

DOI: 10.14750/ME.2019.022

Tekintettel továbbá arra, hogy a jóváhagyott BCR nemzeti jóváhagyására vonatkozó eljárás már csak egy formális eljárás, érdemi vizsgálat ekkor már nem zajlik a nemzeti hatóság előtt, különösen akkor nem, ha a hatóság részt vett az eredeti jóváhagyásra irányuló eljárásban, tulajdonképpen nincs értelme az ilyen nemzeti eljárások lefolytatásának, azon túl, hogy az adott nemzeti nyelvre is lefordítják a BCR-t.

Amennyiben a nemzeti eljárás adminisztrációs érdekeken alapul, úgy előremutatónak találok egy, a jelenleginél részletesebb, a nemzeti hatóságok számára integrált online rendszert, amelyben a jóváhagyás alatt álló vagy már jóváhagyott BCR-k valamennyi jogilag releváns adatához és tartalmához hozzáférhetnek. Mindenestre az Infotv. a nemzeti jóváhagyásra irányuló eljárás előírását akként látom célszerűnek módosítani, hogy egyrészt, amennyiben a NAIH érintett hatóságként részt vett a BCR jóváhagyásában, akkor a nemzeti eljárást már nem kell kérelmezni, hanem a vezető hatóság jóváhagyó döntése ex lege elismert hazánkban is és a BCR automatikusan alkalmazhatóvá válik. Ennek érdekében megfontolandó egy olyan tartalmú törvénymódosítás, amely *a vezető hatóság jóváhagyó döntésének hazai érvényességét, elfogadhatóságát ex lege alapozza meg akkor, ha a NAIH érintett hatóságként részt vett a BCR jóváhagyására irányuló eljárásban*.

Jelen sorok rögzítésekor sincs az Infotv. alapján a NAIH-nak arra irányuló felhatalmazása, hogy más hatóság döntését elismerhetné,[200] még ha az együttműködésre vonatozó GDPR szeritni rendelkezéseket közvetlenül hatályosuló normaként veszi is figyelembe.

[200] HORVÁTH-EGRI (2015) p. 145.

DOI: 10.14750/ME.2019.022

A 29. cikk szerinti munkacsoport 8/2010. számú véleménye[201] ugyan részletesen, már a Weltimmo-ügy[202] és a Google Spain –ügy[203] ismeretében aktualizálta álláspontját az alkalmazandó jog kérdésének vizsgálatára vonatkozóan, a nemzeti hatóságok döntésének (kölcsönös) elismeréséről azonban nem szól, megjegyzendő ezt a korábbi időállapotú szöveg sem rendezte.[204] Itt azonban *nem a döntés kölcsönös elismerésére vonatkozó törvénymódosítást* látok indokoltnak, mint azt Horváth-Egri[205] látta, hanem a vezető hatóság döntésének *ex le hatályosulására teszek javaslatot*, a vezetői engedélyek analógiájára – autót vezethetek bárhol a világon, nem kell külön Kresz vizsgát tennem vagy a jogosítványom jóváhagyását kérnem más uniós tagállamban vagy harmadik országban. Másrészt, amennyiben Magyarországon mint új tagállamban kezdik meg a BCR alkalmazását, úgy egy egyszerűbb, rövidebb vizsgálatot kellene lefolytatni, kizárólag az esetleges - a GDPR jogi természetére tekintettel kis eséllyel előforduló -, a nemzeti joggal ellentétes rendelkezés kiszűrésére.

Mivel a BCR szerinti adattovábbítás nem minősül a GDPR 4. cikk 24. pontja szerinti határokon átnyúló adatkezelésnek[206], ezért a *GDPR 60. cikk szerinti one-stop-shop mechanizmus sem alkalmazandó*. Tehát a BCR jóváhagyására egy ehhez hasonló, de komplexebb hatósági együttműködési/együttdöntési mechanizmust kell megalkotni.

Végső soron célravezetőnek látszik egy olyan átfogó rendszer létrehozása is, amelyben az érintett hatóságokon túl *valamennyi tagállami hatóság megvizsgálná* a BCR tervezetét és csak akkor születhetne jóváhagyó döntés a vezető hatóságnál, ha valamennyi tagállami hatóság kifogást a kérelmező megnyugtatóan rendezne, vagy már első ízben kifogást nem támasztó döntést

[201] WP179 updated
[202] C-230/14. ECLI:EU:C:2015:639
[203] C-131/12. ECLI:EU:C:2014:317
[204] HORVÁTH-EGRI (2015) p. 145.
[205] HORVÁTH-EGRI (2015) p. 145.
[206] A személyes adatok határokon átnyúló kezelése az uniós tagállamokon belüli adatáramlást jelenit

DOI: 10.14750/ME.2019.022

hoztak. Ennek az indoka, hogy a GDPR hatálya és a digitális belső piac az online gazdaság térnyerése révén az adatkezelési műveletek köre már csak nehezen határolható le egy-egy tagállamra, vagy egy-egy tagállam állampolgáraira. Így a BCR hatálya alá kerülő érintettek személye miatt - például nem tudható előre, hogy egy webshopban milyen állampolgárságú személy vásárol – fennállhat adott esetben minden tagállam jogának való megfelelési kötelezettség. Így a 3. és a 7. eljárási stádium kibővülne valamennyi tagállami hatóság részvételével. A megnövekvő munkaterhet ellensúlyozná az uniós szinten meghatározott eljárási költség tagállamonként azonos összegben történő szétosztása, amelynek alapja a vállalkozáscsoport az előző pénzügyi év teljes éves világpiaci forgalmának adott százalékos mértéke lehetne, a bírság összegének megállapításának analógiájára.

Jelen sorok rögzítésének időszakában az Infotv. előírja a nemzeti jóváhagyás lefolytatását. A továbbiakban tehát az eljárás egyes lépéseit elemzem akként, hogy az hazai eljárásjogi környezetbe helyezem el és kiemelem a rendezésre illetve értelmezésre váró kérdéseket.

VI.1. A hazai eljárásjogi környezet

A Magyar Közlöny 2015. évi 102. számában jelent meg az Infotv. módosítása, amely 2015. október 1. napjától léptetett hatályba egy, a magyar jogrendszerben eddig példa nélküli jogintézményt, a „*kötelező szervezeti szabályozást*” és az Infotv. „34/A. A kötelező szervezeti szabályozás jóváhagyására irányuló eljárás” címen a NAIH újabb különleges eljárását is bevezette.

A törvénymódosítás jogértelmezést segítő miniszteri indokolása szerint a BCR hatósági jóváhagyását a 2004. évi CXL. a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény (a továbbiakban: Ket.) szerint rendelte lefolytatni.

DOI: 10.14750/ME.2019.022

Ez az indokolás ésszerű és alátámasztható volt, saját következtetéseim is ezt erősítették,[207] noha volt olyan szerző, aki a Ket. kizártságát állította ugyanekkor.[208]

A Ket. alkalmazásával kapcsolatban azonban *két alapos kifogás* is megfogalmazható volt – bár ezt akkor nemigen tette meg egyetlen szakember sem. Az *egyik kifogás* abból eredt, hogy a Ket. 13. § (2) bekezdés j) pontja részlegesen kivett eljárásnak minősítette az adatvédelmi hatósági eljárást. Ez azt jelenti, hogy a Ket. szabályai csak annyiban voltak alkalmazandók, amennyiben az ügyfajtára vonatkozó törvény eltérő szabályokat nem állapít meg. Az Infotv. mindössze két, de annál fontosabb paragrafusa állapított meg eltéréseket az adatvédelmi hatósági eljárás vonatkozásában, éppen az eljárás tárgyának specialitása okán. Tekintettel arra, hogy az Infotv. 34/A. cím alatti szabályai a BCR jóváhagyására is állapít meg eltérő szabályokat, továbbá a NAIH saját honlapján három, különböző jogállásban eljáró hatóságként kialakított eljárásrendjeit is közzétette, az eljárás tárgyának specialitása elvitathatatlan. Továbbá, mivel a BCR jóváhagyásának eljárása nem tekinthető adatvédelmi hatósági eljárásnak - inkább tekinthető egy klasszikus közigazgatási engedélyezési eljárásnak -, így indokolt lett volna legalább a Ket. 13. (2) bekezdés j) pontjának módosítása, beemelve a részlegesen kivett eljárások közé a kötelező szervezeti szabályozás jóváhagyására irányuló eljárásokat. A jogalkotó ezt nem tette meg, *implicit célja tehát mégiscsak a Ket. alkalmazása volt*, ahogyan a törvény miniszteri indokolása is rögzíti.

A *másik kifogás* azon alapszik, hogy klasszikus közigazgatási hatósági ügynek és hatósági engedélyezései eljárásnak is tekinthető BCR jóváhagyása, amely megalapozza a Ket. alkalmazását, azonban számos olyan különleges eljárási cselekményt kíván meg az eljárás jogi természete, amely ezen általános eljárási keretek közé, a NAIH saját eljárásrendjével kiegészítve is csak nehezen volt beszorítható.

[207] MAKSÓ (2015) p. 150.
[208] HORVÁTH-EGRI (2015) p. 145.

DOI: 10.14750/ME.2019.022

Éppen ezért javasoltam már 2015-ben,[209] hogy indokolt volna a BCR jóváhagyására vonatkozó eljárás rögzítésére az Infotv. nagyobb terjedelmű módosítása vagy az eljárásjogi kérdések alacsonyabb szintű jogszabályban történő részletes rendezése. A tény, hogy a NAIH honlapján tette közzé tájékoztató jelleggel eljárásrendjét, még akkor is, ha az nagyban alapoz a 29. cikk szerinti adatvédelmi munkacsoport soft law jellegű munkadokumentumaira, a jogbizonytalanságnak ad teret. Az a tény, hogy ezen eljárási szabályok jogszabályi keretek közötti rendezése jelen sorok rögzítésének időpontjában is várat magára, talán csak azért nem okozott ezidáig különösebb jogalkalmazói problémát, mert a NAIH főhatóságként még nem hagyott jóvá BCR-t. Nem vezető hatóságként eljárva a már „engedélyezett" BCR jóváhagyására vonatkozó eljárás korántsem jelent olyan komplex folyamatot és nem igényel bonyolult eljárási lépéseket, amelyet a jelenlegi szabályozási környezet ne tudna rendezni. Ettől függetlenül úgy gondolom, hogy *fel kell készülni arra is, hogy a NAIH képes legyen főhatóságként is jogszerűen eljárni*, amelyhez nélkülözhetetlen a pontos *eljárásrend, amely álláspontom szerint jogszabályi keretek között rendezhető* megnyugtatóan.

A BCR jóváhagyására irányuló eljárást az Infotv-ben a „Hatóság által indítható per" és az „Adatvédelmi nyilvántartás" rendelkezései közé helyezte el a jogalkotó 2015-ben. Helyeselhető jogtechnikai lépés volt, hogy a NAIH hatáskörei között kerül feltüntetésre az eljárás, mivel így az egységesség követelménye érvényre jut. Álláspontom szerint azonban a hatásköri szerep azt indokolta volna, hogy az adatvédelmi audit alcímet előzze meg, hiszen jellegében ahhoz az eljárásfajtához áll közel abban a tekintetben, hogy mindkettő az adatkezelő által önkéntesen választható jogi módszer, az adatkezelő eljárásainak jogszerűségét és az adatvédelmi megfelelést szolgálja mindkettő, továbbá a NAIH díj ellenében folytatja le mindkét eljárás típust.

[209] MAKSÓ (2015) p. 153.

DOI: 10.14750/ME.2019.022

Az Országgyűlés 2018 tavaszán a NAIH állásfoglalásával összhangban[210] elfogadott egy módosító törvényjavaslatot,[211] amely kijelölte a NAIH-t, mint felügyeleti hatóságot a GDPR szerinti, Magyarország joghatósága alá tartozó jogalanyok tekintetében a hatósági hatásköröket gyakorló szervnek.

Ezen túl egy, a kis- és középvállalkozások számára könnyítő rendelkezést vezetett be akként, hogy az „előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi GDPR 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik" a hatóság. Ez utóbbi rendelkezés részletes indokolása leírja, hogy elsősorban a hazánkban nagy számú kis- és középvállalkozások és érdekképviseleteik által jelzett aggályok miatt szükséges ez a „hatósági jogalkalmazást orientáló" szabály. Maga az új rendelkezés azonban nem tartalmazza, hogy a figyelmeztetés mint első alkalommal alkalmazható jogkövetkezmény kizárólag a kis- és középvállalkozások esetében volna alkalmazható.

A BCR 2015. évi bevezetése során a törvénymódosítást megelőző hatásvizsgálat a hatósági és *adminisztrációs terhek csökkenését* rögzítette. Az elismerhető volt, hogy - noha hazánkban sosem róttak jelentős adminisztrációs többlet terhet az adatkezelőkre - egyetlen, ám annál komplexebb eljárás lefolytatásával valóban megszűnni látszottak a külföldi adattovábbítások esetén felmerülő többletfeladatok, például szerződéses klauzulák eseti alkalmazása, de legalábbis nagyban leegyszerűsödhetnek a külföldi adattovábbítás adminisztratív követelményei. A NAIH esetében egy korábban nem létező új eljárásfajtát hozott létre a jogalkotó. Ezekhez az eljárásokhoz a jövőben szükségszerűen kapcsolódnak adminisztratív terhek is, valamint a szakszerű ügyintézéshez a hatóság tisztviselői számának bővítése valamint az apparátus ön- illetve továbbképzése is szükséges.

[210] NAIH/2018/2069/2/K
[211] Iromány száma: T/335., Parlex azonosító: W838KPW50003

DOI: 10.14750/ME.2019.022

A 2018. júliusi módosítás hatásvizsgálata ugyancsak azt rögzíti, hogy adminisztratív terheket nem keletkeztetnek ezek a szabályok, mivel az „adatkezelők terheit lényegileg egyensúlyban tartja a bejelentési kötelezettségek szűkítésével és az adatvédelmi hatásvizsgálati kötelezettség előírásával". A NAIH-ra vonatkozóan a hatásvizsgálat azt rögzíti, hogy a többletfeladatok közvetlenül a GDPR-ból fakadnak, a szükséges többletfedezetet a költségvetésbe betervezték.

A jogalkotó azt a megoldást választotta, hogy az Infotv. akként módosult, hogy külön, új cím alá, a „34/A. Az adatkezelési engedélyezési eljárás" szabályai körében rendezi a magatartási kódexek és a BCR jóváhagyását, az ellenőrzési tevékenység engedélyezését, a közigazgatási megállapodásba beillesztendő rendelkezések és a szerződéses klauzulák engedélyezését. Ezen adatkezelési engedélyezési eljárásokra az általános közigazgatási rendtartásról szóló 2016. évi CL. törvényben (a továbbiakban: Ákr.) foglaltakat az Infotv. eltéréseivel kell alkalmazni.

Álláspontom szerint az, hogy hasonló tárgyú eljárásformákat, noha szerkesztéstanilag még mindig vitathatóan, egy külön cím alá rendez az Infotv., immár a korábbihoz képest jobb megoldás. A NAIH-nak új eljárás formát kell bevezetnie, amely új szemléletet, speciális eljárási lépéseket és különösen aktív hatósági és egyben szolgáltató szerepet igényel részéről.

Azt azonban következetlenségnek találom, hogy a *jogalkotó az engedélyezés és a jóváhagyás fogalmakat szinonimaként használja*. A BCR engedélyezése illetve jóváhagyása két eltérő folyamat, sőt e fogalmak jelentése is eltérő tartalmat nyer a BCR hibrid jellege miatt. Míg az engedélyezés esetén alapvetően egy előzetes hatósági vizsgálatot követően kiadott, kifogást nem támasztó pozitív tartalmú döntésre gondolunk, addig a jóváhagyás egy jellemzően utólagos, már a tevékenység végzését követő ellenőrzés jogellenességet vagy nemmegfelelőséget nem mutató eredményeként meghozott hatósági döntés.

DOI: 10.14750/ME.2019.022

A BCR esetében a fentiek eltérő értelmezést nyernek. A következetes az volna, ha új BCR megfelelőségének vizsgálatára – a NAIH akár főhatóságként akár érintett hatóságként járna el – az *engedélyezés fogalmat használná*, összhangban az Infotv. vonatkozó címével, míg más európai hatóság vagy hatóságok által jóváhagyott - azaz engedélyezett - BCR esetében annak - utólagos - jóváhagyását végezné el. A GDPR angol – authorization – szövegváltozata engedélyezést, a német – genehmigung – jóváhagyást, a francia – approuve – jóváhagy, elfogad terminológiát alkalmaz, ettől a különbözőségtől függetlenül is az Infotv-beli következetlenség könnyedén feloldható és a feloldás indokolt volna. A *NAIH nem az adatkezelést engedélyezi, még csak nem is az adattovábbítást, ezért javaslatom, hogy a címből adatkezelési jelzőt a jogalkotó hagyja el, hiszen az megtévesztő.*

Az is helyeselhető, hogy nem külön jogszabály, hanem az Infotv-be kerültek be ezen rendelkezések, így a jogterület integritása megmarad.
A módosítás hatásvizsgálata is kiemeli, hogy a szabályozás helyének és szerkezetének lehetőség szerinti megőrzésével törekszik mérsékelni a kezdeti jogalkalmazásbeli bizonytalanságot, amit a GDPR – és a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló (EU) 2016/680 európai parlamenti és tanácsi irányelv átültetése és – alkalmazása hordoz.
Ez persze maga után vonja azt is, hogy amennyiben a jövőben az eljárási lépéseken módosítani lesz szükséges, úgy kétharmados törvény lévén az hosszú időbe telhet. Továbbá az a kritika sem maradhat el, hogy ugyan a módosítás több részlet vonatkozásában eltér az Ákr. általános szabályától, még így is számos, az engedélyezési eljárásokra vonatkozó értelmezési kérdés marad megválaszolatlan.

DOI: 10.14750/ME.2019.022

Az is megjegyzendő, hogy az Ákr. hatálya már nem tartalmazza az adatvédelmi hatósági eljárást a részlegesen kivett eljárások sorában, így ex lege a hatálya alá kerülnének külön az Infotv-ben lévő rendelkezés hiányában is. Egyértelmű Infotv-beli rendelkezés hiányában, a következőkben az Ákr. néhány jellemző jogintézményét illesztem egy új BCR jóváhagyására vonatkozó eljárás elemeire.

VI.2. Joghatóság, hatáskör és illetékesség

A NAIH hatásköreire vonatkozó szabályok a 2018. júliusi módosítással egy új címmel - „Az adatkezelési engedélyezési eljárás” - bővültek. Az országos illetékességű autonóm közigazgatási szerv az egyetlen, kizárólagosan hatáskörrel rendelkező szerv az adott eljárástípusban. Az Ákr. 18. § szerinti hatásköri vagy illetékességi vita nem merülhet fel a beérkező kérelem alapján hazai szinten.

Nemzetközi szinten a WP107 útmutatása szerint a vezető hatóságot bizonyos szempontok alapján kell kiválasztani.

Elsőként prioritást élvez azon tagállami nemzeti hatóság, amely abban az európai uniós tagállamban működik, ahol a vállalkozáscsoport európai központi irányítási egysége is működik. A WP107 iránymutatása csak annyit mond, hogy európai, álláspontom szerint ez alatt az Európai Uniót kell érteni.

Másodikként követi a vállalkozáscsoporton belül az adatkezelési feladatokra kijelölt vállalat elhelyezkedése szerinti tagállam hatósága, azzal a megjegyzéssel, hogy amennyiben a vállalkozáscsoport központja nem Európai Uniós vagy EGT tagállamban van, úgy ki kell jelölni egy európai, az adatkezelést végző vállalkozást, amely felel azért, hogy a vállalkozáscsoport külföldi tagjai betartják a vállalkozáscsoport adatvédelmi szabályait, kapcsolatot tartanak a vezető hatósággal, és kártérítést fizet a BCR

DOI: 10.14750/ME.2019.022

szabályainak be nem tartásából illetve megszegéséből eredő, a vállalkozáscsoport bármely tagja által okozott kár miatt.

Nem szól a WP arról, hogy ezen tag kijelölésének milyen formai illetve tartalmi követelményei vannak. Érintetti szempontból fontos kritérium, hogy a kijelölt vállalkozásnak van-e fedezete adott esetben a jogsérelem esetén kiszabott sérelemdíj vagy kártérítés megfizetésére, illetve a vállalkozáscsoport milyen módon, például együttesen vagy egyetemlegesen köteles-e helytállni. Ugyan a BCR jóváhagyására vonatkozó kérelem formanyomtatványa tartalmaz erre vonatkozó adatszolgáltatási rovatot, de tisztázatlan, hogy jogosult-e a nemzeti hatóság ezen kijelölést vizsgálni, a kijelölés ellen, amennyiben van másik EGT tagállamban is a vállalkozáscsoportnak tagja, jogosult-e kifogást emelni, és ha igen, milyen szempontok alapján? *Javaslatom, hogy a nemzeti hatóság hatásköri feladatai közé kellene besorolni azt is, hogy a fenti esetben jogosult legyen bizonyos alkalmassági követelmények vizsgálata eredményeként a kijelölést kifogásolni, adott esetben elutasítani a kérelmet kérelmezői jogosultság vagy alkalmasság hiányában.*

E két szempont körében megfontolandó továbbá az is, hogy a 2015-ben az Európai Unió Bíróságának joggyakorlata alapján aktualizált 8/2010. számú vélemény (a továbbiakban: WP179) tág értelmezést ad – igaz ugyan, hogy az alkalmazandó jog kérdése vonatkozásában – „a tagállam területén” a „tevékenységeinek keretében végzett” adatkezelés fogalmának, amely körében értékelendő az „elválaszthatatlanul összekapcsolt” tevékenységek köre is, a harmadik országban működő adatkezelő vonatkozásában is. Ugyanakkor – már a 2010. évi WP179 is rögzíti, hogy – a funkcionális megközelítés alkalmazandó, így értékelendő, hogy melyik letelepedési helyen ténylegesen milyen tevékenységet végez az adatkezelő, a joggyakorlat pedig további hangsúlyt helyez arra, hogy a tevékenység mire illetve milyen célközönségre irányul, kik az érintettek.

DOI: 10.14750/ME.2019.022

A harmadik szempont szerint a BCR jóváhagyására irányuló eljárásban felmerülő irányítási feladatok, adminisztratív terhek szempontjából legalkalmasabb és a vállalkozáscsoporton belüli kikényszerítése szempontjából legkedvezőbb tagállamban lévő vállalat nemzeti hatósága a vezető hatóság szerepére. Ez a forum shopping kvázi legalizált formájának tekinthető, hiszen arra ösztönzi a vállalkozáscsoportot, hogy optimalizálásra törekedve abban a tagállamban kezdeményezze a jóváhagyási eljárást, amelyben egyszerűbb, gyorsabb, olcsóbb a lefolytatása, és csak másodlagos szempont a kikényszerítésre való alkalmasság.

Negyedik szempont az adatkezelés céljára és módjára vonatkozó döntések többsége meghozatalának helye. Álláspontom szerint ez a szempont olyannyira tág, hogy tulajdonképpen alkalmazhatatlan, mivel az adatkezelő személyének meghatározását várja el. Egy vállalkozáscsoporton belül adott esetben több vállalkozás is adatkezelőnek minősülhet, ekkor pedig egy másik szempont szerint kell eljárni. Ugyanakkor az is tény, hogy az uniós jogban általános szempontként alkalmazzák, például a médiairányelv[212] a médiavállakozás honosságának tekintetében.

Ötödik végül az a tagállam, ahonnan a legtöbb adattovábbítás indul az EGT térségen kívülre, azaz a harmadik országokba.

A döntéshozatal helye és az adattovábbítás indulásának helye szerinti technikai-technológiai alapon meghatározott szempontok, szűk értelemben a második, az adatkezelési feladatokra kijelölt vállalat elhelyezkedése szerinti tagállam szempontja részelemeinek a meghatározásából erednek, elvben egybe is eshetnek. Hiszen az adatkezelői minőség egyik attribútuma a személyes adatok kezelésére vonatkozó döntések meghozatalának joga valamint az

[212] Az Európai Parlament és a Tanács 2010/13/EU Irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv) OJ L 95, 15.4.2010, p. 1–24.

DOI: 10.14750/ME.2019.022

adatkezelés fogalmába bele tartozik az adattovábbítás is, mint személyes adatokon végzett művelet. A szempontok nem taxatív és nem is sorrendiséget adó lista[213] - bár prioritást az európai központ szempontja élvez a WP szerint -, a forum shopping lehetőségét mégis elősegíthetik - bár elvben annak nincs jelentősége a vizsgálat tartalmának azonossága okán. A harmadik opportunista szempont azonban éppen arra ösztönzi a vállalkozáscsoportot, hogy az eljárás lefolytatása szempontjából legkedvezőbb tagállami hatóságot jelölje meg. Ez a vállalkozáscsoport számára kedvező, míg az érintett jogvédelme szempontjából a WP semmilyen ellensúlyt nem állít.

A kérelmezőnek is elő kell terjeszteni mindazon információkat, amelyek a vezető hatóságra tett javaslatát alátámasztják. Ezek többek között az alábbiak lehetnek:
- az Európai Unión vagy az EGT tagállamokon belüli adattovábbítások jellege és általános struktúrája, különös tekintettel arra a helyszínre, ahol az erre vonatkozó döntések megszületnek;
- az Európai Unión belüli vállalkozások elhelyezkedése és jogi természete;
- az érintett munkavállalók vagy személyek száma;
- az adatkezelés célja illetve módja;
- a harmadik országokba irányuló adattovábbítások kiindulási helye, függetlenül attól, hogy azok a BCR hatálya alá tartoznak-e;
- a harmadik ország, amely az adattovábbítások célországa.

A kérelem benyújtása szerinti hatóság dönthet úgy, hogy a kiválasztási szempont tartalma és a vállalkozáscsoport indokolása szerint nem a legmegfelelőbb, és a hatóságok egymás között is - mivel a kérelmet befogadó hatóság nyomban megküldi a többi érintett nemzeti hatóságnak az eljárást megindító kérelem első részét, amelyben a releváns információk találhatók - dönthetnek úgy, hogy másik nemzeti hatóság járjon el vezető hatóságként.

[213] WP 107 2.2. pont

DOI: 10.14750/ME.2019.022

Érdekes különbség, hogy míg az alkalmazandó jog körében a vonatkozó szemponttal fennálló leggyengébb kapcsolat is megalapozza az uniós jog alkalmazását, addig a vezető hatóság kiválasztása esetén a legerősebb szempont lesz az irányadó. Míg az alkalmazandó jog körében érthető a megközelítésmód, addig elviekben a vezető hatóság esetén is megfelelő kellene, hogy legyen még a leggyengébb szempont szerinti kapcsolat is, különösen a GDPR szerint harmonizált jogi környezetben.
Ha a vezető hatóságként megjelölt hatóság álláspontja az, hogy a kérelmező nem megfelelően választotta ki, úgy indokolással ellátott javaslatot tesz a megfelelő vezető hatóság kiválasztására.

A WP107 a parttalan viták megelőzése érdekében rögzíti, hogy egy hónapon belül a versengő hatóságoknak döntést kell hozniuk a vezető hatóság személyéről.

A GDPR 65. cikk (1) bekezdés b) pontja szerinti, az EAT vitarendezi eljárás keretében eljár, ha eltérnek az álláspontok azt illetően, hogy az érintett felügyeleti hatóságok közül melyik illetékes a tevékenységi központ tekintetében. Az adattovábbítással érintett nemzeti hatóságok az eljárást lefolytató hatóság eljárása ellen a megindítást követő két héten belül - amely további két héttel meghosszabbítható – élhetnek ellentmondással.

VI.3. A hatósági eljárás altípusai

A NAIH honlapján rövid ismertető leírását adja a jóváhagyás folyamatának. Tekintettel arra, hogy a NAIH ezen leírás szerint jár el - noha az a WP-k iránymutatásán alapuló eljárásrend - indokoltnak találom az eljárásrend jogszabályba foglalását.

DOI: 10.14750/ME.2019.022

A NAIH eljárása formáit három altípusba sorolja attól függően, hogy milyen minőségben jár el:

- vezető hatóságként jár el a jóváhagyásra irányuló eljárásban
- érintett hatóságként, másszóval nem vezető hatóságként jár el jóváhagyásra irányuló eljárásban
- nemzeti eljárás egy, már jóváhagyott BCR esetén

Legkomplexebb és jelentős koordinációs feladatokkal is járó eljárásforma, ha a NAIH vezető hatóságként jár el. Az érintett hatóság - azaz nem vezető hatóság - az eljárás során a vezető hatóság által megküldött BCR-t a nemzeti jog alapján véleményezi, adott esetben módosítási javaslatot tesz, végül a BCR végleges tervezetének megfelelősége esetén a jóváhagyáshoz szükséges megerősítésének küldi meg a vezető hatóságnak.

Amennyiben a vállalkozáscsoport hazai tagja hazánkban is BCR-n alapuló adattovábbítást kíván végezni, úgy a NAIH előtti eljárást – már jóváhagyott BCR esetén – kell kérelmeznie, a kérelem és valamennyi melléklete benyújtásával valamint meg kell fizetnie az eljáráshoz tartozó igazgatási szolgáltatási díjat. A már jóváhagyott BCR esetén a NAIH további követelményt nem támaszt a jóváhagyás érdekében, hivatkozással arra, hogy a BCR-t az együttműködési eljárásban már valamennyi érintett hatóság - köztük adott esetben a NAIH is - megvizsgálta és jóváhagyta, amelyből következik, hogy megfelel az uniós adatvédelmi standardnak.

DOI: 10.14750/ME.2019.022

VI.4. Az eljárás egyes elemeiről

VI.2.1. A nemzeti hatóság a benyújtandó dokumentumokat - a WP-k iránymutatása szerint - a WP 74, WP107 és WP 153 alapján ellenőrzi, ezt követően a BCR tartalmi vizsgálatát végzi a WP 256 és WP 257[214], WP 154 és WP 155 alapján.

VI.4.1. Az eljárás kizárólag kérelemre indítható

A hivatalbóli eljárás a BCR természetéből adódóan kizárt. Árnyalja ezen megállapításom az az eset,[215] amelyben a NAIH kötelezi az adatkezelőt a BCR jóváhagyására vonatkozó eljárás kérelmezésére. Vitatható közigazgatási hatósági rendelkezés egy olyan jogintézmény vonatkozásában, amely alkalmazása önkéntes, és funkcióját az adatkezelő más módon is biztosíthatja.[216]

Az első alapvető eljárási cselekmény, hogy az Ákr. 35. § szerinti kérelem fogalomnak megfelelő formanyomtatványt kell benyújtani, annak kötelező mellékleteivel együtt. Az Infotv. a kérelem bizonyos kötelező tartalmi elemei vonatkozásában is rendelkezik az Ákr. 36. § -ban foglaltakon túl.

Az Infotv. a kérelem *kötelező tartalmi elemeként* rögzíti a BCR tervetété és a BCR kötelező jellegének igazolására szolgáló adatokat. A módosítást megelőzően ugyancsak kötelező volt csatolni az adatkezelő adatvédelmi nyilvántartási számát, vagy azokat az adatokat, amelyeket egyébként a nyilvántartásban is rögzítenie kellene az adatkezelőnek: véleményem szerint ez egy olyan garanciális szabály volt, amely szükségszerűen következik abból, hogy az Infotv. 65. § (3) bekezdés a) pontja - 2018. július 26. napjáig - kivette

[214] A WP 153 aktualizált formái az adatkezelői és az adatfeldolgozói BCR vonatkozásában.
[215] Ügyszám: NAIH/2017/
Előzmény: NAIH/2016/5859/H.
[216] A jogeset elemzését részletesen lásd a VII. fejezetben.

DOI: 10.14750/ME.2019.022

az adatvédelmi nyilvántartásba történő bejelentkezési kötelezettség hatálya alól például a munkáltatókat vagy az ügyfélkapcsolati jogviszonyban fél adatkezelőket. Kötelező tartalmi elem volt továbbá a más EGT-állam hatósága általi jóváhagyást igazoló adatok, amennyiben ilyen eljárásra sor került. Kifogás, hogy ha a BCR-t már más hatóság jóváhagyta, és a NAIH érintett hatóság az adattovábbítások vonatkozásában, úgy az első engedélyeztetési eljárás során nemzeti hatóságunknak is észrevételeznie kellett az eljárás tárgya szerinti BCR-t és a végső döntésről is értesült, így az adat a hatóság által hivatalosan ismert, így az Ákr. 62. § (3) szerint nem kell bizonyítani. Megjegyzendő továbbá, hogy amennyiben az eljáró hatóság az ún. kölcsönös elismerési eljárás[217] részes állama, köteles megfelelőnek elismerni BCR-t további jogcselekmény nélkül. Más kérdés, hogy nemzeti jogunk előírja a NAIH általi jóváhagyását, és hazánk nem is részese a kölcsönös elismerési eljárásnak, de az együttműködési eljárásban részt vesz.[218]

Az előre összeállított[219] *formanyomtatvány* a fenti, bizonyos kötelezően megjelölendő adatok köréhez a NAIH honlapján - mindhárom eljárás típushoz azonos tartalommal - elérhető, benyújtása magyar nyelven, és új BCR jóváhagyására vonatkozó eljárásokban angol nyelven is kötelező.[220] A BCR szövege magyar és angol nyelven egyaránt kötelező mellékletek.

Formanyomtatványt a WP133 is tartalmaz, amellyel a NAIH formanyomtatványát összehasonlítva néhány kisebb, de jelentékeny eltérést tapasztalunk. Az I. rész 1. pont utolsó cellájában a WP133 szerint meg kell jelölni azon EGT tagállamokat, amelyek jóváhagyását a kérelmező kéri. Ehhez képest a NAIH formanyomtatványa ugyanitt azon hatóságok megjelölését is kéri, amelyek már jóváhagyták a BCR-t. Ez vagy már ismert információ a NAIH számára, mert érintett hatóságként már részt vett az eljárásban, vagy

[217] Részletesen lásd: IV.4. pontban.
[218] A nemzeti eljárásra vonatkozó aggályaimról részletesen a VI. fejezetben írok.
[219] A WP108, WP133 alapul vételéve.
[220] Megjegyzés: az angol nyelvű formanyomtatvány a WP 133 részeként érhető el.

DOI: 10.14750/ME.2019.022

olyan információ, amely irreleváns, mert vagy a jóváhagyó határozatot kell mellékelni, és irreleváns a hatóság maga, vagy új BCR jóváhagyása esetén ez a cella üresen marad. Így szükségtelen eleme a formanyomtatványnak.

A NAIH formanyomtatványának további részének szerkesztése innentől eltér a WP133 szerinti mintától, így tartalmi szempontból folytatom az összehasonlítást, formájában a WP133 szerinti struktúrát veszem alapul.

A WP133 az I. rész 2. pontjában az adatkezelés és az adatáramlás folyamatát kéri bemutatni: a BCR hatálya alá tartozó adatok jogi természetét, jellegét, különösen ha egy vagy több kategóriájú adatokra vonatkozik; a tényt, hogy a BCR csak a harmadik országba irányuló adattovábbításokra alkalmazandó, vagy a vállalkozáscsoporton belül minden adattovábbításra; a küldő állam meghatározását; a BCR hatálya alá tartozó adattovábbítások földrajzi körét; beleértve valamennyi fogadó vállalatot, amely EGT államban vagy harmadik országban található. A NAIH formanyomtatványa ugyanezen rovatában számos további információ megadását is megköveteli, csoportosítva az adatkezelés, az adattovábbítás és az adatfeldolgozás körében. Az adatkezelés esetében a tényleges adatkezelés pontos címe vagy web helye, az adatkezelés célja, az érintettek köre, az adatok kezelésének időtartama, az adatok forrása is kitöltendő rovatok. Az adattovábbítás vonatozásában a továbbítás címzettjének neve, teljes címe, az adattovábbítás jogalapja is megadni kért információk. A NAIH formanyomtatványa az adatfeldolgozóra vonatkozóan kéri megadni a kapcsolattartó megnevezését és elérhetőségi adatait, az adatfeldolgozó megnevezését, az adatkezeléssel összefüggő tevékenységét, címét, az adatfeldolgozás helyét (webhely vagy pontos cím), az adatfeldolgozás technológiája (kézi vagy informatikai rendszerrel). Ezeket az adatokat a WP133 II. rész 7. pontban kéri megadni.

DOI: 10.14750/ME.2019.022

A WP133 az I. rész 3. pontjában a vezető hatóság meghatározásának szempontját kéri megjelölni, a NAIH formanyomtatványa ilyen cellát nem tartalmaz. Tekintettel arra, hogy amennyiben a kérelmező az I. részben kitölti a bevonni kért hatóságok cellát, vélelmezhető, hogy a NAIH-t vezető hatóságként kéri eljárni, amennyiben pedig kitölti a BCR-t már jóváhagyó hatóságok cellát, úgy már jóváhagyott BCR nemzeti jóváhagyását kéri. Ha a NAIH érintett hatóság, úgy a kérelmezőtől közvetlenül nem kap iratot. Így tulajdonképpen a fenti adat megjelölésére nincs is szükség.

A nemzeti hatóság, amelyhez a kérelmet benyújtották, megkörözteti a kérelem I. részét az abban feltüntetett nemzeti hatóságok között annak érdekében, hogy a vezető hatóság kiválasztásának megfelelőségét megvizsgálják.

A WP 133 II. rész 4. pontja a BCR kötelező erejének ismertetését tartalmazza, összhangban a NAIH formanyomtatványával. Míg a WP 133-ben a kötelező erő kérdését a vállalkozáscsoport tagjai közötti, a munkavállalókkal szembeni és adatfeldolgozást végző (al)vállalkozóként szerződő partnerei közötti viszonyokban, valamint a kifelé irányuló kötelező erő jogi természetét külön-külön kell bemutatni, a NAIH nyomtatványa szerint a vállalkozáscsoporton belüli és azon kívüli relációkat szeparálja, de azonos tartalmi követelményeket kell megjelölni.

A NAIH formanyomtatványában ezen túl már csak az igazgatási szolgáltatási díj megfizetésére és a számlázásra vonatkozó adatokat kell megjelölni, míg a WP133 számos további pontjában részletezni szükséges az alábbiakat: a BCR gyakorlati hatékonyságát, kikényszeríthetőségét különösen harmadik országokban, a nemzeti hatóságokkal történő együttműködést, a változásbejelentést, valamint a BCR vonatkozó rendelkezésére hivatkozással kell megjelölni az adatvédelmi alapelveknek való megfelelés körülményeit.

DOI: 10.14750/ME.2019.022

Tekintettel a fentiekben kifejtetett számos egyrészt alaki, másrészt tartalmi különbözőségekre, javaslatom, hogy az EAT a GDPR 70. cikk (1) bekezdés i) pontja szerinti jogkörében iránymutatásként, ajánlásoként vagy legjobb gyakorlatonként bocsásson ki egy, *valamennyi tagállamban egységes formanyomtatványt,* amelynek adott rovatai valamennyi tagállamban ugyanazon tartalmi elemre vonatkoznak. A nemzeti eltéréseket egy, a nemzeti hatóság által összeállított, úgynevezett „nemzeti mellékletként" lehessen a kérelemhez csatolni. Ezzel nemcsak a kérelmező, hanem a nemzeti hatóságok munkáját is meg lehetne könnyíteni.

Annak a külön íven benyújtandó dokumentumnak a tartalmáról, amelyet a BCR tervezetén túl az eljáró hatósághoz be kell nyújtani a WP 108 4. pontja az alábbiak szerint rendelkezik. Meg kell jelölni
- a kapcsolattartó személyt
- az adatvédelmi hatóság kiválasztásának indokát
- a vállalkozáscsoport alapvető struktúráját
- az adattovábbítás folyamatát
- a vállalkozáscsoport tagjainak központi ügyintézési helyét
- az adattovábbítás célját és eszközeit
- az adattovábbítás kiindulási helyét és a célországot.

A WP-k szerint az adott eljáráshoz szükséges egyéb dokumentumokat is csatolni kell, melyek nemzeti hatóságonként eltérők lehetnek. Az üzleti titkot tartalmazó, kereskedelmileg érzékeny adatot a kérelemben külön jelezni kell. WP 108 6.3. pontja értelmében a „kereskedelmileg érzékeny", azaz üzleti titoknak minősülő adatot a hatóság az eljárás során nem kíván megismerni, de azt a WP-ben is elismeri az Adatvédelmi Munkacsoport, hogy bizonyos esetekben ez elkerülhetetlen. Meghatározott független személy, osztály kijelölése és egy előre megszerkesztett panasz-bejelentési formanyomtatvány is elvárás a WP 256 2.2. pontja szerint.

DOI: 10.14750/ME.2019.022

Álláspontom szerint a BCR első jóváhagyására irányuló eljárásban valamennyi eljárási cselekmény vonatkozásában hatékony megoldás volna kizárólagosan, legalábbis elsődlegesen az *elektronikus* formát rögzíteni, jogszabályi szinten. Tekintettel a tagállami nemzeti hatóságok kötelező bevonására és az eljárás során keletkező valószínűsíthetően nagy mennyiségű, terjedelmes iratanyag keletkezésére, valamint az eljárás lefolytatása időtartamára, az elektronikus út az eljárás lefolytatásának hatékonyságát bizonyosan növelné. Jelenleg a NAIH formanyomtatványán szereplő útmutató szerint postai úton, szkennelt formában e-mailen vagy faxon is benyújtható a kérelem, amely megítélésem szerint jelentősen növeli az adminisztrációs terheket és nem segíti a környezetvédelmi szempontokat sem.

VI.4.2. Eljárási lépések és határidők

Az Infotv. jelenleg a BCR jóváhagyása vonatkozásában az ügyintézési határidőt az Ákr 50. § (2) bekezdés c) pontja szerinti általános ügyintézési határidőtől hosszabb időtartamban, *180 napban* maximalizálja, azonban más uniós tagállamok gyakorlata ennél jóval hosszabb időtartamot irányoz elő egy-egy eljárás lefolytatásához.[221] Noha a 29. Adatvédelmi munkacsoport magyarázó dokumentumaiban jelezte, hogy a nemzeti adatvédelmi hatóságok szabadon, megkötések nélkül járhatnak el a BCR dokumentumok vizsgálata során a nemzeti jogukkal való összhang vizsgálatakor, erőforrások hiányában (is) az adatvédelmi hatóságok nem, vagy csak hosszú eljárási határidővel tudnak eleget tenni a kérelmeknek.

[221] Az ICO mint az Egyesült Királyság BCR engedélyezésére hatáskörrel rendelkező hatóság tájékoztatója szerint akár 12 hónap is szükséges lehet az eljárás lefolytatásához. https://ico.org.uk/for-organisations/binding-corporate-rules/ (letöltés dátuma: 2015. július 20.)

DOI: 10.14750/ME.2019.022

Jellemzően 1-3 hónap között szóródik az eljárások időtartama az egyes tagállamok nemzeti hatóságai esetében.[222] Ausztriában legfeljebb 6 hónap, Dániában 5 hónap, míg Bulgáriában nagyságrendileg 15 nap alatt hozza meg a nemzeti hatóság döntését, de jellemzően a hazai eljárási időtartam az általános (Cipruson 2-6 hét, Norvégiában és Svédországban legfeljebb 1 hónap, Horvátországban és Olaszországban 45 nap, Hollandiában 6 hét, Csehországban, Észtországban, Litvániában és Lengyelországban valamint Romániában és Szlovéniában szintén 2 hónap, Németország érintett tartományaiban, Liechtensteinben és Spanyolországban legfeljebb 3 hónap). Izland nemzeti hatósága még nem folytatott le BCR jóváhagyására irányuló eljárást, az első időtartamát 5 hónapra becsüli, a következőket már 3 hónap alatt is lefolytathatja.[223]

Ha az EAT vitarendezését kell kezdeményezni illetékességi vita esetén, az eljárás megindulása előtt további egy hónap, amely adott esetben még egy hónappal meghosszabbítható időtartam kalkulálandó, amely az ügyintézési határidőbe az előterjesztés szerint ugyan nem számít be, de a kérelmező vállalkozáscsoport számára előnytelen lehet.

Célszerű volna további, az ügyintézési határidőbe bele nem számítandó időtartamokat meghatározni. Az Infotv. rögzíti, hogy sem a GDPR szerinti együttműködési eljárás, sem pedig az egységességi mechanizmus nem számít bele az eljárási határidőbe. Meg kell jegyezni, hogy a BCR esetén *a GDPR 60. cikk szerinti együttműködési eljárás nem alkalmazható*, így az előterjesztés ezen a ponton nincs figyelemmel a BCR jóváhagyására irányuló speciális eljárás követelményeire, továbbá az egységességi mechanizmus az Ákr. tág értelmezése szerint sem számítana bele a határidőbe.

[222] http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf (2015. október 26.)
[223] http://edz.bib.uni-mannheim.de/daten/edz-k/gdj/16/table_nat_admin_req_en.pdf [2018. április 12.] p. 24.

DOI: 10.14750/ME.2019.022

Álláspontom szerint az Ákr. 48. § (1) bekezdés b) pontja szerinti, a külföldi szerv megkeresésére irányuló, a nemzetközi jogsegélyhez hasonlító jogintézménynek tekinthető az érintett hatóságok kötelező bevonása. Más tagállami (külföldi) nemzeti hatóság vizsgálatát irányozza elő a megkeresés az adott BCR vonatkozásában, ezért indokolható lehet, hogy az eljárás felfüggesztése a jogsegély szerű intézmény igénybevétele esetére is alkalmazható lehessen.

Noha az Ákr. nem rendelkezik a nemzetközi megkeresés, nemzetközi jogsegély intézésének módjáról, ugyanakkor az „EU jogi aktusa, nemzetközi szerződés és törvény felhatalmazást adhat arra is, hogy magyar és külföldi hatóság között együttműködési megállapodás alakítsa ki a nemzetközi jogsegély tartalmát és terjedelmét”.[224] A külföldi szerv fogalma tágan értelmezendő, vagyis az a nem belföldi hatóság, amelyhez a NAIH az Ákr. 25. §-a szerinti megkereséssel nem fordulhat. Tehát a GDPR 47. cikkében meghatározott kötelező erejű vállalati szabályok jóváhagyása esetén az érintett hatóságok megkeresésének valamint észrevételeik a vezető hatósághoz történő beérkezése és azok a kérelmezővel való közlése nem kellene, hogy beleszámítson az eljárási határidőbe.

Az Ákr. bevezett a sommás eljárást. A törvény indokolása szerint sommás eljárás „az egyszerű megítélésű ügyekben alkalmazható, feszes eljárási forma, amely az ügy gyors lezárását teszi lehetővé, ha annak feltételei adottak”. Noha alkalmazására minden olyan ügyben lehetőség van, amelyet a törvény nem zár ki, akkor folytatható le az eljárás ilyen formában, ha a döntés minden jogszabályi feltétele rendelkezésre áll, a tényállás tisztázott, így a döntést nyolc napon belül meg kell hozni. Nyilvánvaló, hogy a BCR jóváhagyására a sommás eljárás nem alkalmazható, ezt az Infotv. 64/c. § (4) bekezdése is deklarálja. A teljes eljárás az a klasszikus közigazgatási eljárási forma, amelyben minden eljárási részcselekmény elvégezhető lehet, amely alkalmas a BCR jóváhagyására vonatkozó eljárás lefolytatására is.

[224] BOROS – DARÁK (2018) 75-78. p.

DOI: 10.14750/ME.2019.022

A kérelmet befogadó nemzeti hatóság köteles megküldeni a BCR tervezetet a többi érintett tagállami adatvédelmi hatóságnak is véleményezésre. A közvetlen megkereséssel érintett nemzeti hatóságok körét az eljárást kezdeményező a kérelmének I. része vonatkozó pontjában megjelölheti. Az eljárás összes dokumentumának tartalma, különösen a BCR tervezetét (consolidated draft), a vállalkozáscsoport struktúráját bemutató adatokat és az adattovábbítás célországainak megjelölését tartalmazó iratok alapján vizsgálhatja a vezető hatóság azt, hogy mely tagállamokat érinti az adattovábbítás akár adatkezelői, adatfeldolgozói, akár az adatalany szempontjából, mind az adatgyűjtés kiindulási országa, mind az adatkezelés vagy adatfeldolgozás célországa vonatkozásában. A megkeresett érintett hatóságok a vezető hatóságnak küldik meg észrevételeiket és módosítási javaslataikat,[225] amelyeket az további megfontolás nélkül köteles volna hiánypótlás vagy módosításra felhívás körében a kérelmező ügyfél számára továbbítani. A BCR tervezetének módosított változatát (final draft) az eljárásban részt vevő valamennyi hatóság megvizsgálja. Megfelelőség esetén a vezető hatóság az érintett hatóságok megerősítése birtokában dönt a BCR jóváhagyása tárgyában. Ezt követően tartalmi kifogásnak nincs helye.

A kérelmezőnek a többi érintett hatóságnál is eleget kell tennie a jóváhagyásra vonatkozó nemzeti eljárás - amennyiben ilyen eljárás lefolytatása szükséges - követelményeinek.

Jelenleg a BCR alkalmazásához valamennyi uniós tagállamban nemzeti jóváhagyás szükséges, kivételt képeznek ez alól Németország egyes tartományai (Baden-Württemberg, Bajorország, Bréma, Hamburg, Hessen, Mecklenburg-Nyugat Pomerania, Szászország), Írország, Szlovák Köztársaság és az Egyesült Királyság. Nem ismeri a nemzeti jog a BCR-t Portugáliában és Lettországban, valamint speciális helyzetben vannak Liechtenstein

[225] Az érintett hatóságok álláspontjának közlése, megítélése, kötelező ereje, jogi természete nem tisztázott. Erre vonatkozó de lege ferenda javaslatom lásd VI. fejezetben.

DOI: 10.14750/ME.2019.022

adatkezelői, mert EGT tagállamként a kormány engedélyezi az adattovábbítást, valójában nem is a BCR-t, a nemzeti hatóság írásos véleménye alapján.[226]

VI.4.3. A módosítás, kiegészítés mint hiánypótlás

Az eljárás során szoros és intenzív párbeszéd folyik a vezető hatóság és a kérelmező között. Ennek oka egyrészt az, hogy a vezető hatóság lesz az a hatósági „kapu", amelyen keresztül a kérelmezőhöz eljut a többi érintett hatóság álláspontja, továbbá a kérelmező is a vezető hatóságnak köteles benyújtani valamennyi iratot és tartani vele a kapcsolatot.
A párbeszéd eredménye, hogy a hatósági észrevételek és kifogások nyomán kialakul a BCR immár *letisztázott szövege (consolidated draft*[227]), amelyet újra valamennyi érintett hatóság észrevételezhet.

Alapesetben az észrevételezés egy hónapon belül lezajlik.
Az észrevételek megtárgyalása során a BCR módosulhat, amely eredményeként létre jön a *végleges szöveg (final draft),* amelyre valamennyi érintett hatóság a jóváhagyáshoz szükséges megerősítést adja.

A közigazgatási hatósági eljárás szerinti *hiánypótlás intézménye* a BCR engedélyezése tárgyában új értelmezést nyerhet, hiszen az Infotv. 64/C. § (3) bekezdése értelmében a NAIH a BCR tervezetének és a kérelem módosítása vagy kiegészítése vonatkozásában nyilatkozattételre hívhatja fel a kérelmezőt. A hatósági észrevételek, módosítási javaslatok, kifogások véleményem szerint nem tekinthetők a klasszikus közigazgatási eljárási értelemben vett hiánypótlásnak, hiszen egy már szabályszerűen előterjesztett és a hatóság által megvizsgált irat ismételt, de megváltoztatott tartalommal

[226] 29. cikk szerinti Adatvédelmi Munkacsoport: National filing requirements for controller BCR ("BCR - C"), 2016. február http://edz.bib.uni-mannheim.de/daten/edz-k/gdj/16/table_nat_admin_req_en.pdf [2018. március 17.]
[227] WP107 8. pont

DOI: 10.14750/ME.2019.022

történő újbóli benyújtása, amelyet módosítás céljából küld vissza a kérelmező ügyfél részére a hatóság. A hiánypótlás jellegét inkább hasonlíthatjuk a közbeszerzési eljárásokban alkalmazott hiánypótlás jogintézményéhez, amely során a hiányok pótlása arra irányul, hogy az ajánlat, itt a BCR megfeleljen az előírásoknak. A hiánypótlás során a már benyújtott iratokat módosítani és kiegészíteni is lehet. Az eljárás eredményes lefolytatása érdekében a hatóság és az ügyfél a szokásosnál szorosabb együttműködésre kell, hogy törekedjen, csak úgy, mint a nemzeti hatóságok egymás közötti eljárásuk során. A NAIH leírása nem rögzíti egyértelműen, de a BCR jóváhagyásáig a nemzeti hatóságok módosítási javaslatainak elege téve akár több alkalommal is, az Infotv. 64/C. § (3) bekezdése értelmében a „szükséges szerinti alkalommal" módosítani szükséges a tervezetet.

Javaslatommal összhangban[228] az Infotv. módosítására vonatkozó 2017. évi előterjesztés *maximalizálta a módosításra felhívások lehetséges számát,* azaz a hatóság három alkalommal hívhatta volna fel a kérelmezőt hiánypótlásra, azonban a módosítás nem tartotta meg a fenti rendelkezést. Ehhez persze az is hozzá tartozik, hogy a hatóságok megfelelő tartalommal, az ügyfél számára érthetően határozzák meg a módosítandó elemek körét, a módosítás indokát és az elvárt tartalom irányait, kereteit. Támogatható a hiánypótlási körök számának maximalizásálása, mert egyrészt a kérelmező számára is kiszámítható eljárási kereteket biztosít, ugyanakkor a hatóságnak is lehetősége van a részletszabályok, a vizsgálat során felvetődő kérdések tisztázására. A hiánypótlás elmulasztása az Ákr. 47. § (1) b) szerinti eljárás megszüntetésére okot ad(hat)ó körülmény. Így indokolt volna itt egy olyan eljárási jellegű szabály megalkotása, amely jogi formát ad ezen módosítási köröknek illetve rögzíti a nem teljesítés esetére vonatkozó jogkövetkezményeket. Javaslatom, hogy a *hiánypótlás nem teljesítése esetére* az *indokolással ellátott benyújtott kérelmezői álláspont megfelelősége* esetén az eljárás jóváhagyással zárulhasson.

[228] MAKSÓ (2015) p. 154.

DOI: 10.14750/ME.2019.022

VI.4.4. Az eljárás nyelve

A WP107 általános irányelvként rögzíti, hogy a kérelem mellékleteként benyújtandó BCR tervezet nyelvi változatait - a különböző nemzeti jogokat tiszteletben tartva és nem sértve a nyelvhasználat szabályait - a vezető hatóság tagállama szerinti nyelven és angol nyelven kell benyújtani. A végleges tervezetet valamennyi érintett hatóság nyelvére le kell fordítani.

Főszabály szerint az eljárás nyelve a NAIH előtt a magyar nyelv, figyelemmel az Ákr. 20. § (1) bekezdésére. Nyilvánvaló azonban, hogy a nemzetközi jelleg a BCR természeténél és funkciójánál fogva szükségszerű eleme az eljárásnak, amely releváns lehet a kérelmező ügyfél, a kérelem és mellékleteinek tartalma, az ügyfél kapcsolattartója vagy a nemzeti hatóságok közreműködése okán is. A kérelmező ügyfél köteles gondoskodni a BCR angol nyelvű, álláspontom szerint hiteles, de legalábbis a kérelmező általi felelős fordításáról. Eltérés vagy értelmezési nehézség esetén a kérelmező nyelve az irányadó, esetünkben a magyar, amelyet szintén jogszabályban kellene rögzíteni álláspontom szerint. A NAIH eljárásrendje is előírja az angol nyelvi változás benyújtását, de nem szól sem a fordítás megfelelőségéről, sem az irányadó változatot nem jelöli ki. A WP dokumentumok iránymutatása szerint a BCR kiemelt nyilvánosságot kell, hogy kapjon, valamint minden alanya számára megismerhetővé kell azt tenni, így azok fordítása valószínűleg nem jelent aránytalan terhet vagy költséget. Bizonyos esetekben a gazdasági szereplők előnyére is szolgál ezek minél szélesebb körben való megismertetése. Munkavállalók esetében például a kollektív szerződéssel vagy az egyedi munkaszerződéssel együtt rendelkezésre bocsátandó. Világszinten ismert termékeket gyártók esetén a honlapjukra töltik fel a jóváhagyott szöveget, ezzel támogatják a BCR nyilvánosságát.[229]

[229] Példák találhatók az alábbi internetes elérhetőségeken: https://www.ericsson.com/en/legal/processor-binding-corporate-rules;

DOI: 10.14750/ME.2019.022

A hatóságok egymás közötti nyelvét bizonyára maguk a hatóságok választják meg a leghatékonyabb kapcsolattartást figyelembe véve. Valószínűleg a gyakorlat és a nemzeti hatóságok emberi erőforrásának képzettsége fogja kialakítani az arra vonatkozó jó gyakorlatot, hogy az egyes nyelvi változatokat hogyan fogják összehasonlítani, értelmezni.

VI.4.5. Eljárási díjak

Az Infotv. miniszteri szinten rendeletben rendeli megállapítani az eljáráshoz kapcsolódó díjakat. A BCR jóváhagyásáért fizetendő igazgatási szolgáltatási díjról szóló 20/2015. (VIII. 31.) IM rendelet 2015. október 1. napi hatállyal az igazgatási szolgáltatási díjat 266.000.-HUF összegben határozta meg. 2018. szeptember 4. napjától az adatkezelési engedélyezési eljárás lefolytatásáért fizetendő igazgatási szolgáltatási díjról szóló 25/2018. (IX. 3.) IM rendelet ugyenzt a díjat már 288.000.-HUF összegen határozza meg.

A díj összegének értékelésekor érdemes figyelembe venni azt a külföldi gyakorlatot, amelyben az egyes adattovábbítások engedélykötelesek. A díjat úgy ajánlatos megállapítani, hogy megérje a gazdasági társaságnak az eljárást megindítani, amellyel hosszú távon kevesebb költsége adódik, mintha az egyes eljárásokat engedélyeztetné vagy adatvédelmi megoldásokat és intézkedéseket vezetne be és alkalmazna hosszú távon.

Megjegyzendő, hogy az a költség, amelyet a BCR kidolgozására illetve a jóváhagyásra vonatkozó eljárási - jellemzően ügyvédi - képviseletre fordítandó, jelenleg még igen magas, ez eltántorító tényező.

http://www.ebayprivacycenter.com/privacy/binding-corporate-rules; http://www8.hp.com/hu/hu/bcr-pages.html;

DOI: 10.14750/ME.2019.022

Meggyőződésem, hogy a díj megállapításakor figyelemmel kell lenni más tagállamok díjaira is, elkerülendő a költségek csökkentés érdekében a forum shopping jelensége.

Összehasonlításként például sem a máltai, sem a dán adatvédelmi hatóság *nem számol fel külön eljárásai díjat* BCR engedélyezésére vonatkozóan.[230] A máltai eljáráshoz hasonlóan azonban támogatandónak találom az éves *átalány összeg* bevezetését arra tekintettel, hogy a BCR egy időszakonként frissülő, módosításra kerülő szabálycsomag, amely hatósági (felül)vizsgálata sem egyszeri alkalom. Ciprus 42.5 euró összegben, Szlovénia 22,66 euró összegben határozta meg díjait, Lengyelországban az illetékbélyeg befizetésének igazolását írták elő.[231]

Az eljáráshoz kapcsolódó költségek további vitatható problémája, hogy valójában több hatóság előtt zajlik az eljárás, azonban a díjat legfeljebb egy hatóság illetve tagállam felé kell megfizetni jelenleg. A többi megkeresett hatóság vajon *kérhet-e díjat eljárásáért* akár a kérelmező ügyféltől, akár a megkereső hatóságtól? Úgy gondolom, erre a kérdésre a rendszeressé váló gyakorlat fogja megadni a mindenki számára kielégítő választ. Amennyiben az az együttműködési forma alakul ki a hatóságok között, hogy a nemzeti hatóság előtti eljárás elmarad, úgy uniós szinten kell egy olyan összeget meghatározni, amely a vezető hatóságnak nagyobb összegű, de arányos, míg a tagállami hatóságoknak azonos összegű eljárási díjat eredményez, de még nem ró aránytalan terhet a kérelmező vállalkozáscsoportra sem.

[230] A máltai és a dán hatóság eljárási díjaira vonatkozó információt a hatóságokkal történő direkt kapcsolatfelvétel útján szereztem.
[231] http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf [2015. augusztus 23.]

DOI: 10.14750/ME.2019.022

VI.4.6. A döntés

A BCR jóváhagyásához a GDPR 47. cikk (1) bekezdés *három feltétel* teljesülését írja elő. A konjunktív feltételrendszert a nemzeti hatóság vizsgálja:
- a vállalkozáscsoport vagy a közös gazdasági tevékenységet folytató vállalkozások csoportja minden érintett tagjára, beleértve az alkalmazottakat is, jogilag kötelező erejű, alkalmazandó és általuk érvényesített;

- kifejezetten rendelkezik az érintetteknek a személyes adataik kezelése tekintetében kikényszeríthető jogairól; és

- megfelel a GDPR 47. cikk (2) bekezdése szerinti tartalmi követelményeknek.

Az eljárás teljeskörű lefolytatását követően a NAIH álláspontom szerint *határozati formában* hozhatja meg érdemi döntését. A határozatban rögzíteni szükséges lehet a Ákr. 81. § (1) bekezdésében foglalt kötelező tartalmi elemeken túl annak kötelező mellékletét, magát a jóváhagyott BCR-t is. Szükséges figyelemfelhívás lehet, akár az indokolásban, hogy az adattovábbítások bármely elemének megváltoztatása esetén a BCR módosítása is hatósági engedélyhez kötött illetve a hatóságok jóváhagyását kell kérelmezni Ebben a körben figyelembe veendő mind a jogszabályi környezet változása, mind a vállalat struktúrájának és az adattovábbítások mechanizmusának változása, amellyel módosul az adattovábbítás folyamata is. A BCR-t alkalmazó vállalkozáscsoportok kötelessége, hogy minden ilyen *változás esetén* a hatóságok engedélyét kérje. Megítélésem szerint ez kevésbé komplex eljárás, mint az eredeti jóváhagyás, így ezen esetekre külön eljárási szabályok rögzítendők.

Mindemellett a BCR-k *időközönkénti kötelező felülvizsgálata* vagy szúrópróba szerű ellenőrzése is támogatandó gyakorlat lehet.

DOI: 10.14750/ME.2019.022

Jóváhagyást megtagadó döntés elvben igen, gyakorlatban nehezen képzelhető el, hiszen a kérelmező vállalkozáscsoport érdeke is az eredményes eljárás, tehát akként fogja módosítani a BCR tervezetét, hogy az kellő mértékben szolgálja érdekeit és megfeleljen a hatóságok elvárásoknak is.

A *BCR nyilvánosságát* támogatandó a NAIH saját honlapján közzéteszi a BCR-t alkalmazó adatkezelő megnevezését. Hasznos lehet, ha az érintett nemzeti hatóságok honlapjain pedig utalhatnak a már engedélyezett BCR-ek elérhetőségére. A WP 153 1.7. pontja szerint is könnyű hozzáférést kell biztosítani a BCR dokumentumhoz. Figyelemmel arra, hogy az eljárással kapcsolatban az ügyfél fogalma a „jogát vagy jogos érdekét az ügy közvetlenül érinti" fordulata szerint jelentős számú ügyfélre[232] terjedhet ki, így az elektronikus közzététel - a hirdetményi úton történő közzététel analógiájára - szintén támogatandó. A NAIH online nyilvánosan elérhető adatbázisa ennek az elvi követelmények akként tesz eleget, hogy abban megjelenik a vállalkozáscsoport megnevezése és hazai tagjainak cégneve, valamint a BCR jóváhagyásának dátuma.[233]

Szélsőséges e körben az uniós gyakorlat. Belgiumban csupán a hatóság véleményét teszik közzé azzal, hogy az adattovábbításokat királyi rendeletben engedélyezik, amelyben hivatkozzák a BCR szövegét is, amely így az igazságügyért felelős minisztérium kezelésében lévő adatként a közérdekű adatokhoz való hozzáférés körében megismerhető, míg Bulgáriában[234], Hollandiában, Lengyelországban és Horvátországban például nem tesz közzé a nemzeti hatóság semmit, Cipruson az adatot továbbító adatkezelő nevét és a célországot a nemzeti hatóság éves beszámolója tartalmazza.
A francia megoldás szerint még a hivatalos lapban is közzéteszik a nemzeti hatóság döntését, amely tartalmazza még az adatkezelő által biztosított

[232] A jelentős számú ügyfél esete állhat fenn például munkavállalók vagy szolgáltatást igénybe vevők esetén, akik automatikusan kerülnek a BCR hatálya alá és lesznek az adattovábbítás érintettjei, adatalanyai.
[233] https://naih.hu/a-bcr-t-magyarorszagon-alkalmazo-adatkezel-k.html [2018. április 13.]
[234] Csupán az adatkezelők nyilvántartása érhető el.

DOI: 10.14750/ME.2019.022

információkat is az adattovábbítás általános céljáról, a továbbítandó adatok jellegéről és jogi természetéről. A legtöbb hatóság az információszabadságra hivatkozással eseti igénylés esetén teszi megismerhetővé az adatokat.

A GDPR 71. cikk i) pontja szerint az EAT saját kezdeményezésére vagy adott esetben az Európai Bizottság kérésére iránymutatásokat, ajánlásokat és legjobb gyakorlatokat bocsát ki az adatkezelők, illetve az adatfeldolgozók által követett, a kötelező erejű vállalati szabályokon alapuló, személyes adatok továbbítására vonatkozó, a 47. cikkben említett szempontok és követelmények, valamint az érintettek személyes adatainak védelmét biztosítani hivatott ugyanazon cikkben említett egyéb szükséges követelmények további pontosítása céljából. Az EAT ezen feladatkörében nemcsak az együttműködési eljárási mechanizmusokat, hanem tartalmi jellegű soft law jellegű jogforrás kibocsátására is felhatalmazást, egyben felkérést is kap az uniós jogalkotótól. A tisztázatlan kérdésekben mielőbb szükség volna iránymutatásra, legalább az EAT-tól, de mindinkább a hazai jogalkotótól.

Az Ákr. 43. § bevezeti a függő hatályú döntés meghozatalának lehetőségét a sommás és a teljes eljárásokban. A BCR jóváhagyására irányuló (teljes) eljárásban a függő hatályú döntés meghozatala kizárt az Ákr. 43. § (8) bekezdés aa) pontja alapján, mivel a NAIH a 2010. évi XLIII. törvény 1. § (2) bekezdés e) pontja szerinti központi államigazgatási szervnek minősül és a döntés központi államigazgatási szerv vezetője hatáskörébe tartozik. Számos jogterületen bevett gyakorlat a hallgatásos szabály alkalmazása, azaz ha a hatóság a jogszabályi határidőben nem hoz döntést, úgy a kérelem szerinti döntés meghozottnak tekintendő. A BCR jóváhagyására életszerűtlen azt feltételezni, hogy több nemzeti hatóság észrevétel nélkül hagyja jóvá a BCR első tervezetét. Továbbá a BCR alkalmazása addig nem lehet is jogszerű, míg azt jóvá nem hagyták, szabályait meg nem vizsgálta a hatóság, tehát a hatóság hallgatása nem minősülhet a BCR alkalmazására vonatkozó engedélynek.

DOI: 10.14750/ME.2019.022

VI.4.7. Jogorvoslat

Az Ákr. 116. § szerint a döntés elleni *fellebbezés* mint rendes jogorvoslat igénybe vétele *kizárt*, tekintettel az Ákr. 116. § (4) bekezdés a) - az elsőfokú döntést központi államigazgatási szerv vezetője hozta - illetve d) - nincs kijelölt másodfokú hatóság - pontjára is tekintettel.

A bírósági felülvizsgálat tárgyában a régi Polgári perrendtartásról szóló 1952. évi III. törvény 327. § (1) bekezdés a) pontja szerinti közigazgatási per körében az ügyfél, mint fogalom fenti értelmezése vitára adhat okot. Jogosult lesz-e például egy munkavállaló bírósági felülvizsgálat igénybe vételével megtámadni a BCR-t jóváhagyó hatósági határozatot, amennyiben az ő személyes adatait is annak hatálya alatt tervezik harmadik országba továbbítani. További kérdés közigazgatási jogvita, hiszen a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) 4 § (5) bekezdés második mondat értelmében egyedi ügyben alkalmazandó általános hatályú rendelkezés akkor lehet közigazgatási jogvita önálló tárgya, ha a jogsérelem az általános hatályú rendelkezés alkalmazása vagy hatályosulása folytán közvetlenül, közigazgatási cselekmény megvalósítása nélkül következett be. Azonban a felperes Kp. 17. § szerinti fogalmának hatálya alá nem fér az érintett, hiszen az „akinek jogát vagy jogos érdekét a közigazgatási tevékenység közvetlenül érinti” fogalmi körbe nem tartozik bele. Ugyanis közvetlenül az adatkezelő magatartása érinti és nem a hatóság döntése, az csak közvetve érinti az érintett adatalany helyzetét, vélt vagy valós jogsérelmét.
Vitatható továbbá, hogy a jogszabálysértést, amennyiben az más tagállami jogszabályra hivatkozással is történik, a nemzeti bíróság hogyan ítéli meg. Perbe lehet-e/kell-e állítani a többi hatóságot is, pl. nem engedélyező döntés elleni jogorvoslat esetén. Kötelezheti-e új eljárás lefolytatására nemzeti bíróság e körben más tagállam nemzeti hatóságát vagy újabb, az eljáró nemzeti hatóság részéről történő megkeresés útján hajtható végre egy ilyen tartalmú bírói döntés?

DOI: 10.14750/ME.2019.022

VII. FEJEZET
EGY NAIH HATÁROZATRÓL

A BCR 2015. októberi bevezetését követően számos vállalkozáscsoport kérelmezte már jóváhagyott BCR-jének nemzeti jóváhagyását a NAIH-tól annak érdekében, hogy külföldi adattovábbításai esetére a megfelelő védelmi szintet a BCR-re hivatkozással biztosíthassa.

Egy vállalkozáscsoport magyarországi tagja viszont nem kérelmezte a BCR nemzeti jóváhagyását, a NAIH pedig határozatban[235] kötelezte erre. A 2017 márciusában született döntés az első olyan, amelynek rendelkező része a kötelezettet a BCR jóváhagyásának kérelmezésére kötelezi, éppen emiatt rendhagyó, de precedens jellege nehezen igazolható. Ebben a fejezetben a határozat kritikai elemzését végzem el.

VII.1. Az ügy tényei

A Kötelezett egy multinacionális vállalkozáscsoport tagja, amely harmadik országba irányuló, de a vállalkozáscsoporton belüli adattovábbításai során a megfelelő védelmi szint biztosítására az adatkezelő által nyújtandó garanciákat kötelező erejű vállalati szabályok (a továbbiakban: BCR) alkalmazásával biztosítja. A BCR-t a francia adatvédelmi hatóság korábban vezető hatóságként már jóváhagyta, az együttműködési eljárásban hazánk - a kötelezett nyilatkozta szerint az adatvédelmi biztos - érintett hatóságként is részt vett. A BCR rendelkezése szerint a Kötelezett azon cégcsoporti tagok közé tartozik, amelyek személyes adatokat továbbítanak harmadik országba. A Kötelezett a BCR a NAIH nemzeti eljárása szerinti jóváhagyását azonban nem kérte.[236]

[235] Ügyszám: NAIH/2017/_; Előzmény: NAIH/2016/5859/H.
[236] A BCR alkalmazhatóságához és a megfelelő védelmi szint biztosítékául való jogi elismertségéhez az érintett tagállami adatvédelmi hatóság nemzeti jóváhagyása is szükséges lehet, a BCR hazai alkalmazásának érvényességi előfeltétele, fogalmi eleme. Részletesen lásd az V. és VI. fejezetben.

DOI: 10.14750/ME.2019.022

VII.2. A pertörténet

2.1. A NAIH - valószínűleg a BCR jóváhagyására irányuló eljárásban érintett hatóságként, bár ez a Kötelezett nyilatkozatának ellentmond - hivatalból észlelte, hogy a vállalkozáscsoport BCR-t kíván alkalmazni.
A BCR szövegének ismeretében azt is észlelte, hogy a vállalkozáscsoport magyarországi tagja a BCR szerint olyan vállalkozás, amely adattovábbítást végez. A határozat rögzíti, hogy a vállalkozáscsoport a WP133 szerinti formanyomtatványon „a BCR jóváhagyását Magyarország vonatkozásában is kérte." A Kötelezett, a BCR a CNIL[237] mint vezető hatóság általi jóváhagyását követően, hazánkban a nemzeti jóváhagyást azonban nem kérelmezte.

2.2. A NAIH azzal kapcsolatban indított vizsgálatot, hogy a Kötelezett a személyes adatok harmadik országba történő továbbítása vonatkozásában betartja-e az Infotv. 8. § szerinti követelményeket.

A NAIH a tényállás tisztázása érdekében a Kötelezettet nyilatkozattételre hívta fel az alábbi tárgykörökben:
- a Kötelezett végez-e harmadik országba irányuló adattovábbítást, és ha igen, adja meg annak részleteit (célország, adattípusok);
- kötelező erővel bír-e a jóváhagyott BCR, és ha igen, a Kötelezett hogyan teljesíti annak tagállami engedélyezésére vonatkozó Infotv-beli előírásokat;
- ha a BCR nem kötelező rá nézve, akkor Kötelezett milyen jogalapon végez harmadik országba irányuló vállalkozáscsoporton belüli adattovábbítást.

A Kötelezett nyilatkozatában előadta, hogy nem végez adattovábbítást harmadik országba, kizárólag a vállalkozáscsoport Franciaországban lévő központjába továbbít adatokat, a francia szerverek tárolják azokat, ahol a francia adatkezelő a francia adatvédelmi jognak megfelelően végzi az

[237] A francia adatvédelmi hatóság elnevezésének rövid változata, a szakirodalomban bevett hivatkozási formája.

DOI: 10.14750/ME.2019.022

adatkezelést és továbbítja az adatokat a harmadik országban lévő tag számára. Rögzítette, hogy a jóváhagyott BCR kötelező erővel bír és alkalmazandó a Kötelezettre is azzal, hogy amennyiben harmadik országba irányuló tag számára adattovábbítást fog végezni a BCR alapján, úgy annak tagállami jóváhagyásáért az Infotv. szabályai szerint fog a NAIH-hoz fordulni.

2.3. A NAIH a tisztességes adatkezelés elvére hivatkozva az adatkezelői kötelező előzetes tájékoztatás tartalmi követelményeit hangsúlyozta, különösen arra az esetre, ha a Kötelezett tudatában van annak, hogy az általa továbbított adatokat másik adatkezelő harmadik országba továbbítja.

A NAIH megállapította, hogy a BCR-ben az exportáló társaságok jegyzékében a Kötelezett is szerepel. A BCR elemzése eredményeként megállapította továbbá, hogy a Kötelezett által kezelt személyes adatok továbbításra kerül(het)nek az adatvédelem megfelelő védelmi szintjét nem biztosító harmadik országba is. Kiemelte továbbá, hogy a BCR 2015. október 1. napját megelőzően jogi elismertsége hiányában hazánkban nem volt alkalmazható „a külföldi adattovábbítás jogalapjaként", azonban bevezetése után is csak akkor lehet hivatkozni rá, mint a megfelelő védelmi szint biztosításának garanciájára, ha azt a NAIH előzetesen jóváhagyta[238].

VII.3. A rendelkezés és a ratio decidendi

3.1. A NAIH annak feltételeként, hogy az hazánkban is érvényesen alkalmazható legyen, a Kötelezettet a vállalkozáscsoportnál alkalmazandó BCR NAIH általi jóváhagyásának kezdeményezésére kötelezte.

3.2. A NAIH álláspontja szerint, ha a BCR az adatkezelőre kötelező, az azt is jelenti, hogy eleget kell tennie az Infotv. által előírt formai követelményeknek.

[238] A jóváhagy ige helyett jelentéstartalma miatt az engedélyez ige használatát javaslom. Részletesen lásd a VI. fejezetben.

DOI: 10.14750/ME.2019.022

A NAIH álláspontja szerint tekintettel arra, hogy a jóváhagyási eljárás nem az egyes adattovábbításokat, hanem a BCR-t egészében érinti, „nem életszerű", hogy a BCR jóváhagyását csak akkor kéri a vállalkozáscsoport magyarországi tagja, amikor felmerül a harmadik országba történő adattovábbítás igénye.

3.3. A NAIH jogfejlesztő céllal rögzíti, hogy ellentétes a BCR céljával az, hogy azt a vállalkozáscsoporti tag magára kötelezőnek ismeri el, azonban a harmadik országba történő adattovábbítás jogalapjaként nem alkalmazza.

3.4. A NAIH a Kötelezett együttműködésre és a szabályozás komplexitására valamint a jogszabályváltozás óta eltelt rövid időre tekintettel bírságot nem szabott ki és enyhítő körülményként értékelte a tényt, hogy a „Hatóság jóváhagyása nélkül alkalmazott BCR segítségével a gyakorlatban csökkentette a jogsértés magánszférára gyakorolt hatását".

VII.4. A jogi érvelés kritikája

Tekintettel arra, hogy még kevés idő telt el ahhoz, hogy a BCR a hazai adatvédelmi gyakorlatban és jogi irodalomban elterjedhessen és ismert jogintézménnyé váljon, a NAIH ezen megállapításával egyetértve szükségesnek tartom a kialakulás folyamatának elemzését. Nemcsak azért, hogy megismerhessük a BCR mögött álló jogi szabályozás tényleges tartalmát, hanem ezért is, hogy a jogfejlesztő elemzés a jogalkalmazó segítségére legyen adott esetben egy vitatható gyakorlat kialakulásának megelőzésében. Ezért a NAIH első olyan határozatát elemzem, amelyben a BCR nemzeti jóváhagyására kötelezte egy vállalkozáscsoport magyarországi tagját.

DOI: 10.14750/ME.2019.022

VII.4.1. Az eljárás lefolytatásának alapja

Az Infotv. VI. fejezete a NAIH hatáskörei vonatkozásában kógens módon rögzíti az eljárás típusokat és azok eredményeként megszülető döntési formákat. A NAIH – többek között - bejelentés alapján vizsgálatot folytat, amelynek eredménye a jelentés. A NAIH hivatalból indít eljárást a bejelentés alapján lefolytatott vizsgálatra tekintettel vagy azokban az esetekben, ha a jogellenes adatkezelés személyek széles körét érinti, vagy nagy érdeksérelmet vagy kárveszélyt idézhet elő. Az eljárásban kötelező hatósági határozatot hoz. Ez a határozat egy hibrid megoldásnak látszik.

A határozat I.2. pontja az eljárás a vizsgálat tárgyát rögzíti. Ha ez alapján feltételezzük, hogy a NAIH vizsgálatot folytatott le, akkor annak eredménye nem lehetne a megszületett határozat – hanem csak egy jelentés, amely nem bír kötelező erővel a kötelezett számára. Tehát ez a hipotézis elvethető.

Ha feltételezzük, hogy a vizsgálatra vonatkozó tartalmat a NAIH mint az előzményi ügyből átvett tartalomként érti, akkor feltételezhetjük azt is, hogy a határozat hatósági eljárás eredményeként született meg és a vizsgálat a hatósági eljárás előzménye volt, amely alapján a hivatalbóli hatósági eljárás indult. Ezzel kapcsolatban egy fontos aggály is felmerül: egyrészt vizsgálat csak bejelentésre indul. Bejelentésre vonatkozó információ a határozatban nem található, tehát bejelentés feltételezhetően nem volt. Másrészt a BCR csekély hazai - jogalkalmazói és szakirodalomi - gyakorlata során nem tisztázott az a kérdés, hogy a BCR vonatkozásában ki minősül érintettnek. Azaz bárki, aki a BCR hatálya alá kerül – például egy ügyfél, aki a vállalkozáscsoport szolgáltatását akár csak egyszer veszi igénybe – élhet-e bejelentéssel? Továbbá a bejelentés tartalma szerint akár a jogellenesség feltételezése, akár csekély valószínűsége esetére is megindul-e az eljárás?

DOI: 10.14750/ME.2019.022

Az érintettek egyelőre tisztázatlan jogaitól függetlenül is, bejelentésre még csak utalás sincs a határozatban, tehát a bejelentésre lefolytatott vizsgálatot követő hatósági eljárás hipotézise elvethető. Megjegyzem az előzményi ügyszám is /H –ra végződik, amelyből egyértelműen következik, hogy az előzményi ügy is határozattal zárult, amely így nem lehetett bejelentésen alapuló vizsgálat.

Ha feltételezzük, hogy az eljárás hivatalból indult hatósági eljárás, akkor ennek megindítására két jogalapot biztosít az Infotv. 60. § (4) bekezdése: a jogellenes adatkezelés személyek széles körét érinti, vagy nagy érdeksérelmet vagy kárveszélyt idézhet elő. A hivatalbóli eljárás indítást alapozza meg mégis az, hogy a határozat azt rögzíti, hogy a NAIH „hivatalból észlelte", hogy a vizsgált BCR szerint a Kötelezett továbbít személyes adatot harmadik országba és a BCR magyarországi jóváhagyását is kérte a vállalkozáscsoport az első jóváhagyás során.

A hivatalbóli eljárás megindításához az Infotv. 60. § (4) bekezdése szerinti vagylagos feltételek egyike sem állt fenn. Egyrészt, tekintettel arra, hogy a NAIH megállapította, hogy a Kötelezett, nyilatkozatával összhangban, nem végez adattovábbítást harmadik országban lévő vállalkozáscsoporti tag számára, a személyek széles körét érintő jogellenesség valószínűsége nem állt fenn. Másrészt a jogellenesség tényét sem lehet igazolni, hiszen ha végzett is volna adattovábbítást a Kötelezett, azt egy már jóváhagyott BCR alapján végezte volna - amelyet a magyar nemzeti hatóság is jóváhagyott az együttműködési eljárásban - tehát az érintettekre nézve annak alkalmazása veszélyt nem eredményezhetett volna, legfeljebb a Kötelezett oldalán a formai követelmények mulasztását. A személyek széles körére vonatkozó feltétel vonatkozásában sem a NAIH vizsgálata, sem a Kötelezett, sem pedig a határozat nem tesz tényállítást, megállapítást, következtetést, így ez a feltétel szintén nem állt fenn.

DOI: 10.14750/ME.2019.022

A nagy érdeksérelem vagy kárveszély előidézésének valószínűsége azért sem állhatot fenn, mivel maga a NAIH állapította meg, hogy a BCR – amelyet jóváhagyott az együttműködés során – megfelel a nemzeti jog elvárásának, tehát annak – akár európai uniós tagállamok közötti, akár harmadik országokban működő vállalkozáscsoporti tagok közötti – alkalmazása jogszerű és biztosítja a megfelelőséget. Ugyanerre alapítottan nem szabott ki bírságot sem a NAIH, azaz a „BCR segítségével a gyakorlatban csökkentette a jogsértés magánszférára gyakorolt hatását" a Kötelezett.

Mivel a BCR szabályai a Kötelezettre nézve kötelezően alkalmazandók, ezért a jogellenesség annak betartása esetén tényszerűen kizárt, így abból érdeksérelem vagy kárveszély nem is következhet. Tehát az egyetlen - feltételezhető - jogsértés kizárólag alaki, a BCR formai követelményét érintheti, amelynek az érintettre semmilyen hatása nincs. Tehát a hivatalbóli eljárás megindítására vonatkozó hipotézis is elvethető.

A fentiekben részletezett alapvető eljárási hiányosság indukálhatja azt a megállapítást, hogy a BCR, mint önkéntes alapon alkalmazható jogi eszköz alkalmazására, illetve azt megelőzően jóváhagyására aggályos kötelezni az adatkezelőt, különösen úgy, hogy a szükségessége ténybelileg sem áll fenn, illetve mind az uniós, mind a nemzeti jog biztosít más jogi lehetőséget is a megfelelésre.

A NAIH hatásköreit az Infotv. a GDPR-ra tekintettel szükséges módosítása bővíteni fogja, de nem támogatandó megoldásnak találnám, ha a hivatalbóli eljárás[239] egyik új alapja lenne az, hogy ha megalapozottan feltételezhető, hogy a vállalkozáscsoport magyarországi tagja BCR alapján harmadik országban működő tag számára továbbít adatot, úgy az együttműködési eljárásban jóváhagyott BCR hazai jóváhagyását – illetve annak elmaradását –

[239] Megjegyzem, a VI. fejezetben foglalom össze, hogy a nemzeti eljárások tulajdonképpen szükségtelenek egy más jóváhagyott BCR esetén, hiszen tartalmi módosítás nem hajtható végre a nemzeti hatóság előírására.

DOI: 10.14750/ME.2019.022

hivatalból észlelve a NAIH az eljárás kezdeményezésére kötelezze a hazai tag adatkezelőt. Fontos, hogy az adattovábbítás tevékenysége és a BCR-re hivatkozás mint konjunktív feltétel igazolható legyen, mert adattovábbítás hiányában okafogyott a BCR alkalmazása, illetve adattovábbítás nemcsak BCR alapján történhet.

VII.4.2. A Kötelezett és más adatkezelők

A NAIH felhívja a Kötelezett figyelmét az adatkezelő tájékoztatási kötelezettségének és az Infotv. 8. § szerinti követelmények teljesítésére arra az esetre, ha az adatokat harmadik országba továbbítják.

Tekintettel arra, hogy mind a Kötelezett nyilatkozata, mind a NAIH megállapítása szerint sem történt a Kötelezett részéről harmadik országba irányuló adattovábbítás, így az Infotv. 8. § szerinti követelményeknek sem kell megfelelnie a Kötelezettnek.

A NAIH helyes megállapítása, hogy a Kötelezettnek tudomással kell bírnia arról, hogy a vállalkozáscsoport EGT–térségen belüli másik adatkezelő tagja harmadik országba irányuló adattovábbítást végez, és erről az érintettet a Kötelezettnek is tájékoztatnia kell. Megjegyzem ez csupán a tisztességes adatkezelés elvéből vezethető le, mert a jogszabályhely szerint ilyen előírás nincs. Kiemelendő, hogy ha az adatokat ténylegesen továbbító vállalkozáscsoport tagja adatkezelőként jár el, úgy a Kötelezett az exportáló tag eljárásért főszabály szerint nem tartozik felelősséggel, hacsak a BCR-ben éppen nem a Kötelezett a felelősség vállalására kijelölt tag.

DOI: 10.14750/ME.2019.022

VII.4.3. Globálisan kötelező

A NAIH rögzíti a határozatban, hogy a BCR fő követelménye, hogy „globálisan kötelező erejű” és kikényszeríthető legyen, hiszen a vállalkozáscsoporton belüli adattovábbítások megfelelőségének garanciáját biztosítja az alkalmazása.

A NAIH ezen megállapításával – jogfejlesztő célzattal – minta eltörölné a különbséget a harmadik országba irányuló adattovábbítás és az EGT-térségen belüli adattovábbítás között, hiszen a BCR céljával összhangban, az adott vállalkozáscsoport esetén így egy egységes adatkezelési és adattovábbítási politika alkalmazandó, függetlenül attól, hogy melyik állam az adattovábbítás célországa. Igaz ugyan, hogy a BCR a vállalkozáscsoport a világ bármely országában működő tagjára kiterjedő szabályozás, de csak a vállalkozáscsoport tagjai tartoznak a hatálya alá, nem az adott harmadik ország. Tehát a BCR csak abban az értelemben globális, hogy a vállalkozáscsoport bármely országban működő tagja alkalmazhatja. Azonban olyan országokba, ahol a nemzeti jog olyan gyenge garanciákat biztosít vagy olyan túlhatalmat enged az adatkezelőknek, hogy a BCR alkalmazásával sem biztosítható a megfelelő védelmi szint, a vállalkozáscsoportok egyszerűen nem továbbítják az uniós polgárok személyes adatait.

A BCR-ben megfogalmazott rendelkezések főszabály szerint éppen az egységesség biztosítása érdekében nem tesznek különbséget a célország szerint a vállalkozáscsoporti tagok között. Feltehetően egyébként adatvédelmi többletkötelezettség csak harmadik országban működő tag számára jelentkezik, míg a harmonizált uniós jogi környezetre tekintettel az EGT-térségen belüli tagok esetén csak csekély mértékű lehet az eltérés.

DOI: 10.14750/ME.2019.022

Elképzelhető olyan vállalkozáscsoport is, amely nem minden tagját vonja a BCR hatálya alá. Valószínűsíthetően azok a tagok maradnak ki, amelyek vagy nem vesznek részt az adattovábbítási-adatkezelési folyamtokban – és adott esetben kizárólag nemzeti adatbázisukat használják –, vagy a nemzeti joggal olyannyira összeegyeztethetetlen az európai standard és a BCR, hogy a megfelelő védelmi szint nem biztosítható, és ezért nem továbbítanak felé személyes adatokat. Ez esetben a vállalkozáscsoportnál alkalmazandó ugyan BCR, de nem minden vállalkozáscsoporti tagra kiterjedően. Jelen ügyben maga a Kötelezett is elismerte, alkalmazandó rá a BCR és magára nézve kötelezőnek is ismerte el, tehát a NAIH erre vonatkozó megállapítása és következtetése a BCR kötelező alkalmazásáról helyes.

VII.4.4. A BCR mint jogalap

A NAIH határozatában többször úgy hivatkozza a BCR-t, mint a külföldi adattovábbítás jogalapját. Ugyanakkor álláspontom szerint a külföldi adattovábbítás *jogalapja nem a BCR.*

A BCR a megfelelő védelmi szint biztosításának egyik módja, de nem minősül jogalapnak. A külföldi adattovábbítás jogalapja – az eljárás lefolytatásakor hatályos- az Infotv. 8. § (1) bekezdés értelmében lehet az érintett kifejezett hozzájárulása vagy az 5. § és 6. § pontban rögzített adatkezelési jogalapok, amelyek egy további konjunktív, esszenciális feltétele a megfelelő védelmi szint biztosítása. Önmagában a BCR léte nem biztosítja az adatkezelés jogalapját. Tegyük fel, hogy egy direkt marketing cég BCR-t alkalmaz, ekkor budapesti székhelyéről az indiai vállalkozáscsoporti tag számára történő külföldi adattovábbítás esetére biztosítja a megfelelő védelmi szintet. Azonban ahhoz, hogy a budapesti cég adatgyűjtése és utóbb továbbítása jogszerű legyen, vagy az érintett hozzájárulása kellett és a továbbítás az Inftov. 8. § (1) bekezdés b) pontja szerint történik – az Infotv. 5. § (1) bekezdés a) pontja szerinti jogalapon és az Infotv. 8. § (2) bekezdés c) pontja szerint biztosított

DOI: 10.14750/ME.2019.022

megfelelő védelmi szint mellett -, vagy pedig az érintett kifejezett hozzájárulása kellett az Infotv. 8. § (1) bekezdés a) pontja alapján. A BCR tehát önmagában nem biztosítja a jogalapot a külföldi adattovábbításokhoz.

VII.4.5. Önkéntes és kötelező

A BCR hibrid jellegét erősít az a jogi jellemzője is, hogy alkalmazása a vállalkozáscsoport önkéntes döntésén alapul. Tekintettel arra, hogy megfelelő védelmi szint biztosítását az adatkezelők más módokon is elérhetik, például szerződéses klauzulák alkalmazásával, a BCR olyan jogi eszköz, amely a vállalkozáscsoport erre irányuló döntésén alapul. A BCR-nek ugyanakkor kötelező ereje van. A kötelező erő értelmezhető kifelé irányuló kötelező erőként, azaz a BCR szabályainak kikényszerítését jelenti harmadik személlyel szemben, például jogsértés esetén az érintetti igényérvényesítés garanciája. A befelé irányuló kötelező erő azt jelenti, hogy a vállalkozáscsoport tagjainak, azok munkavállalóinak is be kell tartania a szabályait, ellenkező esetekre a BCR-nek joghátrányt kell előírnia. Az önkéntesség és a kötelező erő kettőssége eredményezi a BCR azon erősségét, hogy a megfelelési hajlandóság érvényre jut a vállalkozáscsoport mint adatkezelő tevékenységei során.

A NAIH e körben azt is rögzíti, hogy mivel a Kötelezett magára nézve kötelezőnek ismeri el a BCR rendelkezéseit, de azt nem alkalmazza a külföldi adattovábbításainak jogalapjaként, az a BCR fogalmából eredő céljával ellentétes. A BCR célja az, hogy a harmadik országban működő vállalkozáscsoporti tag az uniós standardokat tartsa be és az Európai Unió adatvédelmi védelmi szintjét biztosítsa. Az, hogy az adatkezelő garanciát nyújt, adott esetben a jogellenesség okán bekövetkező kár vagy sérelem reparálása során segíthet, de a fő cél az, hogy a jogellenesség be se következzen, a valószínűsége a lehető legkisebbre csökkenjen. Ezen túl az EGT-térségbeli tagok bármely további jogszerű eljárása nem volna jogellenes,

DOI: 10.14750/ME.2019.022

így fel sem merülhet az érintetti igényérvényesítés kérdése, tehát a kifelé irányuló kötelező erő érvénye nem sérülne, a BCR megszegése pedig a vállalkozáscsoporton belül szankcionálási mechanizmus, tehát a befelé irányuló kötelező erő tárgya, a nemzeti hatóságnak abba főszabály szerint beleszólása nincs. Tehát a NAIH fenti érve igaz, de a gyakorlatban hatásának csak a vállalkozáscsoporton belüli viszonyok rendezésében van jelentősége, amely jogszabály megsértése hiányában valójában a felek között a magánjogi szabályok szerint rendezhető.

A NAIH fenti következtetésével azt is állítja tehát, hogy egy vállalkozáscsoportnál a BCR léte a contratio azt is jelenti, hogy más alapon illetve módon nem biztosítható a megfelelő védelemi szint és ennek következtében a jogalapként is csak az Infotv. 8. § (1) bekezdés b) pontja volt felhívható. Ez a következtetés kétség kívül messze mutat a határozat rendelkező részében foglaltakon, azonban ennek elfogadása mint a döntés ratio decidendi tételmondata, majd a jövőben precedensként hivatkozni hivatott elvi megállapítása is messze elvezet a BCR jóváhagyásának valódi céljától, amely valójában a nemzeti jogokkal való összhang megteremtését szolgálja. Itt azt is érdemes megjegyezni, hogy az érintett szempontjából a BCR alkalmazásán túl kedvezőbb és biztosabb megoldások is léteznek.[240] Az persze igaz, összhangban a hatósági állítással, hogy a BCR célja kétség kívül az egységes adatvédelmi politika kialakítása a vállalkozáscsoporton belül. Ezt az egységet nem volna célszerű azzal megbontani, hogy az egyik tag éppen a külföldi adattovábbításai körében más szabályok szerint jár el, de sem egyedi jogszabályhelyi, sem gyakorlatbeli szabály nem hívható fel arra az esetre, hogy BCR alkalmazása esetén miért ne lehetne más jogalapon adattovábbítást végezni.

[240] Maga a 29. cikk szerinti munkacsoport sem tartja a BCR-t a legjobb eszköznek a megfelelő védelmi szint biztosítására.

DOI: 10.14750/ME.2019.022

Jellemző, hogy a vállalkozáscsoportok olyan tagok számára, amelyek nem tartoznak a BCR hatálya alá, az Európai Bizottság által határozatban elfogadott[241] modell klauzulákat alkalmazzák a megfelelő védelmi szint biztosítására. Sem a GDPR, sem a 29. cikk szerinti Adatvédelmi Munkacsoport vonatkozó ajánlásai illetve munkadokumentumai, sem az Infotv. nem szól arról, hogy a BCR és a modell klauzulák ne volnának párhuzamosan alkalmazandók. Az persze a vállalkozáscsoport szintjén is operatív nehézségeket szülne, ha keveredne a BCR és a modell klauzulák alkalmazása, de a gyakorlatban valószínűleg nem jelentene jelentős különbséget. Összeségében azonban arra vonatkozóan sem kógens, sem soft law jellegű szabály nincs, hogy BCR esetén nem lehetne más módon is biztosítani a megfelelő védelmi szintet.

Amennyiben a NAIH irányadónak tekintette a határozat szerinti álláspontot, azaz hogy BCR esetén a külföldi adattovábbítás kizárólag az Infotv. 8. § (1) bekezdés b) pontja lehetett és a megfelelő védelmi szint kizárólag az Infotv. 8. § (2) bekezdés c) pontja szerint volt biztosítható, a BCR befelé irányuló kötelező erejét megerősítette ugyan, de tételes jogi előírással ezt alátámasztani nem lehetett álláspontom szerint.

VII.4.6. Életszerűség

A NAIH rögzíti, hogy nem életszerű az, ha a BCR jóváhagyását csak akkor kérelmezi a Kötelezett, ha a vállalkozáscsoporton belüli külföldi adattovábbítás igénye felmerül.

[241] Adatkezelők és adatfeldolgozók között: 2010/87/EU A Bizottság határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről HL L 39., 2010.2.12., 5—18. o. Adatkezelők között: 2001/497/EK A Bizottság határozata (2001. június 15.) a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről HL L 181., 2001.7.4., 19—31. o., magyar különkiadás fejezet 13 kötet 26 o. 347 - 360 valamint 2004/915/EK A Bizottság határozata (2004. december 27.) a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről HL L 385., 2004.12.29., 74—84. o.

DOI: 10.14750/ME.2019.022

A legnagyobb előrelátás esetén sem járna el úgy egyetlen cég sem, hogy egy olyan tevékenység megfelelőségi követelményeinek tegyen eleget, amelyet ténylegesen nem végez. A gazdasági szereplők igyekszik elkerülni, hogy olyan költségeket fizessenek meg előre, amely megtérülésére csekély az esély. Márpedig a BCR jóváhagyása az eljárási díjon túl jelentős további költséggel és adminisztrációs feladatokkal jár. A BCR engedélyezése hasonlatos a vadásztársaságok esetére. Egy egyesületi formában működő vadásztársaság tagja bárki lehet, de ahhoz, hogy jogosult legyen vadászni, vadászvizsgát kell tennie. De pusztán azért, mert valaki tagja egy vadásztársaságnak, egyetlen hatóság sem fogja arra kötelezni, hogy tegyen vadászvizsgát. Az érintett fog vizsgát tenni, ha ténylegesen vadászni akar.

Ebben az ügyben is a Kötelezettnek kell kérelmeznie a BCR jóváhagyását, ha adatot továbbít. A NAIH minta figyelmen kívül hagyná azt az eshetőséget is, hogy egy vállalkozáscsoport nem köteles minden tagját a BCR hatálya alá vonni. A BCR hatálya alá nem tartozó harmadik országbeli tagok esetén értelemszerűen más módon kell biztosítani a megfelelő védelmi szintet. A NAIH tehát kizárja annak a helyzetnek az egyébként valószínűsíthető kialakulását, hogy a Kötelezett olyan harmadik országban működő tagnak továbbítana adatot, amely nem tartozik a BCR hatálya alá. Ha elfogadnánk a határozat helyességét, azt oda vezetne, hogy a vállalkozáscsoport olyan tagjának, amely nem tartozik a BCR hatálya alá, végső soron nem is továbbíthatna személyes adatot.

Jelen esetben a vállalkozáscsoport tevékenységének differenciáltságának figyelembe vételével - például egészen biztos, hogy a Kötelezett is fog külföldi adattovábbítást végezni, mert közvetlenül napi kapcsolatban áll a harmadik országbeli tagokkal - tehető csak alappal olyan állítás, hogy életszerűtlen a Kötelezett magatartása, erről azonban a határozat nem tartalmaz tényállítást vagy utalást. A NAIH ugyanakkor helyesen emeli ki, hogy a BCR jóváhagyására vonatkozó eljárás a szabályzatra vonatozik, amely

DOI: 10.14750/ME.2019.022

elválik attól, hogy az egyes adattovábbítások jóváhagyását kellene kérni. Megjegyzem a magyar adatvédelmi jogban a külföldi adattovábbítás sosem volt hatósági engedélyhez vagy utólagos jóváhagyáshoz kötve, csupán[242] az adatvédelmi nyilvántartás egyik tartalmi eleme volt az adattovábbítási művelet megjelölése.

VII.4.7. Jóváhagyás vagy engedélyezés

A határozat szövegében elválik (6. oldal 7. sor) a jóváhagyási és az engedélyeztetési eljárás. Mi a helyes értelmezés, melyik az eljárás megfelelő terminológiája? Amint azt a VI. fejezet első pontjában is megfogalmazom, a jóváhagyás alapvetően egy utólagos megfelelőségi ellenőrzést jelent, míg a BCR esetében éppen egy előzetes ellenőrzés folyik a jóváhagyási eljárás során. A jogász-nyelvész munkája során gyakran kerül szembe hasonló szemantikai kihívással. Jelen esetben a GDPR magyar, angol, német és francia szövegváltozata is a jóváhagy, jóváhagyás kifejezéseket tartalmazza, feltételezem, a magyar jogalkotó ezért nem kívánta a szemantikailag helyes jelentéstartalmú „engedélyez" igét bevezetni a vonatkozó jogi környezetbe, noha helyeselhető lett volna. A NAIH állításából azonban az a közvetkeztetés is adódhatna, hogy az engedélyeztetés illetve az engedélyezés az első, a vezető hatóság és az érintett hatóságok előtti eljárás, míg a jóváhagyásra irányuló eljárás a nemzeti hatóságok előtti nemzeti eljárás. Ezt az értelmezést támogathatónak tartom. Az eljárások különbözőségét hangsúlyozó elnevezés-pár a fentebb felvetett szemantikai problémát is feloldhatná, hiszen az első eljárás valóban egy előzetes vizsgálat, míg a nemzeti eljárások egy már ellenőrzött – bár még alkalmazás előtt álló BCR-re vonatkozó – megfelelőségi vizsgálatot jelentenek. Ehhez azonban az egyértelműség érdekében mind a GDPR magyar nyelvi változatának, mind az Infotv. vonatkozó szakaszainak megfelelő újraszövegezésére volna szükség.

[242] Az első olvasásra jelentősnek tűnő tényező sok esetben nem alkalmazandó, mert az adatvédelmi nyilvántartásba való bejelentkezési kötelezettség egyrészt számos kivételt tartalmaz, másrészt a GDPR alkalmazása körében a hatóság által vezetett adatvédelmi nyilvántartás megszűnik.

DOI: 10.14750/ME.2019.022

VII.5. Az eset jelentősége

A határozat azon az alapon áll, hogy a BCR-ben exportáló állam a Kötelezett, és fennáll a lehetősége a külföldi adattovábbításnak, amely során a vállalkozáscsoportnál a megfelelő védelmi szint igazolása csak a BCR lehet, mivel az érvényes és alkalmazandó. A fentiekben számos ponton tettem kritikai megjegyzést az eljárás megindítására vonatkozóan, majd annak tételmondatai vonatkozásában.

Fontosabbak azonban azok a következtetések, amelyek elfogadása a BCR jogi környezetét gyakorlatiasabbá és kevésbé elrettentővé tennék. Mára okafogyott, de kerülendő lett volna kimondani azt, hogy BCR esetén a külföldi adattovábbítás kizárólag az Infotv. 8. § (1) bekezdés b) pontja lehet és a megfelelő védelmi szint kizárólag az Infotv. 8. § (2) bekezdés c) pontja szerint volt biztosítható. Szükséges volna az eljárás elnevezésére vonatkozó, szemantikai megfontolásokból is helyes meghatározást - az engedélyezést - bevezetni, különösen azért is, mert az Infotv. módosítása is az 34/A. Az adatkezelési engedélyezési eljárás címet tartalmazza, amely csak részben helyes, az engedélyezési fordulata. A helytelenség legfőbb oka az, hogy a cím félrevezető. Maga az adatkezelés nem engedélyköteles tevékenység, tehát a NAIH nem az adatkezelést magát engedélyezi, hanem azokat a magatartási kódexeket, ellenőrzési tevékenységeket, amely az adatkezeléseket az adott jogi személynél szabályozza. Továbbá nemcsak az adatkezeléseket, hanem - a BCR például különösen a külföldi adattovábbítást rendezi -, így szűkítő értelmezéssel a BCR jóváhagyása – engedélyezése – nem tartozna e körbe.

Azon túl, hogy az eset közigazgatási jogi szempontból kuriózum a 4.1. pontban megfogalmazott kritikai nézőpont szerint, az első is hazánk BCR-gyakorlatából. Épp emiatt bármilyen tendencia vagy jó gyakorlat megállapítása még nem lehetséges, azért sem, mert – nem állítom, hogy nincs – de kutató munkám során nem találkoztam hasonló külföldi döntéssel sem.

DOI: 10.14750/ME.2019.022

VIII. FEJEZET
TARTALMI ELEMZÉS

A BCR akkor éri el a célját, ha olyan rendelkezéseket tartalmaz, amelyek nem csak „papírtigrisek”[243] hanem valóban a megfelelő szintű adatvédelmi garanciákat biztosítják és kötelező erővel bírnak, mind a vállalkozáscsoport tagjai és munkavállalói tekintetében, mind az érintettek jogérvényesítése vonatkozásában. A BCR minimum tartalmi elemeit a GDPR 47. cikk (2) bekezdése tartalmazza, azonban a lista nem kimerítő, további támpontot a 29-es Adatvédelmi Munkacsoport magyarázó dokumentumai[244] biztosítanak. Ebben a fejezetben a WP154 rendszerét követem, amely egy minta-struktúrát vázol. Ezzel párhuzamosan vizsgálom a GDPR rendelkezését és a WP 153 iránymutatását. Ezekhez igazodva vizsgálom néhány vállalkozáscsoport BCR-jének közzétett szövegét azzal a céllal, hogy egyrészt az egyes rendelkezések gyakorlati példáit rögzítsem, másrészt hogy rámutassak akár a jogi, akár a gyakorlatban tapaszalt jó gyakorlatokra vagy éppen hiányosságokra.

Világszerte ismert multinacionális vállalkozáscsoportok nyilvános BCR rendelkezéseinek tartalmát vizsgálom, amely során kiemelt figyelmet fordítok arra, hogy a vizsgált szabályrendszerek hogyan felelnek meg a GDPR és a WP-k szabályainak és beilleszthetőek-e a magyar jogrendbe.

Az adatfeldolgozásra vonatkozó szerződésekhez is csatolni szükséges a megbízó adatkezelő BCR-jét, és már nem ritka az sem, hogy az adatfeldolgozó maga is adatfeldolgozói BCR-t alkalmaz. A GDPR hatályba lépése kapcsán felmerült az az alapkérdés is, hogy a már korábban jóváhagyott BCR-k érvényesek maradnak-e továbbra is.

---

[243] BAKER (2006) p. 15.

[244] WP108: ellenőrzőlista a BCR minimum tartalmi elemeihez; WP153: BCR minimum tartalmi elemei táblázatos formában; WP154 tartalmi elemek meghatározása és szerkezeti támpontok.

DOI: 10.14750/ME.2019.022

Egzakt kutatási eredményeket nem lehet e körben felmutatni, de az a véleményem, hogy ez esetben a jogi szabályt a már létező gyakorlat szerint alkották meg, így nem valószínű, hogy már érvényes BCR ne tenne eleget a GDPR szerinti fogalmi meghatározásnak. Az persze korántsem biztos, hogy tartalmában is megfelel a GDPR szabályainak egy, az Adatvédelmi Irányelvre és a tagállami jogszabályokra alapított BCR, azonban tartalmi módosításával korrigálható a nemmegfelelőség. Így nem látom logikus indokát annak, hogy miért ne maradhatna érvényes egy, még a GDPR hatályba lépése előtt jóváhagyott BCR. Megjegyzem azt is, hogy a BCR iránti megélénkült érdeklődés a GDPR hatályba lépése után élénkült meg igazán, amikor már látható volt a jogintézmény uniós szintű elismertsége. Hiszen korábban melyik vállalkozáscsoport alkalmazott volna olyan jogi eszközt, amelyet a tagállamok többségének jogrendszere nem ismer, a jogalanyok nem alkalmazzák, a jogalkalmazásnak nincs hatásköre a vonatkozó feladatokban eljárni?

Azt fontos kiemelni ugyanakkor, hogy az online elérhető BCR szövegek a vállalkozáscsoport adatvédelmi keretrendszerének töredékét mutatják csupán. A BCR jóváhagyásához a nemzeti hatóságok több dokumentum együttes érvényesülését veszik figyelembe. A BCR a törzse az adatvédelmi politikának, és társul hozzá számos egyéb dokumentum is, amelyekben kiegészítő, szektorális, vagy az üzleti titok és a kereskedelmileg érzékeny adatok vonatkozásában megalkotott adatvédelmi szabályokat rögzítettek, ezeket a nemzeti hatóságok megvizsgálják, de a nyilvánosságra hozataluk adott esetben kifejezetten tilos. Példa erre az adatbiztonsági intézkedések rendezése is, amelyek nyilvánosságra hozatala éppen hatékonyságukat ásná alá és tenné ki veszélynek a vállalkozáscsoport adat- és információvédelmi rendszerét.

DOI: 10.14750/ME.2019.022

VIII.1. A BCR szerkezete

A WP 154 bemutat egy minta-struktúrát, amely vázra felépíthető egy érvényes BCR törzsszövege az alábbiak szerint:

Bevezetés: kötelezettségvállalás a BCR rendelkezéseinek betartására, a BCR céljainak megfogalmazása, hivatkozás az irányadó jogi környezetre.

1. Hatály: szervi, területi és tárgyi hatály rögzítése, az adattovábbítási folyamatok általános leírása és azok célja.

2. Értelmező rendelkezések: alapvető általános fogalmak és különleges terminológiák azonosítása, magyarázata.

3. Célhoz kötöttség elvének megerősítése: a törvényes és meghatározott célok rögzítése, amely érdekében a személyes adatokat továbbítják.

4. Adatminőség és arányosság elvének megerősítése: kötelezettségvállalás az adatok pontos, naprakész minőségének fenntartására, valamint az adatminimalizálás és a szükségesség szempontjainak betartására.

5. Az adatkezelés jogalapja: az adatkezelés akkor jogszerű, ha az a GDPR 6. cikkében foglalt jogalapok legalább egyikének megfelel.

6. A személyes adatok különleges kategóriái kezelésének jogalapja: az adatkezelés akkor jogszerű, ha az a GDPR 6. cikkében foglalt jogalapok legalább egyikének megfelel és a 9. cikk szerinti különleges feltételeknek legalább egyikének is megfelel.

DOI: 10.14750/ME.2019.022

7. Átláthatóság és hozzáférhetőség: kötelezettségvállalás arra, hogy a BCR-t minden érintett megismerheti, továbbá annak leírása, hogy az érintett miként ismerheti meg az adatkezelő adatkezelési és adattovábbítási tevékenységét.

8. Érintetti jogok: kötelezettségvállalás arra nézve, hogy az érintettek gyakorolhatják a hozzáféréshez, helyesbítéshez, törléséhez és korlátozásához való jogukat, valamint ezek gyakorlása módjának leírása.

9. Automatizált döntéshozatal: kötelezettségvállalás arra nézve, hogy az érintettet jelentősen érintő kérdésekben – a kivételes eseteket leszámítva – nem születik döntés kizárólag a személyes adatok automatizált kezelése eredményeként.

10. Adatbiztonság és bizalmasság: kötelezettségvállalás arra nézve, hogy az adatkezelő bevezeti és fenntartja a szükséges technikai, technológiai és szervezési intézkedéseket az adatvédelmi incidensekkel szemben, azok megelőzése érdekében.

11. Kapcsolat olyan adatfeldolgozókkal, akik a vállalkozáscsoport tagjai: be kell mutatni, hogy a személyes adatok védelme miként valósul meg akkor, ha az adatkezelő adatfeldolgozót vesz igénybe, ha az adatfeldolgozó a vállalkozáscsoport tagja.

12. Korlátozások olyan adattovábbítások és olyan adatfeldolgozók igénybe vétele esetére, akik nem a vállalkozáscsoport tagjai: be kell mutatni, hogy a személyes adatok védelme miként valósul meg akkor, ha az adatkezelő olyan címzettnek továbbítja a személyes adatokat vagy olyan adatfeldolgozót vesz igénybe, aki nem a vállalkozáscsoport tagja.

13. Képzés: kötelezettségvállalás arra nézve, hogy az adatkezelő a munkavállalói részére képzést tart az adatvédelmi kötelezettségek betartásáról.

DOI: 10.14750/ME.2019.022

14. Audit program: kötelezettségvállalás arra nézve, hogy az adatkezelő rendszeresen ellenőrzi a BCR szabályainak betartását.

15. A megfelelés és annak felülvizsgálata: az adatvédelemért felelős személyi állomány létrehozása, a struktúra ismertetése, valamint kötelezettségvállalás arra nézve, hogy kijelölik azt a megfelelő, egy meghatározott személy mint vezető által irányított szervezi egységet, amely felügyeli az adatvédelmi szabályok betartását.

16. Cselekvési terv a nemzeti jog ellentétes rendelkezése esetén: kötelezettségvállalás és a feladatok meghatározása arra az esete, ha az egyik vállalkozáscsoporti tag nemzeti joga akként módosul, hogy annak betartása ellentétes lenne a BCR szabályaival.

17. Belső panaszkezelési mechanizmus: kötelezettségvállalás arra nézve, hogy bármely érintett panasza esetén rendelkezésre áll a vállalkozáscsoporton belül olyan személyzet és eljárás, amely a panasz elbírálására köteles.

18. Az érintett mint harmadik személy jogai: kifejezett nyilatkozat arra vonatkozóan, hogy az érintett mint harmadik személy jogosult hatósági vagy bírósági úton kikényszeríteni a BCR betartását, jogellenesség esetén pedig jogosult kárának megtérítésére.

19. Felelősség: kötelezettségvállalás arra nézve, hogy a vállalkozáscsoport kijelölt tagja felelősséget vállal a jogsértések orvoslásáért. Akkor mentesülhet, ha bizonyítja, hogy a vállalkozáscsoport tagja nem felelős a jogellenességért.

20. Kölcsönös támogatás és együttműködés a felügyeleti hatóságokkal: kötelezettségvállalás arra nézve, hogy a BCR helyes alkalmazása és a panaszkezelési eljárások során a vállalkozáscsoport tagjai egymást támogatják és betartják a tagállami adatvédelmi hatóságok ajánlásait.

DOI: 10.14750/ME.2019.022

21. A szabályok frissítése és aktualizálása: kötelezettségvállalás arra nézve, hogy a jogi környezet és a vállalkozáscsoport struktúrájának változása esetén a BCR szükséges módosítását bejelentik a felügyelő hatóságok felé.

22. A BCR és a nemzeti jog viszonya: annak bemutatása, hogy a BCR vagy a nemzeti illetve uniós jog alkalmazandó-e az adott helyzetben.

23. Záró rendelkezések: a BCR hatályba lépésének időpontja és az átmeneti időre vonatkozó rendelkezések.

VIII.2. A BCR bevezető része

A bevezető részben világos kötelezettségvállalást kell tenni arra vonatkozóan, hogy a vállalkozáscsoport valamennyi tagja és valamennyi munkavállalója elfogadja, tiszteletben tartja és betartja a BCR rendelkezéseit.

Az egyik BCR-ben[245] az 1. pont szerint a „(cégnév) vállalatok a következőket vállalják" kifejezés utal arra, hogy a vállalkozáscsoport tagjai a BCR-ben foglaltakat magukra nézve kötelezőnek ismerik el. A záró rendelkezések között ugyancsak megerősítik, hogy a BCR rendelkezései a cég „felelősségre vonhatóságának részét képezik."

Egy másik[246] akként biztosítja a megfelelés kötelezettségét, hogy deklarálja, hogy adatkezelésének „ […] ezen alapvető követelményrendszere […]" azért készült, hogy a(z) (cégnév) vállalat és minden leányvállalata, fióktelepe, telephelye „ennek megfelelően járjon el […]", továbbá „minden (cégnév) jogalany kötve van ezen szabályok betartásához". A BCR-t kötelezően végrehajtandó magatartások egységesen alkalmazandó magánélet-védelmi szabályok a vállalkozáscsoporton belüli iránymutatásának nevezi, amely

[245] http://www8.hp.com/hu/hu/binding-corporate-rules.html
[246] Mivel a BCR dokumentum angol nyelvű hivatalos verzióját vizsgálom, jelen fejezetben saját fordításban interpretálom a rendelkezéseit.

DOI: 10.14750/ME.2019.022

megszegése vagy teljesítésének elmaradása valamilyen negatív jogkövetkezményt, például a munkaviszony megszüntetését vagy más szankciót vonhat maga után.

A legegyértelműbb megfogalmazás[247]:„… csoport valamennyi tagja, az alkalmazottak és az alkalmi munkaerő egyaránt köteles tiszteletben tartani a BCR-t…”.

A bevezetésben kell rögzíteni a BCR elsődleges célját, azaz a tényt, hogy a BCR arra szolgál, hogy a vállalkozáscsoporton belüli adatkezelési tevékenységhez és adattovábbításokhoz biztosítsa a megfelelő védelmi szintet.

Az egyik[248] BCR így fogalmaz: „A BCR célja egységes, megfelelő és globális adat- és magánszféra standardok alkalmazása…”, egy másikban[249] ez olvasható: „ A BCR segít abban, hogy […] eleget tegyünk az Európai Unió és az Európai Gazdasági Térség adatvédelmi szabványainak.”

A bevezetésben hivatkozni kell az alapul fekvő joganyagra is. Ezt az egyik BCR az alábbi szöveggel teljesíti: „figyelemmel a mindenkor hatályos adatvédelmi szabályokra, értve ezalatt különösen, de nem kizárólagosan az EU által alkotott adatvédelmi szabályokat”. Egy másik, igaz módosításra szoruló BCR már pontosan megjelöli az Adatvédelmi Irányelvet olyan jogszabályként, amelyre tekintettel a BCR szabályi értelmezendők és alkalmazandók.

A helyes megoldás itt a GDPR-ra hivatkozás, illetve tekintettel arra, hogy a tagállamok számos a GDPR szabályait részletező, szigorító vagy végrehajtási jellegű jogot alkothatnak, érdemes volna ebben a részben utalni rá vagy listázni azon államokat, de legalábbis a szektorális joganyagot megjelölni

[247] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf
[248] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf
[249] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf

DOI: 10.14750/ME.2019.022

legalább általánosan, amelyek adatvédelmi rendelkezései irányadók a GDPR mellett. Ide tartozhatnak például egy gyógyszercég esetén az egészségügyi adatokra vonatkozó adatkezelői többletkötelezettségek.

VIII.3. A BCR hatálya

A BCR hatályára vonatkozó rendelkezések között rögzíteni kell különösen azt, hogy a szabályokat valamennyi vállalkozáscsoporton belüli adattovábbításra és adatkezelésre alkalmazni kell, vagyis meg kell határozni a BCR tárgyi hatályát. Itt különbséget lehet tenni aközött, hogy a BCR csak a harmadik országokba irányuló adattovábbítások, vagy a vállalkozáscsoport valamennyi adattovábbítási és adatkezelési tevékenységére irányadó-e. Jelentősége ez előbbi esetben van a szabályok betartásának, ugyanakkor célszerű kiterjeszteni valamennyi adattovábbításra, mert úgy egységes, általános, ezért rutinná váló adatvédelmi intézkedések épülhetnek be a mindennapi működésbe.

Ezen túl meg kell határozni további szűkítő vagy pontosító szabályokat, például hogy a BCR alkalmazandó-e a papír alapú vagy csak az automatizált elektronikus továbbításra, illetve hogy mely adatkategóriák vagy érintetti csoportok mely adatkategóriái tartoznak hatálya alá.

Az egyik[250] vizsgált BCR ekként rendelkezik: „BCR rendelkezései érvényesek valamennyi, a (cégnév) vállalatcsoporthoz tartozó társaság adatkezelésére". Egy másik[251] szövegében pedig „jelen BCR érvényessége az egész (cégnév) csoportra kiterjed". Ugyan ez a BCR egy másik pontjában a „(cégnév) csoport fő egységeinek jegyzéke" elnevezésű linket illeszt be, amely a honlapján a vállalkozáscsoport tagjainak székhelyét mutatja be.

[250] http://www.evosoft.hu/kotelezo-ereju-vallalati-szabalyok-binding-corporate-rules
[251] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf

DOI: 10.14750/ME.2019.022

A tárgyi hatály körében így rendelkezik a BCR: „A dokumentum érvényessége kiterjed egyebek között az alábbi műveletekre” és ezt követően az adatkezelő ügycsoportokat sorol fel, például ügyféltámogatás és adatbányászat, big data elemzés.

Egy másik BCR[252] a tárgyi hatály vonatkozásában az „európai alkalmazottai és ügyfelei személyes adatait” jelöli ki, adatfeldolgozóként pedig olyan harmadik országbeli „szolgáltatók” és „beszállítók” tartoznak a BCR alkalmazási körébe, amelyek „a nemzetközi (cégnév) csoport más vállalatai”, és „támogatják” a kereskedelmi szolgáltatásaikat az ügyféltámogatás, marketing és az alkalmazottak juttatásai vonatkozásában.

Be kell mutatni az adattovábbítások általános leírását és az adatkezelés célját. E körben rögzíteni kell a továbbított adatok természetét, azaz az adatok kategóriáit, adott esetben a személyes adatok különleges kategóriáit is. Az általános leíráson túl a BCR rendelkezéseiben be kell mutatni különösen az adattovábbítás természetét, célját valamint az adatkezelők és az adatfeldolgozók rendszerét A bemutatás azért szükséges, hogy a jóváhagyó hatóságok értékelni tudják a folyamat megfelelőségét. Azonban az üzleti titok védelme és más stratégiai okokból ezen információk közzététele a vállalkozáscsoport stratégiája, üzleti titkai körébe tartozhat, viszont titokban tartásuk az átláthatóság érvényesülését és az adatalany jogérvényesítését akadályozná. Így azt a szükséges részletességet kell itt elérni, amely már elegendő a jóváhagyáshoz és a transzparencia alapelv érvényesüléséhez, ugyanakkor nem okoz gazdasági hátrányt a vállalkozáscsoportnak. Ezt támasztja alá a WP 153. 6.2. pontja is, amely szerint nem szükséges rögzíteni a BCR-ben az Európai Unión belüli küldő és a harmadik országbeli fogadó tagok listáját.

[252] http://www8.hp.com/hu/hu/binding-corporate-rules.html

DOI: 10.14750/ME.2019.022

A célok tekintetében az egyik[253] BCR számos példát rögzít: ilyenek a vásárlói kérések teljesítésének elősegítése, fogyasztói panaszok rendezése, online és offline ajánlatokról szóló tájékoztatás, a fizetési kötelezettségek nem teljesítése esetére szóló beszedés, a csalás és más büntetendő cselekmények elleni védelem és felderítés.

Az egyik[254] vizsgált BCR-t adatfeldolgozó hozta létre, amelyet ekként deklarált: „Ügyfeleink meghatározzák az adatok feldolgozásának okát és módját, mi pedig elvégezzük a megbízásukból a feldolgozást. Annak biztosítására, hogy Ügyfeleink megbízható partnerei legyünk, saját BCR-t fogadtunk el…".

A fenti elemek lefedik a GDPR 47. cikk (2) bekezdés a) pontja és b) pontja szerinti kötelező minimum tartalmi elemek körét. A GDPR részletező jellegű szabályából arra következtethetnénk, hogy az érintett valóban megismeri az adatkezelés részleteit, azonban szigorúan értelmezve egyetlen vizsgált BCR sem tesz maradéktalanul eleget a fenti szabályoknak, tekintettel arra, hogy a lehető legáltalánosabban fogalmazzák meg az adatkezelésekre vonatkozó információkat.

VIII.4. Alapfogalmak

Értelmező rendelkezésekként szükséges rögzíteni a BCR alkalmazása körében értelmezendő alapvető olyan fogalmakat, mint például a személyes adat, a személyes adat különleges kategóriája, az adatalany, az adatkezelő, az adatfeldolgozó, az adatkezelés, a harmadik szermély, a hatóság fogalmát.

[253] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf
[254] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf

DOI: 10.14750/ME.2019.022

A legtöbb adatvédelmi szabályzat legterjedelmesebb részét adják a fogalommagyarázatok, amelyek jellemzően szóról szóra veszik át a jogforrás fogalmait. Ennek tulajdonképpen így nincs értelme, hiszen az értő olvasónak külön jogszabályi kivonat nélkül is ismertek a terminus technicusok, a laikus érintett számára pedig egy magyarázó jellegű, rövid és lényegre törő ismertetés lenne szükséges, illetve a forrást megjelölő jogszabálykivonat, amellyel pedig sajnos ritkán találkozik az olvasó.

Az egyik[255] BCR hiánypótló módon meghatározza az adattovábbítás fogalmát: adattovábbításnak minősül a személyes adat hálózaton keresztül történő másolása, áthelyezése vagy mással történő megosztása, valamint a külső és a fogadó fél természetétől függetlenül egy küldő féltől egy fogadó fél részére a személyes adat hálózaton keresztül történő másolása, áthelyezése vagy megosztása, akkor ha mindez azzal a céllal történik, hogy a fogadó fél az adatokat kezelje. A leírás helyesen azonosítja az adattovábbítási tevékenységeket, az adattovábbításban részt vevő feleket és a művelet célját is.

A vizsgált BCR-ek közül kettő[256] tartalmazott csupán alapfogalmakat magyarázó részt. Ebben a körben, összhangban a WP 154 2. részében foglaltakkal, hivatkozni kell arra, hogy a fogalmakat a vonatkozó jogi környezetben bevett értelemzésükkel azonosan, a vonatkozó jogi környezettel összhangban kell értelmezni.

Az alapfogalmak mellett indokolt azonban az olyan terminus technicusok magyarázata, amelyek az adott adatkezelő esetében eltérnek a köznapi jelentéstől vagy külön részletezést és figyelemfelhívást igényelnek. Ebbe a körben sorolja a WP 154 például az adatexporter, a tevékenységi

[255] https://www.sanofi.com/media/Project/One-Sanofi-Web/sanofi-com/common/docs/download-center/Binding_Corporate_Rules_List_of_Sanofi_affiliates_having_signed_the_BCR_Janvier_2017.pdf

[256] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf https://www.sanofi.com/media/Project/One-Sanofi-Web/sanofi-com/common/docs/download-center/Binding_Corporate_Rules_List_of_Sanofi_affiliates_having_signed_the_BCR_Janvier_2017.pdf

DOI: 10.14750/ME.2019.022

központ és a felelősséget vállaló tag kifejezéseket, a vizsgált BCR-ek esetén ilyen az Ügyfél vagy a Global Privacy Steering Committee fogalma. A hétköznapitól eltérő jelentéstartalmú vagy idegen kifejezéseket, mint például az adatvédelmi incidens, szintén ebben a részben kell(ene) bemutatni.

VIII.5. Célhoz kötöttség és más elvek

A BCR-ben rögzíteni szükséges az adatkezelés és az adattovábbítás célját, azaz meg kell erősíteni az egyedi és jogszerű célt, a célhoz kötöttség alapelvének megtartását valamint a személyes adatok különleges kategóriának kezelése során biztosítandó többlet garanciákat. Ebben a részben a GDPR 47. cikk (2) bekezdés d) pontjának első fordulata szerinti tartalmi elemek beillesztésének kötelezettségét lehet megtenni.

Ugyanebben a részben kell összefoglalni az alkalmazandó egyéb, bár nem kevésbé fontos elveket, mint például az adattakarékosság, korlátozott tárolási időtartamok, a beépített és alapértelmezett adatvédelem, az adatminőség elvét, azok alapvető tartalmi magyarázatával együtt.

A vizsgált BCR-ek – egy kivételével – rögzítették, hogy tiszteletben tartják az adatvédelmi alapelveket, és egy-egy tartalommagyarázó mondatban bemutatták az alapelvek esszenciáját.

VIII.6. Az adatkezelés jogalapja

Az egyik legfontosabb attribútuma minden adatkezelésnek, hogy mi a jogalapja. Az ezidáig a legjelentősebb és a leggyakrabban alkalmazott jogalapot, az érintett hozzájárulását több, gyakorlatias szemléletű jogalap beiktatásával a jogalkotó mintha visszaszorítani kívánta volna.[257]

[257] A GDPR a jogalkotás során kifejezett nyomásra mégis megtartotta az információs önrendelkezés főszabályát, tehát az érintett hozzájárulása mint alapeset és kiindulási pont.

DOI: 10.14750/ME.2019.022

A GDPR 6. cikke és 9. cikke valamint az V. fejezetben szabályozott harmadik országokba illetve nemzetközi szervezet részére végzett adattovábbítások esetére az uniós jogalkotó újabb jogalapokat hozott létre, amelyek az érintett hozzájárulásán túl más megfontolásokból is jogszerűvé tesz bizonyos adatkezeléseket. A vizsgált BCR-k jellemzően a GDRP 6. és 9. cikkét ismétlik meg, mintegy általános deklarációként, nem konkretizálva az egyes adatkezelésekre vonatkozó jogalapokat. Elfogadva azt, hogy egy-egy adatkezelési tevékenység akár több jogalapon is állhat, és bizonyos helyzetekben az adatkezelés jogalapja meg is változhat,[258] álláspontom szerint az alapesetet mégis be kellene azonosítani, a megfelelő tájékoztatás nem merülhet ki a lehetséges jogalapok felsorolásával.

VIII.7. Átláthatóság és hozzáférhetőség

A WP 153 1.7. pontja szerint könnyű hozzáférést kell biztosítani a BCR-hez. A WP 154 minta struktúra 7. pontja ugyancsak azt javasolja, hogy kötelezettséget kell vállalni arra nézve, hogy a BCR-t minden érintett számára megismerhetővé teszik, és abban minden érintett számára felvilágosítást nyújtanak arról, hogy hogyan kaphatnak további információt az adatkezelésekről. Az átláthatóság mindvégig az adatvédelem középpontjában állt, párhuzamosan az érintett hozzáférési, megismerési jogának azonos hatású, az adatkezelő oldalán jelentkező kötelezettségként. Ezért a GDPR 47. cikk (2) bekezdés g) pontja szerint a BCR kötelező tartalmi eleme az információ halmaz, amely arra vonatkozik, hogy az érintett hogyan ismerheti meg a BCR-t és a vállalkozás teljes adatvédelmi politikáját.

[258] Például a 6. cikk (1) bekezdés b) pont szerinti szerződéses jogalap a szerződésszegés esetén egyes álláspontok szerint akár az f) pont szerinti jogos érdek körébe kerülhet át. Ennek elemzéséről lásd: BÁRTFAI (2018)

DOI: 10.14750/ME.2019.022

Az egyik[259] vizsgált BCR weboldalán az adatkezelő biztosít panaszkezelő felületet, ahol azonnali kapcsolatfelvétel lehetséges az adatvédelemért felelős személyekkel. Egy másik[260] BCR pedig explicit módon deklarálja, hogy minden munkavállalója számára bármikor biztosít egy példányt a BCR teljes szövegéből, továbbá azt nemzeti adatvédelmi hatóság is bármikor megismerheti.

(A vizsgált BCR-k törzsszövege korlátozásmentesen elérhető online, azonban a NAIH vagy az Európai Bizottság oldalán található nyilvántartás szerinti vállalkozáscsoportok nem mindegyike tette közzé online BCR-jét, vagy azok nem könnyen elérhetők.)

VIII.8. Az érintett jogai

A WP 154 minta-struktúra szerint és a GDPR 47. cikk (1) bekezdés b) pontja és a (2) bekezdésnek e) pontja szerint rögzíteni kell az érintett jogait és a jogok gyakorlásának módját is be kell mutatni. A GDPR az alábbi jogokat nevesíti különösen e körben:

- a kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntések alóli mentesülés jogát,

- az érintett hatékony bírósági illetve hatósági jogorvoslathoz való jogát, beleértve a panasz benyújtására vonatkozó jogát is, valamint

- a BCR megsértése esetén a kártérítéshez való jogát, adott esetben.[261]

[259] http://www8.hp.com/hu/hu/binding-corporate-rules.html
[260] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf
[261] Az „adott esetben" kifejezés jelentése egyelőre még nem ismert ebben a kontextusban, mindenesetre elképzelhető eszerint olyan helyzet, amikor a BCR megsértése esetén a kártérítéshez való jog nem illeti meg az érintettet. Ha ez a kimentés lehetőségére irányul, akkor a szövegezés hibás, mert a kártérítéshez való jog akkor is megilleti az érinettet.

DOI: 10.14750/ME.2019.022

A fentieken túl az érintetti jogok teljes GDRP szerinti kimerítő listáját érdemes feltüntetni, hiszen az adatkezelő a 13. cikk (2) bekezdés b) pontja valamint 14. cikk (2) bekezdés c) pontja szerint is köteles rendelkezésre bocsátani az információt arról, hogy az érintett kérelmezheti a személyes adataihoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat[262] a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról.

VIII.9. A BCR kötelező erejéről

A GDPR 47 cikk (2) bekezdés c) pontja értelmében ez a rész deklarálja a BCR „belső és külső tekintetben jogilag kötelező jellegét". A BCR kötelező erejét ezen két szempontból vizsgálom a továbbiakban.

VIII.9.1. Megfelelési kötelezettség – befelé irányuló kötelező erő

A BCR kötelező jellegének egyik dimenziója a befelé irányuló kötelező erő, azaz a megfelelési kötelezettség. Mindazon rendelkezések, amelyek azt hivatottak bizonyítani és biztosítani, hogy a vállalkozáscsoport tagjai és a munkavállalók betartják a BCR szabályait.

A WP 153. 1.2. pontja értelmében ennek részletezését a BCR-ben nem kell rögzíteni, elegendő azt a jóváhagyási eljárás során bemutatni.

A vállalkozáscsoporton belül a BCR rendelkezéseinek kötelező jellegét akként lehet rögzíteni, hogy egy vállalkozáscsoporton belüli (intra group) megállapodást hoznak létre, egyoldalú kötelezettségvállalásokat tesznek a tagok és az ellenőrző vállalkozás, vagy a vállalkozáscsoport általános üzletpolitikájába foglalják.

[262] Amennyiben az adatkezelés a GDRP 6. cikk (1) bekezdésének e) vagy f) pontján alapul.

DOI: 10.14750/ME.2019.022

Az egyes munkavállalók irányában egyéni megállapodások útján a munkaszerződés egyik pontjaként vagy kollektív szerződés részeként hozható létre a kötelező jellege.

A hatóságok vizsgálatuk során a fentiek részletes ismertetését és magyarázatát várják el a kérelmező vállalkozáscsoporttól. Be kell továbbá mutatni azt is, hogy a vállalkozáscsoporttal szerződő vállalkozásokra nézve mennyiben kötelező és milyen módon érvényesíthető kötelező jellege. Példa erre az egyik[263] BCR-ben: „Az itt foglalt szabályok a további külső adatfeldolgozásról szóló megállapodások esetén is érvényesek."

VIII.9.2. Érintetti jogérvényesítés – kifelé irányuló kötelező erő

A kikényszeríthetőség – külső vagy kifelé irányuló kötelező erő – azt jelenti, hogy az érintett, aki a BCR hatálya alá tartozik, jogosult bírósági vagy hatósági úton a vállalkozáscsoportot arra szorítani, hogy a BCR-ben foglaltaknak megfelelően járjon el, valamint jogsérelem esetén az érintett jogosult bírói illetve hatósági jogérvényesítésre, amely eredményeként kártérítést és sérelemdíjat is követelhet.

A GDPR 47. cikk (2) bekezdés e) pontja szerint a panasz benyújtására vonatkozó jog, továbbá a jogorvoslathoz való jog valamint adott esetben a BCR megsértése esetén a kártérítéshez való jog deklarálása és a jogérvényesítés módjának leírása a BCR kötelező tartalmi eleme.

A kifelé irányuló kötelező erő, azaz az érintetti jogérvényesítés szempontjából a hatóság vizsgálja, hogy az érintett számára biztosított-e az a joga, hogy az adattovábbítás kiinduló pontja szerinti vállalkozás, vagy az Európai Unión belüli központ vagy az Európai Unión belül működő, az adatvédelmi kötelezettségekért felelős vállalkozáscsoporti tag működése szerinti

[263] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf

DOI: 10.14750/ME.2019.022

joghatóság alatt nyújtható-e be panasz a vállalkozáscsoport vélt vagy valós jogellenessége esetén. Ezért a vállalkozásnak be kell mutatnia, hogy az érintettnek milyen tényleges lépéseket kell tennie annak érdekében, hogy jogsérelem esetén a kára megtérüljön.

A hatóság vizsgálja azt is, hogy a kérelmező bemutatta-e a panaszkezelés vállalkozácsoporton belüli módját, mechanizmusait, megnevezte-e a panaszkezeléssel foglalkozó szervezeti egységét, ahogyan azt kötelező tartalmi elemként a GDPR 47. cikk (2) bekezdés i) pontja előírja. Példaként hozza a WP108 5.16. pontja azt az esetet, ha a vállalkozáscsoport központja és a vezető hatóság Belgiumban van, de az olasz tag sértette meg a BCR előírását, úgy az érintett számára világossá kell tenni, hogy igényét választása szerint az olasz taggal és/vagy a belga taggal szemben is érvényesítheti.

A tartalmi szempontból vizsgált egyik BCR[264] harmadik egyben utolsó pontja rendezi a panasz benyújtásának elektronikus útra terelését egy letölthető űrlap kitöltésével. A hivatkozott pontban a BCR arról nem szól, hogy tagállami vállalkozás esetén mi a teendő, csak a harmadik országbeli jogérvényesítés egy módját adja meg. Szűkszavúan a vállalkozás Adatvédelmi Irodájához irányítja a panaszost. Egy másik BCR-ben[265] a panaszkezelési eljárás struktúrája árnyaltabb. Az érintett első lépésként bejelentéssel élhet az adatkezelő felé elektronikus úton vagy a „Segítség” fül alatt egyéni belépési lehetőséggel veheti fel az Ügyféltámogatással foglalkozó munkatársakkal a kapcsolatot. Ők jogosultak vizsgálatot lefolytatni. Amennyiben a panaszt nem bírálták el vagy nem kielégítő módon sikerült megoldani, a bejelentést az érintett kérésére felterjesztik a jogi osztály vagy a magánéletvédelmi csoport elé, ahol az elbírálásnak „ésszerű időn belül” kell végbe mennie.

[264] http://www8.hp.com/hu/hu/binding-corporate-rules.html
[265] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf

DOI: 10.14750/ME.2019.022

Megítélésem szerint ez az általánosnál rövidebb határidőt jelent, hiszen például az online kereskedelemben a tranzakciók és az információcsere felgyorsul, így az érintett panaszának vizsgálatát is hamarabb kell megkezdni és lefolytatni. A hatósági, bírói jogérvényesítéstől a továbbiakban sincs elzárva az érintett.

Az adatalany szempontjából a leggyorsabb módja a sérelem orvoslásának, ha a jogsértő vállalkozáshoz fordul panaszával, mely során azonban nyelvi, technikai, időbeli akadályokba ütközhet, ám ha a vállalkozás nyitott a jogsérelem orvoslására, mégis ez lehet a leghatékonyabb módszer. A bírói út költséges, időigényes lehet, azonban valós jogsérelem esetén biztos kompenzációt ígér, noha a jogellenes adatkezelés okozta bizonyos károk helyrehozhatatlansága és visszafordíthatatlansága okán ez esetenként elmarad.

A GDPR 47. cikk (2) bekezdés f) pontja kötelező tartalmi elemként írja elő azt, hogy a BCR-ben rendelkezni kell valamely tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó felelősségének elismeréséről - helyesen a felelősség telepítéséről, amely alól kimentés is lehetséges - abban az esetben, ha a BCR-t a vállalkozáscsoportnak az Európai Unióban tevékenységi hellyel nem rendelkező bármely tagja megsérti. A WP 204 4.6.2.2. pontja az adatfeldolgozói BCR vonatkozásában részletezi az előírást akként, hogy az adatfeldolgozó BCR-jében deklarálni kell, hogy az adatkezelő - és nem az érintett közvetlenül[266] - jogosult az adatfeldolgozó vállalkozáscsoport bármely tagjával szemben a jogellenesség következtében igényt érvényesíteni csak úgy, mint az adatfeldolgozó bármely al-adatfeldolgozójával szemben.

[266] A felelősségi lánc az érintett és az adatkezelő, majd az adatkezelő és az adatfeldolgozó között jön létre.

DOI: 10.14750/ME.2019.022

A vállalkozáscsoport az Európai Unióban székhellyel rendelkező, illetve a központi ügyvitel helye szerinti, az Európai Unió tagállamában működő tagja vállalja, hogy felelősséggel tartozik a harmadik országban elkövetett jogsértéseket követően az Európai Unión kívüli vállalkozáscsoporti tag magatartásáért akként, hogy kártérítés és sérelemdíj megfizetését illetve egyéb jogorvoslat végrehajtását vállalja. Tehát az összes unión kívüli tag tekintetében közvetlen felelősséget vállal egy, az Európai Unió tagállamában működő vállalkozás. Esetről esetre is történhet a felelős tag kiválasztása, azonban ez az adatalany jogérvényesítése szempontjából nem lehet kedvezőtlen. Itt utalok arra, hogy a mellékletek között benyújtandó az a dokumentum is, amelyben a felelősséget vállaló tag vagyoni viszonyait kell bemutatni. A WP 153. 1.6. pontja értelmében a BCR-ben ugyan nem, de a jóváhagyási eljárásban „meg kell erősíteni”, hogy a felelősséget vállaló tagnak van vagyona, amelyből fedezni tud egy esetleges kártérítésre marasztalást. Arra vonatkozóan azonban nincs iránymutatás, hogy a hatóságok a kijelölést érdemben vizsgálhatják-e, kérhetik-e például másik tag kijelölését. Az üzleti titkok védelmével összeegyeztethető részletesebb beszámoló indokolatlanul sok, míg a nyilatkozati forma túl csekély garancia volna a megerősítéshez, azonban az ismertetés elfogadható formájáról sem a GDPR, sem a vonatkozó WP-k nem rendelkeznek. Célravezetőnek találom, ha a vállalkozás előző évi mérleg alapján, a bírság mértékének megállapítása analógiájára, történne ezen feltétel megítélése. Ezzel kapcsolatosan pedig már most jelzem, hogy egzakt szabályozás és jó gyakorlat hiányában ez a pont lehet az érintetti jogérvényesítés valós korlátja.[267]

Ezen túl deklarálni kell azt is, hogy az eljárás során a bizonyítási teher az adattovábbítás kiinduló pontja szerinti vállalkozáson, vagy az Európai Unión belüli központon vagy az Európai Unión belül működő, az adatvédelmi kötelezettségekért felelős vállalkozáscsoporti tagon van.

[267] Hiszen ha a kijelölt tagnak nincs elegendő vagyona a kártérítés vagy sérelemdíj megfizetésére, úgy az érintett jogsérelme elvben reparáció nélkül maradhat.

DOI: 10.14750/ME.2019.022

Kimentéses a bizonyítás, azaz a felelősséget vállaló tag csak akkor mentesülhet - részben vagy egészben - a felelőség alól, ha bizonyítja, hogy a vállalkozáscsoport tagja nem felelős a kár előidézésében.

Ez a formula a magyar polgári jogi felelősségi alakzatoktól, mind a szerződésszegéssel okozott károk megtérítése, mint a szerződésen kívüli károkozásra vonatkozó felelősségi alakzatoktól eltér, az Infotv - ben foglalt felelősségi alakzathoz[268] pedig egyáltalán nem igazodik, bár ez utóbbi a GDPR közvetlen hatálya és közvetlen alkalmazhatósága miatt már nem is alkalmazandó. Tekintettel arra, hogy az adatkezelési tevékenységek az esetek többségében szerződésen - vagy az érintett hozzájárulásán - alapulnak, a BCR esetében pedig bizonyosan indokolt „szerződés" létét megállapítani - indokolt volna szigorúbb, akár a szerződésszegéssel okozott károkért való felelősségi szabály[269] alkalmazása. Még akkor is indokoltnak látom ezen felelősségi alakzat alkalmazását, ha maga az alapul fekvő szerződés elsődleges közvetlen tárgya nem is az adatkezelési tevékenységre irányul.

A GDPR-beli rendelkezés ezekben a helyzetekben az érintett számára hátrányos, mert az adatkezelő számára könnyebb kimentési módot deklarál, mint ha az érintett tisztán polgári jogi jogviszonya alapján érvényesítené igényét. Azokban az esetekben, amikor nem hozzájárulás, és nem szerződés a jogalapja az adatkezelésnek, mert például az adatkezelő jogos érdeke vagy jogi kötelezettsége alapozza meg a jogszerű adatkezelést, ott elképzelhető a GDPR-beli kimentés megfelelősége, amely hasonlít a magyar polgári jogi szerződésen kívüli – deliktuális – károkozás alóli kimentésre.[270]

[268] Infotv. 23. § szerint mentesül az adatkezelő, ha bizonyítja, hogy az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

[269] Ptk. 6:142 második fordulata: Mentesül a felelősség alól, ha bizonyítja, hogy a szerződésszegést ellenőrzési körén kívül eső, a szerződéskötés időpontjában előre nem látható körülmény okozta, és nem volt elvárható, hogy a körülményt elkerülje vagy a kárt elhárítsa.

[270] Ptk. 6:518 második fordulata: Mentesül a felelősség alól a károkozó, ha bizonyítja, hogy magatartása nem volt felróható.

DOI: 10.14750/ME.2019.022

A felróható magatartás tanúsítása, azaz ha valamiért felelős az adatkezelő, vagy más szóval „*nem járt el az adott helyzetben elvárható kellő gondossággal*”[271], alapozza csak meg a kárfelelősséget.

Tehát míg a szerződésszegéssel okozott kárért való felelősség szigorúbb viszonyai között „a vétkesség (szubjektív felróhatóság) bizonyítási terhe vélelmezett, addig a deliktuális szubjektív felelősség terén a vétkesség nem vélelmezett, s bizonyítási terhét a károsult viseli”.[272] Megfordul a bizonyítási teher, a vétkesség hiányát a károkozó köteles bizonyítani szerződésszegés esetén, míg a deliktuális kárfelelősség esetén a károsultnak kell bizonyítania. A GDPR a BCR megszegése esetén is egy kevésbé szigorú felelősségi alakzatot állít fel – indokolatlanul -, mint amelyet a hazai polgári jog szerint érvényesíthetne az érintett, amely egy multinacionális vállalkozáscsoport esetében ismét felveti a forum shopping kérdését: vagyis telepítse-e úgy adatkezelési központját vagy a felelősséget viselő tag kijelölését az adatkezelő vállalkozáscsoport, hogy az adott állam polgári jogi jogviszonyai között a GDPR szerinti enyhébb felelősségi alakzat szerinti kimentés alkalmazható legyen. Megjegyzem érdekes helyzet, hogy a lex specialis, itt a GDPR, enyhébb felelősségi szabályt alkalmaz, mint a lex generális Ptk. Az GDPR szerinti bírósági igényérvényesítésre még bizonyosan nincs kialakult jó gyakorlat, a BCR alapján pedig alapvetően kétséges az érintett jogérvényesítési lehetősége – azaz hivatkozhat-e az érintett a BCR önként vállalt szabályára vagy helyette az alapul szolgáló GDPR rendelkezést - ha egyáltalán van annak megfelelő - lehet csak a vélt vagy valós jogsértés megítélésekor figyelembe venni. Mindenesetre az érintetti jogérvényesítés kívül esik e disszertáció tartalmi keretein, de a fenti sorokban foglalt kétségek egy széles körű jövőbeni elemzés tárgyát képezhetik.

[271] KEMENES (2017) p. 1.
[272] SZALMA (2015) p. 345.

DOI: 10.14750/ME.2019.022

Az egyik vizsgált BCR arról rendelkezik, hogy bírósági eljárás során az „európai HP vállalat alperesként" vesz részt a perben, „terheli annak bizonyítása, hogy nem történt szabálysértés" és „kötelezett […] a megítélt kártérítési összeget megfizetni." Egy másik BCR a vállalkozáscsoport luxemburgi korlátolt felelősségű társaságát jelöli meg a felelősséget vállaló cégcsoporti tagként.

VIII.10. Automatizált döntéshozatal

A GDPR 47. cikk (2) bekezdés e) pontjának második fordulata előírja, hogy az érintetti jogok körében rendelkezni kell az automatizált adatkezelésen alapuló döntések és a profilalkotás alóli mentesülés jogáról.

Főszabályként rögzítendő, hogy az érintettet jelentősen érintő kérdésekben nem születik döntés kizárólag a személyes adatok automatizált kezelése eredményeként. Kivétel lehet ez alól egy olyan szerződés előkészítése illetve teljesítése, amelyet az érintett kezdeményezett vagy ha az érintett jogos érdekének biztosítására megfelelő biztosítékok álltak fenn.

Az egyik[273] vizsgált BCR kifejezetten rögzíti, hogy a felhasználó jogos érdekét automatizált döntéshozatal esetén cégénél egy fogyasztóvédelmi képviselő látja el, aki manuálisan is modellezi a döntést és lehetőséget biztosít a felhasználó számára álláspontja kifejtésére.

[273] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf

DOI: 10.14750/ME.2019.022

VIII.11. Adatbiztonsági intézkedések, audit, személyzet

A BCR-ben kötelezettséget kell vállalni arra, hogy adatkezelő bevezeti és fenntartja a szükséges technikai, technológiai és szervezési intézkedéseket az adatvédelmi incidensek bekövetkezésének megelőzése és kezelése érdekében.[274] Az adatbiztonsági intézkedések elsősorban az adatokat fizikai valójukban védik, de fontos az is, hogy az információs magánszférát, az adatalanyokat is védjék ezek az intézkedések, maga a technológia gátolja meg a visszaéléseket, jogsértéseket.[275]

A BCR-ben számot kell adni a meglévő és alkalmazott adatvédelmi mechanizmusokról, képzett személyzet alkalmazásáról (GDPR 47. cikk (2) bekezdés h) pont), a felelős személyzet számára kötelező képzésről (GDPR 47. cikk (2) bekezdés n) pont), valamint a jelenlegi belső panaszkezelési módszerekről. Az alkalmazott adatvédelmi audit jellemzőit is meg kell jelölni, függetlenül attól, hogy azt belső vagy külső egység végezte. Eredményét továbbítani kell az ellenőrző vállalkozás valamint az adatvédelmi tisztviselők vagy az adatvédelmi megfeleléséért és képzésért felelős személyek vagy szervezetek számára a GDPR 47. cikk (2) bekezdés j) pontja alapján. A WP108 6.3. pontja értelmében a nemzeti hatóságok az audit jelentések azon részébe, amelyek nem kapcsolódnak az adatkezelési műveletekhez, nem tekinthetnek be. Meghatározott független személy, osztály kijelölése és egy előre megszerkesztett panasz-bejelentési formanyomtatvány is elvárás a WP 153 2.2. pontja szerint.

[274] A magas költségek miatt az adatkezelők jellemzően inkább nem alkalmaznak standardizált megoldásokat vagy szabványokat, egyedül a pénzügyi szektorban érzékelhető hajlandóság ebben a tekintetben. Részletesen lásd: SZÁDECZKY (2010)
[275] Az adatvédelem és az adatbiztonság kapcsolatáról és egymás viszonylatában elért fejlődésükről részletesen: BALOGH – KISS – POLYÁK – SZÁDECZKY – SZŐKE (2014)

DOI: 10.14750/ME.2019.022

Az egyik[276] vizsgált BCR értelmében a vállalkozáscsoport adatvédelmi intézkedései alkalmasak az engedély nélküli hozzáférés és adatkezelés, valamint az adatok elvesztése vagy károsodása elleni védelem megvalósításához, nevesítve ezek a módszerek a titkosítás, a tűzfalak, a hozzáférés-korlátozások és más védelmi mechanizmusok alkalmazása.

Az adatvédelmi tudatosságra vonatkozó képzések és fejlesztések célja, hogy felhívja a munkavállalók figyelmét és informálják őket a védelem szükségességéről. Indoka, hogy a BCR megsértése esetükben akár fegyelmi büntetés vagy munkaviszony megszüntetésének következményét vonhatja maga után.

A vizsgált BCR deklarálja, hogy a magánélet-védelmi csoport rendszeres ellenőrzést végez az adatkezelési műveletek vonatkozásában. A belső audit csoport, amely egy független tanácsadói stáb, jelentést tesz a központi igazgatótanácsnak, vizsgálatot folytat le meghatározott adatkezelési műveletek esetében, majd akciótervet készít. Emellett független, külső adatvédelmi auditorok alkalmazása is megengedett.

Egy másik[277] BCR részletezi az adatbiztonsági tevékenységeket is, ilyen például a belépés ellenőrzése, a rendszerhez való hozzáférés ellenőrzése, az adatokhoz való hozzáférés ellenőrzése.

VIII.12. A folyamatos változásokról

Amennyiben valamely tagállam jogi környezete módosul vagy a vállalkozáscsoport az adatkezeléseket érintően módosítja struktúráját, és ennek következtében a BCR is módosításra szorul, a nemzeti adatvédelmi hatóságokat és valamennyi cégcsoporti tagot értesíteni kell.

[276] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf
[277] http://www.evosoft.hu/kotelezo-ereju-vallalati-szabalyok-binding-corporate-rules

DOI: 10.14750/ME.2019.022

Ezt nemcsak az ésszerűség és a WP 154 szerinti minta struktúra, hanem a GDPR 47. cikk (2) bekezdés k) és m) pontja is előírja. Az adatvédelmi megfelelésért felelős személy vagy szervezeti egység a BCR frissítéséről és aktualizálásáról is gondoskodni köteles. A frissítés vagy módosítás során nem újra-engedélyezési eljárást kíván meg a WP 153, csupán egy meghatározott felelős személy feltüntetését, aki nyomon követi, nyilván tartja és bejelenti a módosításokat, éves rendszerességgel jelentést készít a BCR lényeges szabályainak megváltoztatásáról és a cégcsoport tagjainak változásáról.

Az egyik[278] vizsgált BCR fenntartja a jogot a BCR megváltoztatására. Indoka az alkalmazandó jogszabályok változása, a cégcsoport strukturális átalakulása, illetve az adatvédelmi hatóságok feltételeinek teljesítése.
A módosításokat a magánélet-védelmi csoportnak el kell fogadnia, ezt követően bejelentik az illetékes adatvédelmi hatóságnak.

A változások hatályba lépése után lehet az új BCR-t alkalmazni, amelyet az érintettek számára hozzáférhetővé kell tenni külön értesítési kötelezettség mellett. Az új tagoknak magukra kötelezőnek kell elismerniük még az első adattovábbítást megelőzően az új szabályokat. Nem jogszerű adatot továbbítani mindaddig, amíg a vállalkozáscsoport új tagja kifejezetten nem lesz kötve a BCR-ben foglalt szabályrendszerhez. Megítélésem szerint ilyen esetben az érintett taghoz továbbított személyes adatot a kollízió kiküszöböléséig vagy a BCR elfogadásáig nem volna szabad kezelni, az addig végrehajtott továbbítások során kezelt adatokat pedig törölni, de legalábbis zárolni volna szükséges. Az adatok megosztásáról és továbbításáról való rendelkezések között jogalapként tünteti fel a jogos üzleti érdeket, amennyiben megfelelő technikai és szervezeti védelmi intézkedések állnak fenn a célországban működő tagnál. Ennek hiányában az Európai Unióban alkalmazandó szerződéses minta klauzulák alkalmazását teszi kötelezővé.

[278] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf

DOI: 10.14750/ME.2019.022

VIII.13. Kapcsolat a nemzeti joggal

A BCR fontos tulajdonsága, noha sem feltüntetni nem kötelező benne, sem a hatósági eljárás során nem kell nyilatkozni róla, hogy hogyan viszonyul a nemzeti joghoz. Alapvető tétel, hogy amennyiben a nemzeti jog a BCR-ben foglaltakhoz képest magasabb védelmi szint biztosítását írja elő, akkor az prioritást élvez és megelőzi a BCR szabályait. Mivel azonban a tagállamokban kötelező volt implementálni az 95/46/EK adatvédelmi irányelvet is, a GDPR pedig közvetlenül hatályos és alkalmazandó, így elméletileg a különbség a tagállamok szabályozása között igen csekély lehet, jellemzően a szektorális és a végrehajtási kérdésekben találunk eltéréseket.
A harmadik országokban jellemzően alacsonyabb a személyes adatok védelmi szintje - ezért is alkalmaznak BCR-t a vállalkozáscsoportok -, így az a helyzet, hogy harmadik országban szigorúbb a nemzeti jog, szinte sosem áll elő.
A jogérvényesítés szempontjából valamely Európai Uniós tagállam bír joghatósággal és jár el, az ott székhellyel rendelkező vagy felelősséget vállaló tag lesz az alperes, így az alkalmazandó jog kérdése tulajdonképpen csak formális nyilatkozat.

Az egyik[279] vizsgált BCR több ízben is „jogszabályok szerint", „vonatkozó jogszabályoknak megfelelő" és „amennyiben vonatkozó jogszabályok megengedik" kifejezésekkel tanúsítja, hogy a nemzeti jogokat tiszteletben tartva jár el az adattovábbítás során, tehát mintegy szubszidiárius szabályrendszerként tekint a BCR rendelkezéseire.

Egy másik BCR[280] szintén a szigorúbb nemzeti jog elsőbbségét nyilvánítja ki. A BCR szabályai általános „iránymutatások", amelyek összhangban vannak az alkalmazandó joggal, amelyek szigorúbb szabályai felülírják a BCR rendelkezéseit. Amennyiben a nemzeti jog alacsonyabb védelmi szintet ír elő,

[279] http://www8.hp.com/hu/hu/binding-corporate-rules.html
[280] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf

DOI: 10.14750/ME.2019.022

a BCR prioritást élvez. Többféle értelmezési lehetőség esetén a hatályos jogi környezet céljaival és alapelveivel leginkább konzisztens módon és összhangban kell az alkalmazandó norma tartalmát felfedni és alkalmazni, rögzíti a BCR. Amennyiben a nemzeti jog nem teszi lehetővé a BCR szabályainak betartását, azt jelenteni kell a felelősséget vállaló tagnak és a nemzeti adatvédelmi hatóság felé is.

Az egyik[281] BCR szintén a nemzeti jog elsődlegességét rögzíti. Kötelezettségként állapítja meg, hogy valamennyi vállalkozáscsoporti tag köteles megvizsgálni a vonatkozó nemzeti jogszabályokat, és kötelesek gondoskodni betartásukról, amennyiben azok a BCR-nél szigorúbban rendeznek bizonyos helyzeteket.

VIII.14. Kapcsolat az adatfeldolgozókkal

Az adatkezelő adatfeldolgozót vehet igénybe, amely lehet a vállalkozáscsoport tagja vagy a vállalkozáscsoporton kívüli cég is. Az adatkezelő a vállalkozáscsoporton belüli adatfeldolgozót úgy köteles kiválasztani, hogy az megfelelő adatbiztonsági intézkedéseket mellett képes legyen ellátni az adatkezelő utasításainak megfelelően a tevékenységet. A vállalkozáscsoporton kívüli adatfeldolgozó esetén korlátozásokat szükséges bevezetni attól függően is, hogy az harmadik országban vagy Európai Uniós tagállamban működik-e.

A WP 108 rendelkezik arról, hogy a BCR jóváhagyására irányuló kérelemben meg kell jelölni, hogy az adatfeldolgozó, aki nem a vállalkozáscsoport tagja, hanem annak például szerződéses partnere, milyen alapon tartozik a BCR betartásáért felelősséggel és milyen jogalapon történik számára az adattovábbítás.

[281] http://www.evosoft.hu/kotelezo-ereju-vallalati-szabalyok-binding-corporate-rules

DOI: 10.14750/ME.2019.022

Az egyik vizsgált BCR[282] „harmadik fél feldolgozóként" nevesíti az üzletvitelben támogatást nyújtó szolgáltatót. Esetében a megfelelő védelmi szintet nem a BCR, hanem a szerződéses klauzulák alkalmazása garantálja, mivel nem tagja a vállalkozáscsoportnak. Hasonlóan a szerződéses klauzulák alkalmazásáról rendelkezik egy másik[283] BCR is, amely külön feltételként írja elő, hogy amerikai adatfeldolgozó esetén a vállalkozás legyen a Privacy Shield alapján tanúsított adatfeldolgozó. Racionális jogi megoldás, hiszen az adatfeldolgozóval kötendő szerződéses kapcsolat egyébként is kívül esik a BCR alkalmazási körén, valamint a szerződés megkötésével egyidejűleg a standard klauzulák elfogadása is rendezhető.

Egy másik BCR[284] adatfeldolgozói BCR akként rendelkezik, hogy az „itt foglalt szabályok a további külső adatfeldolgozásról szóló megállapodások esetén is érvényesek." Ennek értelmében, függetlenül attól, hogy az al-adatfeldolgozó a vállalkozáscsoport tagja-e, a BCR szervi hatálya alá tartozik és köteles betartani annak szabályait. Ez persze csak úgy várható el tőle, ha az adatfeldolgozó erről előzetesen tájékoztatja és a közöttük létre jövő szerződés keretei között ebben megállapodnak.

A további adatfeldolgozó igénybe vételének lehetősége gyökeresen megváltozott az előző generációs szabályozáshoz képest. Míg az Avtv. 4/A. (2) második mondata az adatfeldolgozó számára tilalmazta tevékenységének ellátása érdekében további adatfeldolgozó igénybevételét, az Infotv. 10. § (2) bekezdése viszont lehetővé teszi az al-adatfeldolgozó bevonását, amelyet az adatkezelő rendelkezéséhez köt. A módosító 2013. évi L. törvény 28. § indokolása szerint a módosításra azért volt szükség, mert „az adatfeldolgozás kiszervezésének korábbi tilalma korszerűtlenné vált". A GDPR szintén lehetővé teszi további adatfeldolgozó bevonását, amelyet a 28. cikk (2) bekezdése az adatkezelő előzetesen írásban tett eseti vagy általános

[282] https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf
[283] http://www.evosoft.hu/kotelezo-ereju-vallalati-szabalyok-binding-corporate-rules
[284] https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf

DOI: 10.14750/ME.2019.022

felhatalmazásához köti. Ez a tény azért bír nagy jelentőséggel, mert további adatfeldolgozó bevonásával a BCR szabályaihoz kötött vállalkozások láncolata megszakadhat, hiszen az adatkezelő külön erre irányuló kikötése illetve az adatfeldolgozóval kötendő szerződében foglalt rendelkezés hiányában az al-adatfeldolgozó olyan jogi környezetben kezelhet személyes adatot, amely nem biztosít megfelelő védelmi szintet, és a BCR hatálya sem terjed ki rá. Tehát elképzelhető az a hipotetikus eset, amikor az al-adatfeldolgozó nem áll a BCR és a GDPR hatálya alatt sem, nemzeti joga nem biztosít megfelelő védelmi szintet, és az adatalany személyes adatainak védelméhez való joga nem érvényesülhet, még akkor sem, ha a GDPR 28. cikk (4) bekezdés a megbízó adatfeldolgozó az adatkezelő felé fennálló teljes felelősségét deklarálja.

Ezért értékes a WP 108 fentebb hivatkozott rendelkezése, amely szerint a BCR jóváhagyási eljárása során a kérelemben meg kell jelölni az al-adatfeldolgozóra vonatkozó információkat. Azonban a további adatfeldolgozó igénybe vételének korlátlan lehetősége, még ha az adatkezelő erre vonatkozóan rendelkezett is előzetesen, egy olyan végtelen elemből álló adatfeldolgozói láncolat létre hozásának adhat lehetőséget, amely az érintett tényleges önrendelkezési jogának újabb részletét üresíti ki.

VIII.15. Együttműködési kötelezettség

A vállalkozáscsoport tagjai egymással és az érintett adatvédelmi felügyelő hatósággal is kötelezően együttműködnek, ezt a GDPR 47. cikk (2) bekezdés l) pontja is előírja. A vizsgált BCR-k mindegyike rögzíti e kötelezettséget, fenntartások vagy kivételek rögzítése nélkül. Az együttműködés kiterjed a BCR szabályainak betartására, értelmezésére, alkalmazására, a panaszkezelési és a hatósági eljárások cselekményeire is.

DOI: 10.14750/ME.2019.022

A vállalkozáscsoport tagjai kötelesek az „adatvédelmi hatóságok BCR-rel kapcsolatos megkereséseit megfelelő határidőben és módon megválaszolni, valamint a hatóság javaslatait és döntéseit a BCR implementálása során figyelembe venni”.[285]

VIII.16. Mellékletek

Ahogyan arra a fejezet bevezető részében is utaltam, a BCR „tiszta” szövege az adatvédelmi politika egy része csupán. A hatósági jóváhagyáshoz a BCR tervezetén és a WP133 szerinti nemzeti kérelmek benyújtásán túl a vállalkozáscsoportoknak a további mellékleteket is a hatóságok rendelkezésére kell bocsátaniuk.

A NAIH az Infotv. 64/A. § (2) bekezdése szerint az alábbi iratösszesség benyújtását írja elő:

- az adatkezelés nyilvántartási számát vagy ennek hiányában, mivel a GDPR hatályba lépésére tekintettel ilyen nyilvántartást a NAIH a továbbiakban már nem vezet, az alábbi adatokat:

a) az adatkezelés célját,

b) az adatkezelés jogalapját,

c) az érintettek körét,

d) az érintettekre vonatkozó adatok leírását,

e) az adatok forrását,

f) az adatok kezelésének időtartamát,

g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is,

h) az adatkezelő, valamint az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,

[285] http://www.evosoft.hu/kotelezo-ereju-vallalati-szabalyok-binding-corporate-rules

DOI: 10.14750/ME.2019.022

i) az alkalmazott adatfeldolgozási technológia jellegét,

j) a belső adatvédelmi felelős alkalmazása esetén annak nevét és elérhetőségi adatait.

- a BCR tervezetét,

- a BCR kötelező jellegének igazolására szolgáló adatokat,

- ha a BCR-t más EGT-állam adatvédelmi hatósága jóváhagyta, az ennek igazolására szolgáló adatokat.

Igaz, hogy ezen rendelkezés inkább eljárásjogi típusú rendelkezés, mégis megerősíti azt a megállapításom, hogy a BCR (nyilvános, közzétett) szövege mindössze a törzse a megfelelésnek, a megfelelő védelmi szint biztosításának megállapíthatóságához a vállalkozáscsoportnak teljes adatvédelmi gyakorlatát, politikáját összességében kell értékelni.

A WP154 szerinti *minta-struktúra* is meghatározza azokat a mellékleteket,[286] amelyeket csatolni szükséges a BCR-hez. Ennek alapján a jóváhagyó hatóság rendelkezésére kell bocsátani:
- az adatvédelmi politikát, amely adatkezelési tevékenységenként tájékoztatja az érintettet arról, hogy a vállalkozáscsoport hogyan kezeli és védi a személyes adatokat;
- egy iránymutatást, amely azoknak a munkavállalóknak készült, akik személyes adatokhoz férnek hozzá és azokkal dolgoznak. Az iránymutatás segítségével a dolgozóknak könnyen meg kell érteniük és alkalmazni kell tudniuk a BCR szabályait, például egy panaszkezelési eljárás vagy az érintett hozzáférési jogának gyakorlása során;
- adatvédelmi audit tervet és programot, amelyet a vállalkozáscsoporton belül működő auditor vagy külső auditáló szervezet segítségével állítottak össze;
- az adatvédelmi képzések leírását vagy azokra példákat;

[286] WP 154 p. 10.

DOI: 10.14750/ME.2019.022

- dokumentációt arra vonatkozóan, hogy amennyiben az adattovábbítás kiinduló pontja harmadik országbeli tag, úgy az Európai Unión belüli tevékenységi központ vagy az EU-n belüli felelősséget vállaló vállalkozáscsoporti tag megfelelő vagyonnal rendelkezik arra az esetre, ha kártérítés vagy sérelemdíj fizetésére kötelezné a vállalkozáscsoportot a BCR megsértése miatt.

Ebből további ezidáig megválaszolatlan kérdések is adódnak. *Egyrészt* egyetlen WP sem rendezi, hogy akár a főhatóság, akár az érintett hatóságok milyen szempontok alapján bírálják el a vagyon mértékének megfelelőségét. Ennek azért lehet jelentősége, mert az egyes tagállamok között – de még a tagállamok egyes bíróságai között is – eltérő az ítélkezési gyakorlat a sérelemdíj mértéke kapcsán. Azaz többet érhet a háborítatlan magánélet egy kis faluban, mint egy fővárosban, és sokkal többet érhet a magánélet védelme egy zárt, konzervatív közösségben, mint egy nyitott társadalmi csoportban.

Másrészt kérdéses, hogy jogosult-e bármely hatóság ezen kijelölés ellen olyan kifogást támasztani, hogy másik tagot kelljen kijelölni a felelősséget viselő vállalkozáscsoporti tagként. Harmadrészt az sem tisztázott még, hogy az érintett hivatkozhat-e a BCR megsértésre a vállalkozáscsoport tagjával szemben. Ha nem, akkor kizárólag azt kell figyelembe venni, hogy a vállalkozáscsoport képes-e a GDPR szerinti bírság megfizetésére, amelynek kiszabása szintén tagállami hatósági hatáskörbe tartozik, így mértéke és összege is eltérő lehet a GDPR adta maximum keretben. Mindezek megfontolását követően javaslatom, hogy a BCR kötelező tartalmi elemeként kelljen a vállalkozáscsoport valamennyi tagjának egyetemleges kötelezettséget vállalnia a jogsértő tag magatartása esetén kiszabott kár megtérítésére, de legalábbis sortartó kezességet vállalni a jogsértő tag nemteljesítése esetére. Így elvben az érintett jogsérelme esetén nagyobb valószínűséggel biztosítható a kár megtérítéséhez szükséges anyagi fedezet.

DOI: 10.14750/ME.2019.022

- a vállalkozáscsoport belső panaszkezelési mechanizmusának bemutatását;

- a BCR hatálya alá tartozó tagok megnevezését;

- az adatbiztonsági intézkedések és az informatikai rendszer információvédelmi rendszerének bemutatását;

- annak igazolására szolgáló folyamatleírást, hogy a jövőben bevezetendő új, a személyes adatok kezelésére és feldolgozására felhasználandó technológiák miként felelnek meg a BCR rendelkezéseinek;

- a vállalkozáscsoport tagjaként vagy azon kívüli adatfeldolgozókkal kötendő szerződés mintákat;

- az adatvédelmi tisztviselő vagy az adatvédelmi megfelelésért felelős más munkavállaló munkakörének leírását.

A WP 108 4. pontja rendelkezik még egy külön íven benyújtandó dokumentumnak a tartalmáról, melyet az eljáró hatósághoz be kell nyújtani:
- a kapcsolattartó személy nevét, elérhetőségét,
- a vezető hatóság kiválasztásának indokát,
- a vállalkozáscsoport alapvető struktúráját,
- az adattovábbítás folyamatát, célját és eszközeit,
- a vállalkozáscsoport tagjainak üzletviteli helyét,
- az adattovábbítás kiindulási helyét és a fogadó fél adatait.

A jóváhagyáshoz nemzeti hatóságonként eltérő lehet a csatolandó egyéb dokumentumok köre. Az üzleti titkot tartalmazó, kereskedelmileg érzékeny adatot a kérelemben külön jelezni kell.

Ezek a dokumentumok jellemzően nem nyilvánosak, a vállalkozáscsoport nem teszi közzé őket, de a BCR megfelelésének megítélése érdekében szükségesek.

DOI: 10.14750/ME.2019.022

Az azonban nem tisztázott, hogy a vezető hatóság vagy az érintett hatóságok a jóváhagyási eljárás során a BCR tervezetén túl ezen dokumentumok és az alapul szolgáló gyakorlatok vonatkozásában is kiköthetik-e a módosítás szükségességét, vagy csak azt jogosultak vizsgálni, hogy ezen gyakorlatok függvényében megfelelőek-e a BCR rendelkezései.

VIII.17. Konklúzió a tartalmi elemzés nyomán

Megállapítható, hogy a GDPR 47. cikk (2) bekezdésében foglalt kötelező minimum tartalmi elemek *egybevágnak a WP 154 szerinti minta-struktúra elemeivel*. Ha nem tudnánk, hogy a WP 154 2008-ban készült, azt is gondolhatnánk, hogy a GDPR szabálya szerint állította a 29. cikk szerinti munkacsoport a dokumentumot, pedig éppen fordítva történt. Ez a tény azt támasztja alá, hogy jelen esetben a jogalkotó *egy régi piaci igényre reagált*. Amelyet a soft law jogforrási környezet már előirányzott, azt jogalkotó a GDPR-ban deklarálta.

Megállapítható az is, hogy a BCR *dinamikus és statikus részekből* áll. Dinamikus tartalmi elemek körébe sorolom az olyan tartalmi elemeket, amely gyakran vagy időszakosan változhatnak, emiatt a BCR vonatkozó rendelkezésének módosítását követelik meg. Statikus részeknek nevezem azokat az információkat, amelyet hosszú távra konstruálható, állandó rendelkezések lesznek, mert a jogi környezet változása hiányában azok nem szorulnak majd módosításra. Jellemzően dinamikus részek a BCR hatálya alá tartozó vállalkozáscsoporti tagok listája, az adattovábbítások leírása, a küldő és a fogadó vállalkozások listája, a továbbítandó adatok köre, az érintettek köre, az adatfeldolgozókra vonatkozó rendelkezések, az adatbiztonságra vonatkozó rendelkezések, a képzések és a megfelelés ellenőrzésének kérdése. Jellemzően statikus részek az adatvédelmi elvek és alapfogalmak, az érintettek jogai és azok gyakorlásának módja, a felelősségi kérdések és a panaszkezelésre, jogérvényesítésre vonatkozó rendelkezések, valamint

DOI: 10.14750/ME.2019.022

jellemzően az adatkezelés jogalapja. A vizsgált BCR-k között volt olyan, amely még az Adatvédelmi Irányelvre hivatkozott alapul fekvő jogforrásként, kijelölt adatvédelmi tisztviselőt pedig egyik sem említett. A tartalmi elemek nem determináltan változó vagy állandó rendelkezések, mert a vállalkozáscsoport struktúrája, tevékenysége illetve az uniós vagy a nemzeti jog változása bármikor indukálhatja a szabályok változtatásának kényszerét.

A BCR természetéből adódóan nem lehet olyan részletes, mint egy jogszabály, elegendő hivatkozni benne az alapul fekvő joganyagra.
A BCR ugyanakkor több ponton a vállalkozáscsoport adatvédelmi politikájába illeszkedő *jogszabályi kivonat*, amelyet mindennapi működésében saját magára nézve kötelezettségvállalás módjára teljesít, jól megfontolt esetekben szerződéses viszonyaiban is kötelezővé tesz. Jelentőségét abban nyeri el, hogy mind egyoldalú kötelezettségvállalás, mind általános szerződési feltételek nézőpontból tekintve kötelezővé válik azok vállalkozáscsoporti tagok számára is, amelyeket a harmadik ország nemzeti joga egyébként nem kötne (uniós szintű) adatvédelmi intézkedések megvalósításához. Egy vitatható pont ebből a szempontból az *al-adatfeldozó igénybevételének lehetősége,* amely a BCR valós funkcióját olthatja ki. Míg a BCR a vállalkozáscsoport tagjai számára az adatvédelmi politika keretrendszere, egy harmadik országban adatfeldolgozást végző nem vállalkozáscsoporti tag nem tartozik a hatálya alá, tevékenysége a BCR személyi és tárgyi hatályán kívül esik. Ha pedig nemzeti joga alacsonyabb adatvédelmi standardjai kötik csupán, a megfelelő védelmi szint biztosítása részéről nem biztosított. Érdemes lett volna elfogadni még a jogalkotási eljárás során tett azon javaslatot,[287] amely a további adatfeldolgozókat is automatikusan a BCR hatálya alá rendeli. Ennek hiányában csak az adatkezelő tudatosságában bízhat az érintett, vagyis abban, hogy először is megfontolja harmadik országban működő adatfeldolgozó igénybe vételét, amennyiben pedig ilyen adatfeldolgozót vesz igénybe, a

[287] Részletesen lásd a III. fejezet 2.2. pontjában.

DOI: 10.14750/ME.2019.022

köztük megkötendő szerződésben rendelkezik a további adatfeldolgozó bevonásáról és a BCR – vagy más jogi eszköz – kötelező alkalmazásáról a megfelelő védelmi szint érdekében.

Fontos emlékeztetni arra, hogy a BCR *nem a célország megfelelő védelmi szintjét biztosítja*, hanem csupán a vállalkozáscsoporti tag biztosítéka. A BCR nem egy közjogi, állami közhatalom által nyújtott védelem, hanem egy magánjogi, a gazdasági társaság belső rendszerének szabályai szerint keletkező biztosíték, noha állami szinten történik a jóváhagyása és eseti kikényszerítése is. Annak tudatában, hogy a BCR tehát csak a vállalkozáscsoport tagját köti, akire a nemzeti jog nem szab szigorú adatvédelmi kötelezettséget a harmadik országban, azt várnánk, hogy jogszabályszerű pontossággal és részletességgel tegye azt meg a BCR. A tartalmi elemzés során azonban az volt tapasztalható, hogy a BCR-k online elérhető törzsszövege jellemzően általános rendelkezéseket állít, szó szerint idézi a jogszabályszöveget, de nem konkretizálja a szabályt az egyedi esetre.

Az a követelmény, hogy a BCR a harmadik országban működő vállalkozásra absztrakt jogi normaszöveg-szerű szabályozása kötelező erővel bír, a harmadik ország szabályozásának teljes hiánya vagy a szabályozás megfelelő védelmi szintjének hiánya fényében, mégis megvalósulni látszik. Ahhoz, hogy a BCR alapvető célját értékelni tudjuk, hátra kell egyet lépni. Nem európai szemmel kell vizsgálni a szabályokat, és saját, hosszú múltra visszatekintő, szigorú szabályozásunkhoz kell azt mérni, hanem ahhoz, hogy egy olyan környezetben kell azokat betartani, ahol ezidáig közel sem voltak ehhez hasonló kötelezettségek, elvek, szabályok. Persze azt el kell ismerni, hogy a védelmi szintből engedni nem szabad, ezért mégiscsak saját, szigorú európai szabályainkat kell exportálni a harmadik országba, a BCR alkalmazásával is.

DOI: 10.14750/ME.2019.022

IX. FEJEZET
SWOT ANALÍZIS

XI.1. Nézőpontok

A BCR vizsgálata körében egy, a stratégiai elemzési folyamatok során alkalmazandó alaptechnikát vettem alapul annak érdekében, hogy a BCR hasznosságát illetve hátrányait, fejlesztési lehetőségeit és az alkalmazásában rejlő veszélyeket rendszerezzem. Alapállásom, hogy a BCR-nek mint jogintézménynek az adatvédelmi jogi környezetben betöltendő szerepét vizsgálom, elsősorban adatkezelői szempontból. Amennyiben a BCR iránt érdeklődő gazdasági szereplő adatkezelő vizsgálja meg a táblázatot, a szempontok segítséget nyújthatnak abban, hogy a jogintézmény a vállalkozáscsoport számára milyen előnyöket nyújthat, illetve hogy milyen kezdeti, majd távlati nehézségekkel kell szembenéznie az adatkezelőnek. Az adatalany számára a hátrány és veszély rubrikákból tűnhet ki, hogy alapvetően egy, elsődlegesen az adatkezelői érdekeket szolgáló, mégis adatvédelmi eszköz a BCR, amely a kiforratlan, több tagállamban egyelőre nem is létező jogi környezet és jogalkalmazói jó gyakorlat hiányában az érintetti jogvédelem egyik vitatható, bár népszerű bástyája.

A SWOT analízis során S mint strengths azaz az erősségek rovatba sorolom azokat a tényezőket és jellemzőket, amelyek a vizsgált jogintézmény jogi természetéből adódnak és támogatásuk, fejlesztésük a BCR előnyeit szolgálják. Ezzel szemben a W mint weaknesses azaz gyengeségek olyan jellemzők, amelyek kiküszöbölése vagy reformálása szükséges. A lehetőségek O mint opportunities rovatban olyan külső tényezőket lehet felsorakoztatni, amelyek a BCR fejlesztéséhez, elterjedéséhez szükségesek, de legalábbis hasznosak lehetnek, míg a T mint threats azaz veszélyek cella azokat a külső tényezőket tartalmazza, amelyek a BCR szűken vett anyagi jogi természetétől függetlenül hatnak negatívan alkalmazásának körülményeire és hatásaira.

DOI: 10.14750/ME.2019.022

S	W
- szerződéses klauzulák alkalmazását váltja ki a megfelelő védelmi szint biztosítása körében - szektorspecifikus, egyediesíthető - összehangolja az adatvédelmi politikát a vállalkozáscsoportban - átláthatóvá teszi az adatkezelési mechanizmusokat - erősebb megfelelési hajlandóság - in house probléma megoldás, elszámoltathatóság - integrálja az adatvédelmi politikát a vállalkozáscsoport a gazdasági ügyvitelébe - EU adatvédelmi politikájának exportja	- adatalany önrendelkezési jogának bizonyos fokú korlátozása, céges érdekek elsődlegessége - általánosítja a védelmi szintet - kollízió lehet a harmadik ország nemzeti jogával - nyilvános részében a részletek és pontosság hiánya - több érintett hatóság, nehezebb megfelelés - szabályozás hiányában bizonytalan a jogérvényesítés - nem tisztázott az alkalmazásra jogosultak köre hazánkban (pl. egyesület, alapítvány) - a vállalkozáscsoportra nézve kötelező, nem a harmadik ország védelmi szintjét biztosítja - a BCR alkalmazásához szükséges az anyagi és eljárás jogi környezet illetve jó gyakorlat kialakítása minden uniós tagállamban - időigényes és drága engedélyeztetési eljárás - versenytorzító/befolyásoló hatása lehet
O	T
- új szolgáltató szektori alanyok BCR kidolgozására - az EU adatvédelmi szabályozási logikáját terjesztheti - PR tényező - jobb kapcsolat a nemzeti hatósággal - kölcsönös elismerési eljárás - adatvédelmi tudatosság növelése a kollektíván belül, „érzékenyítés” - DPO munkájának megkönnyítése, esetenként bonyolítása	- kétséges a valós kötelező erő - szerződés / egyoldalú nyilatkozat / ÁSZF? - változhat a vállalkozáscsoport struktúrája – aktualizálás - változó jogi környezetben új engedélyeztetés? - forum shopping lehetősége az engedélyeztetéskor, az igényérvényesítés esetére

DOI: 10.14750/ME.2019.022

A táblázatból, azonban azon túl, hogy számszerűsítjük a szempontokat az egyes rovatokban, számos következtetés vonható le a szempontok értékelő elemzését követően.

IX.2. Előnyök és gyengeségek - S és W

Alkalmazzunk-e vállalkozáscsoportunknál BCR-t? A hipotetikus kérdésre az elméleti választ az S és a W cellák elemzésével adhatjuk meg.

Tekintettel arra, hogy a vállalkozáscsoport egyes tagjai más-más államban, jellemzően harmadik országban is végeznek adatkezelő illetve adatfeldolgozó tevékenységet, így egyes tagjai más joghatóság alá tartoznak, eltérőek a nemzeti adatvédelmi jogszabályok és adatvédelmi gyakorlatuk különböző lehet. A BCR elsődleges célja, hogy biztosítsa a megfelelő védelmi szintet a vállalkozáscsoport tagjai által végzett, harmadik országba is irányuló adattovábbítások vonatkozásában, amely a harmadik országba irányuló adattovábbítás egyik alapvető érvényességi kelléke is.

Fontos azonban kiemelni, hogy a BCR „csak” a vállalkozáscsoport adatkezelési tevékenységére tartalmaz kötelező rendelkezéseket, és nem a harmadik ország megfelelő védelmi szintjét eredményezi, nem jogalkotói garancia. Ebből adódóan pedig felmerül annak a veszélye, hogy amennyiben a vállalkozáscsoport harmadik országbeli tagja mint adatfeldolgozó a vállalkozáscsoporton kívüli további adatfeldolgozót vesz igénybe saját harmadik országában, úgy a BCR és a GDPR garanciái már nem érvényesülnek.

Ez az automatikus védelmi szint csökkenés jellemezte még az Adatvédelmi Irányelv jogi környezetét, azonban a GDPR megoldani látszik a problémát.

DOI: 10.14750/ME.2019.022

A GDPR 28. cikk (4) bekezdése értelmében más jogi aktus útján - például BCR alapján - erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben vagy jogi aktusban – a BCR-ben – szerepelnek. Így a további adatfeldolgozónak is megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen a GDPR követelményeinek. A GDPR felelősségtelepítő rendelkezése a további adatfeldolgozót megbízó adatfeldolgozó vonatozásában kimondja, hogy amennyiben a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé. Ezzel megoldani látszanak az al-adatfeldolgozó, a GDPR terminológiája szerint további adatfeldolgozó igénybe vételéből adódó, az európai és tagállami jog alól kibújni szándékozó adatkezelő illetve adatfeldolgozó felelősségi viszonyai. Így a felelősség csökkentése érdekében nem lesz értelme harmadik országbeli további adatfeldolgozót igénybe venni, tekintve hogy az európai uniós adatvédelmi standard exportja valósul meg, nemcsak a további adatfeldolgozó, hanem valamennyi harmadik országbeli adatkezelő és adatfeldolgozó vonatkozásában, amennyiben a GDPR hatálya alá tartozik tevékenységük, akár BCR alapján is.

A BCR további célja, hogy a vállalkozáscsoporton belül egységes adatvédelmi és adattovábbítási szabályrendszert hozzon létre, mivel a magatartási kódex jellegű keretrendszer támpontokat biztosít az egységesítéshez, a különböző gyakorlatok összehangolásához, amely az adatvédelmi standard azonos színvonalát, megbízhatóságát eredményezi a vállalkozáscsoporton belül.

A BCR általánosít a védelmi szint tekintetében. A vállalkozáscsoport tagjai számára azonos követelményeket állít fel, amelynek elvileg a vállalkozáscsoport tagjai közül a legmagasabb védelmi szintet megkövetelő tagállamában fennálló szinthez kellene igazodnia. Ennek következtében pedig

DOI: 10.14750/ME.2019.022

különbségek alakulhatnak ki a az egyes tagok adatvédelmi gyakorlatai között. Tartalmi kérdés ugyan a BCR és a nemzeti jogok viszonyának szabályozása, azonban általánosan elfogadott, hogy a védelem szigora tekintetében a nemzeti jog prioritást élvez, tehát a meglévő - a nemzeti jogszabálynak megfelelő - védelmi szintet nem ronthatná le. Ered ez abból is, hogy a törvényi kogenciát és a nemzeti jogrendszer imperatív szabályait a felek megállapodása – jelesül itt a BCR mint egyoldalú nyilatkozat, szerződés, általános szerződési feltételek – nem csökkentheti. A BCR elvileg ellentétbe is kerülhet az adott nemzeti joggal, ha alacsonyabb védelmi szint megvalósítására alkalmas csupán, azonban a jóváhagyás során, mikor valamennyi, az adattovábbítással érintett tagállami hatóság megvizsgálja a szabályait, az együttműködési mechanizmus eredményeként nem volna szabad, hogy kollízió alakuljon ki, a GDPR jogegységesítő hatása okán sem. A harmadik országbeli szabályozást tekintve nagyobb eséllyel alakul ki kollízió - mivel azt a BCR jóváhagyása során ezt nem vizsgálják hatóságok -, amely ütközést a BCR és a nemzeti jog viszonyának rögzítése sem minden esetben oldhat fel. Amennyiben a harmadik országbeli hatóság rendelkezése jogszerű, de ellentétes a BCR adatkezelési szabályaival, úgy vitás helyzet alakulhat ki a vállalkozáscsoport tagja vonatozásában. Ilyen esetben az adatkezelő eljárhat-e a nemzeti hatósága által meghatározott rendelkezéssel ellentétesen, például adatközlés vagy az kért személyes adatokhoz való hozzáférés megtagadásával?[288]

A BCR tartalmi elemzése körében rögzített megállapítások[289] itt is irányadók azzal, hogy a nemzeti jog és a BCR szabályainak kollíziója esetén valószínűsíthető, hogy nem lesz elterjedt gyakorlat a fent hivatkozott példa.

[288] Nagy médiavisszhangot kiváltó eset volt 2016 decemberében, hogy az Apple Inc nem tett eleget az FBI megkeresésének, amelyben a san bernardino-i lövöldözés elkövetőjének mobiltelefonjához kértek szoftveres hozzáférést a titkosítás feltörésével. Megjegyzendő, hogy a hozzáféréshez egy szoftvert kellett volna létre hozniuk az Apple fejlesztőinek, amellyel minden ilyen típusú mobiltelefon titkosítása feltörhető, amely magas adatvédelmi kockázatot jelenthetett volna a jövőben, ezen túl az Apple minden segítséget megadott a nyomozáshoz. A cég nyilatkozata: https://www.apple.com/customer-letter/ [2018. február 21.]
[289] Részletesen lást a VIII. Fejezetben.

DOI: 10.14750/ME.2019.022

A nemzeti közjog előírása valószínűleg felülírja majd a BCR mint magánjogi rendelkezés előírását, így tulajdonképpen ebből a szempontból a BCR nem biztosít semmilyen védelmi szintet a harmadik országban. Az megjegyzendő azonban, hogy a magánjogi viszonyokban valószínűleg visszatartó erő lesz az európai vállalkozáscsoporti tagok részéről, az eddig az adatvédelmi jogterületen nem jellemző, magas összegű bírság lehetősége, és nem fognak kockáztatni a harmadik országbeli közreműködő igénybe vételével, hacsak a harmadik országbeli nemzeti jog maga nem biztosítja a közel megfelelő védelmi szintet. Azonban mivel megfelelőségi határozat meghozatalát a harmadik ország vonatkozásában egy vállalkozáscsoport nem kezdeményezhet, így saját megoldást kell találnia, például BCR alkalmazását.

A BCR-t jellemzően olyan a vállalkozáscsoportok alkalmazzák, amelyek számos tagállamban és harmadik országokban rendelkeznek vállalkozáscsoporti taggal és tömeges mennyiségű, rendszeres adattovábbítást végeznek. A BCR-rel hosszútávon jelentős adminisztratív tehertől szabadulnak, például az eseti szerződéses klauzulák alkalmazásától is. A BCR a jogszabályi előírásoknak úgy tehet eleget, hogy szabályai illeszkednek a vállalkozáscsoport struktúrájára és tevékenységére, illetve az adott gazdasági szektor sajátosságaira. Ez az adatalany szempontjából azért lehet előnyös, mert közvetve így az ő helyzetére is jobban illeszkedő és alkalmazható szabály szerint kezelik és továbbítják személyes adatait, amely végső soron az adatalany önrendelkezési jogát is kevésbé korlátozhatja. Mindemellett látni kell, hogy a BCR elsősorban a vállalkozáscsoport adattovábbítási tevékenységének érdekeit szolgálja, és másodlagos az érintett jogainak biztosítása.

Az ügyfél, a munkavállaló automatikusan, kötelező jelleggel alanyává válhat a BCR-eknek, mivel azok személyi hatálya kifejezetten rájuk terjed ki. Az ügyfél a termék megszerzésével, a szolgáltatás igénybevételével, a munkavállaló pedig a munkáltatóval létrejött munkaviszony alapján alanya az

DOI: 10.14750/ME.2019.022

adatgyűjtésnek, adatkezelésnek és így az adattovábbításnak és adatfeldolgozásnak is. Az „opt in” vagy „opt out” jog biztosítása a BCR elsődleges céljával volna ellentétes, így gyakorlatban megvalósíthatatlannak látom egyedi igények alapján a BCR alkalmazásának kizárását, tekintettel az általában tömeges adattovábbítási folyamatok természetére. Ebből adódóan pedig egyértelműen az információs önrendelkezési jog jelentős korlátozása.

A contrario adódik, hogy a BCR nem hatékony kisebb vállalkozáscsoportok számára. Felmerül továbbá, hogy a BCR alkalmazási köre nem tisztázott. A GDPR rendezi ugyan a vállalkozáscsoport fogalmát, azonban a magyar szabályozás, valószínűleg szándékosan, bizonytalan jogfogalmat alkalmazott. Míg a GDPR egyértelműen a vállalkozáscsoporthoz köti BCR alkalmazását, addig az Infotv. 2018 júliusáig hatályos szövege nem rögzítette az alkalmazni jogosultak körét, sőt egy kifejezetten széles értelmezési lehetőséggel élve a „szervezet” elnevezést használta. Ennek következtében akár egy egyesület, vagy alapítvány is alkalmazhatott volna BCR-t Magyarországon, kérdés azonban, hogy a GDPR alapján is BCR-nek minősült volna-e az adott jogi eszköz. Álláspontom szerint nem, tekintettel az alanyi kör GDPR szerinti eltérése miatt. Rövidtávon a valamennyi érintett nemzeti hatóság általi jóváhagyása, még ha a tagállamok részt is vesznek akár az együttműködési, akár a kölcsön elismerési mechanizmusban, időigényes, akár egyévi időtartamot felölelő eljárás is lehet. Mindaddig, amíg az anyagi jogi és eljárás jogi környezet illetve jó gyakorlat kialakítására sor kerül minden uniós tagállamban, addig a BCR jóváhagyása jellemzően soft law jogforrásokon alapuló eljárás marad, amely jogbizonytalanságot hordoz.

Hasonló kétségek merülnek fel az érintetti jogérvényesítés körében is minden olyan államban, ahol a BCR szabályozása nem teljes körűen történik meg, az adatalany gyakorlatilag el van a zárva a jogérvényesítéstől. Minél több hatóság vesz részt a jóváhagyási folyamatban, minél több nemzeti joggal kell összeegyeztethetőnek lennie, annál körülményesebb és magasabb minőségű

DOI: 10.14750/ME.2019.022

szakmai tudást igényel a BCR megalkotása. A felmerülő eljárási díjak illetve a szakértő közreműködő igénybe vételének költsége pedig egyelőre messze meghaladja a BCR alkalmazásából származó előnyöket. Arra persze nincs még adat, hogy a GDPR szerinti bírságolási gyakorlat változtathat-e ezen a helyzeten, valószínűleg a BCR javára dől el a kétséges helyzet.

Mivel az adattovábbítás a gazdasági társaság működésének és profitjának motorja lehet, az adatvédelmi politika és a BCR szerves részét fogja képezni a vállalkozáscsoport üzletpolitikájában, így pedig legalábbis hasonló kiemelt figyelmet kap majd, mint bármely más beruházás, figyelemmel a GDPR szerinti bírság maximumokra. Mindez erősíteni fogja a megfelelési hajlandóságot is, amelyet segíteni fog az is, hogy a BCR szabályait a vállalkozáscsoport tevékenységére szabták, így az adott helyzetekre pontosan illeszkedő kvázi lex specialis alkalmazása „könnyebb" lesz, mint az „általános" GDPR rendelkezésének értelmezése. A BCR-ban kidolgozott in-house probléma megoldás pedig nemcsak a vállalkozás ügyfélkapcsolati politikájában lehet erősítő tényező, hanem a GDPR szerinti elszámoltathatóság elvével való összhang megteremtését is szolgálja.

Az elszámoltathatóság mellett az adatkezelés transzparenciája már régi elvárás és követelmény is. A BCR átláthatóvá teszi a vállalkozáscsoporton belüli adatkezelési mechanizmusokat, mivel szabályszerűen rögzíti azok menetét, a felelősségi rendelkezéseket. Ezen túl a nemzeti hatósági és az Európai Bizottság által vezetett nyilvános adatbázis biztosítja, hogy azok a jóváhagyott BCR-t alkalmazó vállalkozáscsoportok cégnevei bárki számára megismerhető legyen.

Ez persze nem azt jelenti, hogy valóban átláthatóbb volna az adattovábbítás tényleges gyakorlata az érintettek számára, hiszen a BCR-k nyilvános része az általános szabályokon túl nem tartalmaz részletszabályokat, jellemzően általánosít. A BCR tényleges tartalmát, amely adott esetben know how-t,

DOI: 10.14750/ME.2019.022

üzleti titok, üzletpolitikai és gazdasági stratégiai megalapozottságú ismereteket tartalmaz, csak a hatósági jóváhagyáshoz nyújtja be a vállalkozáscsoport, de nem teszi nyilvánosan hozzáférhetővé. Így az érintett személyes adatai sorsa felett érdemben információt nem szerez.

Az Adatvédelmi Irányelv szerinti, a harmadik országba irányuló adattovábbítás esetére előírt, a nemzeti adatvédelmi hatóság részére történő előzetes bejelentést a BCR kiváltja. Tekintettel arra, hogy a GDPR ilyen előzetes bejelentési kötelezettséget nem ír elő, így a BCR ilyen funkciót 2018. május 25. napjától már nem tölt be. Azonban ahhoz, hogy a BCR hatálya alatti adattovábbítás jogszerű legyen, az uniós tagállamok többségében a BCR előzetes hatósági jóváhagyása szükséges. Nem kell előzetes jóváhagyás alkalmazásukhoz például Dániában, Olaszországban, Liechtensteinben, Hollandiában, az Egyesült Királyságban és egyes német tartományokban.[290]

IX.3. A BCR alkalmazásából adódó lehetőségek – O

A vállalkozáscsoport hosszú távon költségeket takarít meg a BCR alkalmazásával, hiszen a szerződéses tárgyalások és a hatósági bejelentési kötelezettség anyagi vonzatait sem kell esetenként viselnie. Hatékonyabb szolgáltatást nyújthat, például husszonnégyórás ügyfélszolgálatot a harmadik országban, marketing terén előnyöket szerezhet, piaci megítélése is javulhat, partnereket is könnyebben szerezhet.

Ezzel párhuzamosan fejlődhet az adatvédelem általános, globális szintje is, mivel a vállalkozáscsoport kiterjeszti saját és az uniós adatvédelmi politika logikáját a harmadik országokban működő tagjaira, akik adott esetben további adatfeldolgozó igénybe vételével várják el és egyben terjesztik a harmadik országban az európai standard szerinti elvárásokat.

[290] Európai Bizottság: National filing requirements for authorisation of transfers on the basis of BCR http://ec.europa.eu/justice/data-protection/document/international-transfers/files/table_nat_admin_req_en.pdf [2018. február 12.]

DOI: 10.14750/ME.2019.022

A jogszabályi védelmen túl ezek a vállalkozáscsoportok a megfelelésen túl egy újabb garanciát nyújtanak, jelesül egy önként vállalt adatvédelmi keretrendszer önkéntes betartását, amely az ügyfelek szempontjából is egy vonzó jellemző lehet.

A vállalkozáscsoporton belül a BCR bevezetése számos végrehajtási és felelősségi változást eredményezhet. Fontos a tudatosság növelése érdekében a vállalkozáscsoporton belül ismeretterjesztő workshopok, egyeztetések megszervezése, amely eredményeként az operatív munka során a BCR szabályait automatizmusként fogják betartani és nem mintegy felesleges adminisztratív, gátló munkafolyamatként tekintenek rá. Ebben a körben az adatvédelmi tisztviselő, ha a vállalkozáscsoportnál ilyen személyt kijelöltek, kulcs szerepet játszhat.

A vállalkozáscsoport és a nemzeti hatóság a BCR jóváhagyási eljárása során közvetlen kapcsolatot alakít ki, amely az ügyfélbarát szolgáltató közigazgatás egyik jellemzőjeként tovább növelheti a megfelelési hajlandóságot és a jogkövető magatartást. A BCR létrehozása a tagállami jogalkotási kötelezettségen túl, amely véleményem szerint megvalósulhat az adatvédelmi, illetve a fogyasztóvédelmi és ezzel párhuzamosan a munkajog területén is, új jogi, informatikai és gazdasági szaktudást is igényel, egy új szolgáltató szektor nyerhet létjogosultságot, mind a BCR megalkotása és jóváhagyási eljárásának lebonyolítása, mind monitoring rendszerének működtetése és frissítése körében.

IX.4. A veszélyekre érdemes figyelni – T

A magyar jogrendszer kötelező erejűnek ismeri el az egyoldalú nyilatkozatokat, így azok kikényszeríthetők és végrehajthatók. Tehát ha a BCR-t a vállalkozáscsoport által tett egyoldalú nyilatkozatnak tekintjük, melyben magára nézve kötelezettségeket vállal, akkor kötelező

DOI: 10.14750/ME.2019.022

jellege megkérdőjelezhetetlen. Ha egy adatvédelmi általános szerződési feltételként vizsgáljuk, ami automatikus, a felek erre vonatkozó külön tárgyalása nélkül a szerződés – itt az adattovábbításra és feldolgozásra vonatkozó szerződés – automatikus részévé válik, mert nyilvánosságából adódóan a szerződő felek megismerhetik tartalmát, hozzáférhetnek, így pedig a „pacta sund servanda" szerződésjogi alapelv értelmében köti a feleket. Azonban ha a vállalkozáscsoport tagjai között nincs vagy nem is volt szerződés az adattovábbítás és adatfeldolgozás vonatkozásában, a BCR általános szerződési feltételek jellege nem értelmezhető. Ha kizárólag munkavállalók tekintetében vizsgáljuk a BCR helyzetét, a hazánkban kötelező jellege azzal érhető el legegyszerűbben, ha kollektív szerződés mintájára lesz közvetlenül alanya az adott cég minden munkavállalója. A munkaszerződéssel egyidejű ismertetése pedig eleget tesz a tájékozott információs önrendelkezés bizonyos fokú kielégítésének, tekintettel arra, hogy a munkavállaló a BCR egészét, vagy annak csak nyilvános részét ismerheti-e meg. Ha magatartási kódexként tekintünk a BCR-re, akkor kötelező jellege szempontjából abba a nyilvánvaló ténybe ütközünk, hogy mivel az nem jogszabály, ezért a vállalkozáscsoporton múlik, hogy az önmaga által létrehozott normákat betartja-e, megszegése esetén alkalmaz-e joghátrányt, és kikényszeríthetőségük is vitathatóvá válik.

A folyamatos változás és fejlődés okán, mely jellemzi nemcsak a piacot és így a gazdasági társaságok struktúráját, hanem a jogrendszereket is, a BCR-eket is folyamatosan frissíteni szükséges. Ilyen esetben egy újabb engedélyeztetési eljárás a BCR létrehozásának lényegét oltaná ki, jelesül hogy egyetlen eljárás lebonyolítása elegendő a jövőben az az alapján végrehajtandó cselekmények igazolására és szolgál azokhoz követendő magatartásmintaként.

DOI: 10.14750/ME.2019.022

A frissítés módjának meghatározása tartalmi kérdés, így ezzel részletesen későbbi fejezetekben foglalkozom majd, azonban az már most látható, hogy ha a BCR módosítását a vállalkozáscsoport saját szervezetén belül, vagy azon kívüli, de kijelölt felelős személy hajtja végre és csak periodikusan, esetleges hatósági ellenőrzéssel sem megnyugtató a szabályrendszer valós hatékonysága és jogszabályoknak való megfelelősége.

További veszélyforrás - bár adatkezelői szempontból inkább lehetőség - a jóváhagyás körében a „forum shopping" jelenség lehetősége. A BCR jóváhagyására irányuló hatósági eljárást a vállalkozáscsoport olyan tagállamban indíthatja meg - attól függetlenül, hogy a vezető hatóság kiválasztása szerinti szempontrendszer alapján melyik hatóság előtt kellene[291] -, ahol a nemzeti jogszabályok vagy az eljáró nemzeti hatóság eljárásának, illetve diszkrecionális jogkörének gyakorlása során számára kedvezőbb, gyorsabb döntés születhet. Ez persze csak elvben lehet így, mert a jóváhagyásra irányuló eljárás során minden, az adattovábbítással és feldolgozással érintett nemzeti hatóságnak meg kell küldeni véleményezésre a BCR tervezett szövegét, és a nemzeti hatóságoknak egy hónapon belül kell észrevételeiket megtenniük az engedélyező vezető hatóságnak, amit a vezető hatóság az eljárást megindító ügyféllel közöl. Amennyiben a kérelmező megfelelő intézkedéseket tett az észrevételek vonatkozásában, a BCR végleges szövegét a vezető hatóság ismét megküldi jóváhagyásra minden érintett nemzeti hatóságnak.[292] Mivel minden hatóság saját nemzeti jogszabályi elvárásainak megfelelően vizsgálhatja a BCR tartalmát, így elvben nem lehet eredményes a „forum shopping" alkalmazása sem.

[291] Nem kizárólag a székhely tagállamban indítható jóváhagyás iránti eljárás, melyet más nézőpontból később vizsgálok majd, továbbá a letelepedés szabadságából adódóan ma az uniós tagállamokban nem okozhat jogi problémát a székhelyáthelyezés sem.
[292] WP 107

DOI: 10.14750/ME.2019.022

IX.5. Konklúzió

S10-W16-O10-T5 avagy a SWOT számokban. Ahogyan a fejezet bevezető részében is utaltam rá, maga a tény, hogy melyik rovat hány darab jellemzőt tartalmaz, nem irányadó a BCR megítélésében. Nem mondhatjuk, hogy több a hátrány, mint az előny, tehát a BCR rossz. Azt sem mondhatjuk, hogy sok fejlesztési lehetőség kínálkozik, várjunk a BCR bevezetésével. A jellemzők érdemi, tartalmi összehasonlítása kell, hogy következtetések alapja legyen, azzal a fenntartással, hogy a jogintézmény ténylegese elterjedése a GDPR kötelező alkalmazásának időpontját követően várható.

Az „önszabályozás" ilyen módja azonban csak „kiegészítő eszköz lehet,"[293] hiszen reálisan szemlélve belátható, hogy az elsődlegesen a gazdasági társaság profitszerzését, de legalábbis felmerülő költségeinek megtakarítását célozza, és nem az adatalany adatvédelmi és információs önrendelkezési joga érdekei élveznek prioritás. Olyan döntő súllyal bíró érvek, gyakorlati tények szólnak a BCR ellen, melyet nem kompenzálhatnak elvont, általános érvek és nehezen megvalósítható célok, csakis az elkötelezett jogkövetés. Emellett azonban úgy gondolom, hogy az adatvédelem mellett vitathatatlanul elkötelezett adatkezelők körében és az adatalanyt hatékonyan védő jogi környezetben működőképes, de csak kiegészítő eszköz lehet.

A BCR elsődleges célja, hogy biztosítsa a megfelelő védelmi szintet a vállalkozáscsoport tagjai által végzett, harmadik országba is irányuló adattovábbítások vonatkozásában, de mit érhet a belső szabályzat, ha a nemzeti jog annulálhatja azt. A magánjogi, üzleti viszonyokban azonban kétségtelenül jelentékeny tényező, hiszen olyan államokban működő partnerek szolgáltatásit tudja igénybe venni az adatkezelő, vagy olyan harmadik országban tudja tevékenységét a vállalkozáscsoporton belül végezni, amelyben megfelelőségi határozat hiányában egyébként nem végezhetné jogszerűen.

[293] JÓRI (2009)

DOI: 10.14750/ME.2019.022

A BCR bevezetése rövidtávon időigényes és drága, hosszútávon még nem látni a költséghatékonyságát, kisebb méretű vagy kevés adatforgalmú cégek számára nem optimális. Van viszont két kiemelkedő jellemzője, amely nagyban segíti elterjedését. Az egyik a rugalmas szabályrendszer kialakításának lehetősége, amely a hatósági jóváhagyás eredményeként kvázi biztosítja a cég adatvédelmi megfelelését, hatósági közreműködéssel. A BCR betartása pedig hosszú távon garantálja a jogellenesség hiányát, a bírság elkerülését. A másik, hogy a vállalkozáscsoport aszerint választhatja meg a harmadik országot, ahol működni szeretne, hogy ebben az adatvédelmi szabályok meggátolnák. Saját maga biztosítja a megfelelő védelmi szintet, így politikai hatásoknak[294] sincs kitéve.

Miért érdemes tehát éppen a BCR alkalmazása mellett döntenie a multinacionális társaságoknak?

A vállalatcsoporton belül harmonizálja az adatvédelmi politikát, mivel valamennyi tag köteles betartani a megfogalmazott szabályokat, mindamellett, hogy a BCR létrehozása önkéntes alapon működik főszabályként. Átláthatóvá teszi az adatkezelési műveleteket mind az érintettek, mint a vállalkozáscsoport tagjai számára, tiszta viszonyokat teremt a jogosultságok, a felelősség kérdésében. Az adatvédelem beépül az üzleti, tudatos működésbe, amelyre a GDPR előirányozta bírság maximumokra tekintettel szükség is van.

A BCR rugalmasan alakítható a vállalatcsoport, szektor igényeire, kiegészítve a jogi keretrendszert. Az adatvédelmi szint exportját eredményezi a harmadik országokban működő vállalkozáscsoporti tagokra nézve, amely az érintett számára ugyan nem teljes, de fennálló garanciát jelenthet.

[294] Politikai hatások körében gondolhatunk itt a Safe Harbor-döntés indokolásában foglalt, az USA-val szemben megfogalmazott aggályokra valamint a Privacy Shield létrehozásának és működésének körülményeire.

DOI: 10.14750/ME.2019.022

A BCR alkalmazása – leszámítva az engedélyeztetése és tagállamonkénti jóváhagyása folyamatait – főszabály szerint az adatvédelmi adminisztrációs terhek – például az adattovábbítások hatósági előzetes bejelentének – csökkenését eredményezi. A BCR egyfajta in-house probléma megoldási és panaszkezelési mechanizmust is magában hordoz, önkéntes létrehozása pedig a cégek megfelelésre való hajlandóságát növeli.

DOI: 10.14750/ME.2019.022

X. FEJEZET
AZ USA MINT HARMADIK ORSZÁG SPECIÁLIS HELYZETE

"A 2000/520 határozat érvénytelen."[295] A Schrems-ügyben meghozott határozatával az Európai Unió Bírósága megsemmisítette azt az Európai Bizottság által hozott határozatot, amely megteremtette az USA-ba mint harmadik országba irányuló adattovábbításokhoz szükséges, a megfelelő védelmi szint biztosítását szolgáló keretrendszert. Több, a döntést megalapozó indok közül a legjelentősebb az USA az európai adatvédelmi joggal össze nem egyeztethető gyakorlatának megítélésén alapult, azaz azon, hogy a szövetségi állami szervek és ügynökségek az USA-ba továbbított személyes adatokhoz szinte korlátlanul hozzáférhettek, míg az uniós polgároknak nem voltak ténylegesen érvényesíthető jogaik ezen eljárásokkal szemben. Az USA mint harmadik ország nem minősült megfelelő védelmi szintet biztosító országnak és a Safe Harbor rezsimhez önként csatlakozó vállalkozások sem voltak képesek a gyakorlatban a megfelelő védelmi szint garantálására.

Tényleges - állami, hatósági - felügyelet hiányában, az érintetti jogok csupán elméleti, névleges biztosítása és a vállalkozások visszaélései indukálták azt a döntést, amellyel a Safe Harbor határozatot[296] érvénytelenné nyilvánították. Meg kell jegyeznem, a határozat nem volt az Adatvédelmi Irányelv 26. cikk (6) bekezdése szerinti megfelelőségi határozat, mert nem mondta ki az Európai Bizottság, hogy az USA megfelelő védelmi szintet biztosít, helyette létrehozott egy önkéntesen alkalmazható tanúsítási rendszert.

---

[295] C-362/14. sz. ügy Maximillian Schrems kontra Data Protection Commissioner, ECLI:EU:C:2015:650 106.
Az ügyet ebben a fejezetben részletesen is ismertetem abból a szempontból, hogy milyen hatása volt a harmadik országba irányuló, különösen az USA-ba továbbítandó személyes adatok továbbítások szabályrendszerére.

[296] 2000/520/EK bizottsági határozat, A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről, Hivatalos Lap L 215 , 25/08/2000 o. 0007 - 0047

DOI: 10.14750/ME.2019.022

Azok az USA-ban letelepedett vállalkozások, amelyek a rendszerhez csatlakoztak, olyannak minősültek, amelyek mint adatkezelők vagy adatfeldolgozók biztosítják a megfelelő védelmi szintet.

Ezen túl persze más módon[297] is biztosítható volt a megfelelő védelmi szint, a Safe Harbor-hoz hasonló szövetségi szintű ernyő-megoldás hiányában azonban az egyedi megoldások – a szerződéses modell klauzulák és a BCR - kerültek előtérbe.

Igaz ugyan, hogy az azóta felállított és 2016. augusztus 1. napjától aktív Privacy Shield rendszer[298] a Safe Harbor rezsim hiányosságait hivatott orvosolni és pótolni hasonló önkéntes csatlakozási illetve tanúsítási módszer alkalmazásával, ám az első éves értékelése mégis azt mutatja, hogy bevezetésével az érintetti jogérvényesítés lehetősége és a védelem valós biztosítása korántsem megfelelő.[299]

Ebben a fejezetben azt vizsgálom, hogy a Safe Harbor rendszere illetve a Privacy Shield rezsim működése hátrányosabb-e attól, ha a vállalkozáscsoport BCR alapján végzi adatkezelési és adattovábbítási tevékenységét az USA-ban működő tagjuk irányában. E vizsgálódásomat arra szűkítem le, hogy a BCR jogi természete előnyösebb-e, és ha igen, mennyiben a két öntanúsítási rendszer alkalmazásánál.

[297] Például az Európai Bizottság által megalkotott szerződéses klauzulák alkalmazásával.
[298] A BIZOTTSÁG (EU) 2016/1250 VÉGREHAJTÁSI HATÁROZATA (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről HL L 207., 2016.8.1., 1—112. o.
[299] Európai Bizottság: Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, {SWD(2017) 344 final}, Brussels, 18.10.2017 COM(2017) 611 final

DOI: 10.14750/ME.2019.022

X.1. Biztonságos kikötő és a viharos vizek

Minden adatkezelőnek és adatfeldolgozónak tiszteletben kell tartania az érintett személyes adatok védelméhez való jogát, így a megfelelő védelmi szintet nem biztosító harmadik országokba adattovábbítások nem végezhetők. A legnagyobb gazdasággal bíró harmadik országokban az adatkezelési tevékenységek tényleges állami felügyeletének elmaradása és a magánszférára is kiterjedő átfogó adatvédelmi jogi környezet hiánya indokolja, hogy az európai jogalkotónak kell intézkednie annak érdekében, hogy az európai polgárok személyes adatai a megfelelő védelemben részesüljenek.[300] Ezt a GDPR segítségével a jogalkotó akként éri el, hogy extraterritorriális hatása révén exportálja egyes szabályainak kötelező erejét a harmadik országokban működő adatkezelőre is[301] úgy, hogy a GDPR 44. cikke rögzíti az Adatvédelmi Irányelvhez hasonló implicite tilalmat azon adattovábbítások vonatkozásában, amelyek címzettje nem biztosítja a megfelelő védelmi szintet.

Az Adatvédelmi Irányelv 25. cikkében foglalt alapszabály deklarálta, hogy személyes adatok csak akkor továbbíthatók harmadik országba, ha az adott harmadik ország megfelelő védelmi szintet tud biztosítani.
A jól ismert Lindqvist-ügy precedensszerű ratio decidendi tétele a jogi helyzetet akként fejlesztette tovább, hogy megállapította, hogy a külföldi adattovábbításnak nincs egzakt fogalma.

Tartalmi jogfejlesztést legközelebb C-362/14. számú, közismert néven Schrems-ügyben végzett az Európai Unió Bírósága. Az ítélet 73. és 74. pontja nyújt támpontot arra vonatkozóan, hogy a „megfelelő védelmi szint” a gyakorlatban mit jelent: nem követelhető meg, hogy a harmadik ország az uniós jogrendben biztosított védelmi szinttel megegyező védelmi szintet biztosítson, de azt megköveteli, hogy e harmadik ország – belföldi joga, vagy

[300] KAMARINOU (2013)
[301] KUNER (2015),
A GDRP hatályáról és az alkalmazandó jogról részletesen lásd a IV. fejezetben.

DOI: 10.14750/ME.2019.022

vállalt nemzetközi kötelezettségei alapján – az Unióban […] biztosított védelmi szinttel *lényegében azonos* védelmi szintet biztosítson ténylegesen […]. Az alkalmazott jogi eszközök eltérhetnek, de a gyakorlatban hatékonynak kell lenniük.

Az USA vonatkozásában az Adatvédelmi Irányelv 26. cikk (6) bekezdése szerinti megfelelőségi határozat nem volt hatályban, hiszen mint harmadik ország nem is biztosította a megfelelő védelmi szintet, de a Safe Harbur határozattal egy olyan tanúsítás-szerű rendszert hozott létre, amely alkalmas az egyes vállalkozások adatkezelési tevékenysége vonatkozásában megállapítani a megfelelő védelmi szint biztosítását. Azonban a határozat hatályba lépésétől éles viták kísérték működését és az érvénytelenítését megelőző időszakban különösen éles kritika érte a teljes adatvédelmi gyakorlatot, illetve annak tulajdonképpen teljes hiányát.

Az USA adatvédelmi és magánéletvédelmi politikája közismerten a mélyebb társadalmi, kulturális és jogi különbözőségek miatt már alapjaiban is eltér az európai szemlélettől.[302] A privacy védelem vitathatatlanul mind az amerikai common law típusú, mind az európai kontinentális jogrendekben a nagy hatású Warren-Brandeis-féle értelmezésből ered, de a jogfejlődés és az annak alapjául szolgáló társadalmi viszonyok két rendkívül eltérő rezsimet eredményeztek. Míg az európai jogrendszerekben átfogó jogi szabályozások vannak hatályban mind átalános, mint szektorális szinten, addig az amerikai rezsimben jellemzően az egyes szektorális jogterületek ad hoc rendelkezései vonatkoznak adatvédelmi kérdésekre. A common law alapján a magánjogi jogviszonyokban érvényesülő magánszférához való jog az Egyesült Államokban nem a szövetségi Alkotmányon, hanem a bírói ítéleteken és az egyes államok törvényein nyugszik.[303] Adatvédelmi jellegű kérdéseket szabályoz például a bankjog, a gyermekek online tevékenységével kapcsolatos joganyag, a közvetlen üzletszerzés, a fogyasztóvédelem, éppen

[302] PELTZ-STEELE (2015)
[303] SIMON (2007) p. 41.

DOI: 10.14750/ME.2019.022

ezért az adatvédelmi szabályozás nem szisztematikus, integrált, inkább csak részleges, mint szektorális.[304] Az európai rezsimben alkotmányos alapjogként tételezett a személyes adatok védelméhez való jog, az amerikai álláspont ezzel szemben három másik alapvető joghoz kapcsol adatvédelmi kontextust: ezek a személyes autonómia, az „egyedül hagyatáshoz" való jog és az információs privacy. Míg az amerikai álláspont szerint a magánélet eredője a (szellemi) tulajdon és a szerződés, amely az érintettől valamelyest elidegenített, addig az európai hozzáállás szerint a személyes adat a személyiség része.[305] A felügyelő hatóság az európai rezsimben átfogó hatósági jogkörökkel bír és bírságolási joga is van, ezzel szemben az amerikai állami szervek különböző szektorális területeken, eltérő modellben, különböző hatáskörrel és alkalmazható jogi eszközökkel járnak el. A szövetségi Magánéletvédelmi törvény (1974) nem alkalmazható gazdasági szereplőkre, annak elsődleges célja, hogy védelmet nyújtson az érintettek számára a szövetségi szervek adatgyűjtése ellen. Sokkal enyhébb a szabályozási szemlélete az európainál még úgy is, hogy törvény korlátozza az adatok nyilvánosságra hozatalát, az érintetteknek hozzáférési és helyesbítéshe való jogot biztosít, valamit létrehozza a „fair információs gyakorlatot".[306]

Erős tradíciója van viszont az önszabályozásnak, amelyet előszeretettel részesítenek előnyben a vállalkozáscsoportok az állami szabályozással szemben,[307] azt azonban mára tudhatjuk, hogy a Safe Harbor rezsimet leszámítva, amelyet erős állami támogatás övezett, a legtöbb önszabályozási rendszer hamar elbukott.[308] Ennek ellenére az európai adatvédelmi jogalkotás tendenciája éppen erre, az önszabályozás és a tanúsítás ösztönzése irányában erősödik,[309] amely álláspontom szerint – amerikai példával ellentétben - az európai adatvédelmi jogi keretek, jó gyakorlatok és hozzáállás mellett

[304] SZIGETI (2009) p. 159-165.
[305] PELTZ-STEELE (2015) p. 25.
[306] United States Department Of Justice: Overview Of The Privacy Act Of 1974, 2015 Edition https://www.justice.gov/opcl/file/793026/download (2018.03.11.)
[307] SZŐKE (2015) pp. 52-54.
[308] WRIGHT-DE HERT (2016)
[309] SZŐKE (2015) p. 92-115.

DOI: 10.14750/ME.2019.022

valószínűleg eredményesebb lehet. Értem ez alatt mindazokat a tényezőket, amelyek alapjaiban megkülönböztetik az európai adatvédelmi rezsimet az amerikaitől, vagyis az erős állami felügyeletet, az átfogó szabályozást és az adatkezelők és adatfeldolgozók tudatosságát, végezetül az állam általi cél és korlátok nélküli adatgyűjtés régóta[310] fennálló tilalmát.

Annak érdekében tehát, hogy az USA-ba irányuló adattovábbítások jogszerűek lehessenek, az Európai Bizottság 2000. július 26-i 2000/520/EK határozata[311] a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről döntött. Ezzel a döntéssel az Európai Unió elismerte, hogy az USA-ban működő és a Safe Harbor keretrendszerhez csatlakozó vállalkozásoknak jogszerűen továbbítható személyes adat az Európai Unióból, mert azok megfelelő védelmi szintet biztosítanak.

A Safe Harbor keretrendszerhez csatlakozó vállalkozásoktól az Egyesült Államok Kereskedelmi Minisztériuma által 2000. július 21. napján kiadott hét alapelv és a gyakran felvetőtő kérdésekre adott válaszokban foglaltak betartását várták el. Ez a fajta öntanúsítási módszer alkalmazása önkéntes alapon történt.

[310] Portugáliában 1976-tól tilos országosan egységes személyi szám hozzárendelése az állampolgárokhoz, a német Szövetségi Alkotmánybíróság pedig 1969-ben mondta ki, a „polgárok teljes személyiségét érintő regisztrálása és katalogizálása" az emberi méltósággal összeegyeztethetetlen, hazánkban a 15/1991. (IV. 13.) AB határozat rögzítette, hogy a személyi szám egyes állami szerveknél kötelező, másoknál lehetséges korlátlan használata alkotmányellenes. ABH 1991/40, Budapest, 1991.04.09.
[311] HL L 215., 2000.8.25., 7. o.

DOI: 10.14750/ME.2019.022

X.1.1. Alapelvek

A "biztonságos kikötő" adatvédelmi alapelvek a következők voltak:

- tájékoztatás és értesítés: a vállalkozásoknak tájékoztatnia kell az egyéneket az adatgyűjtés céljairól, a kapcsolatfelvétel és a panaszkezelés módjáról, a harmadik személyek típusairól, amelyek részére az adatokat továbbítják valamint azokról a korlátozási lehetőségekről, amelyeket a vállalkozás biztosít az érintett számára az adatai felhasználásának és nyilvánosságra hozatalának körében. A tájékoztatást világos és érthető megfogalmazásban kell megadni minden esetben az adatkezelést megelőzően.

- választási lehetőség: opt out jogot kell biztosítani az érintetteknek arra, hogy személyes adataikat a vállalkozás átadhatja-e harmadik személynek vagy felhasználhatja-e olyan célra, amely nem összeegyeztethető az adagyűjtés eredeti céljával.

- adattovábbítás harmadik fél részére: ahhoz, hogy a személyes adatot harmadik fél számára átadhassák, a vállalkozásnak alkalmaznia kell az értesítés és a választási lehetőség elveit a fentiek szerint.

- adatbiztonság: a vállalkozásnak meg kell óvnia a személyes adatot az elvesztéstől, a hibás felhasználástól és a jogosulatlan hozzáféréstől, a nem megengedett nyilvánosságra hozataltól, a jogosulatlan megváltoztatástól és a jogosulatlan megsemmisítéstől.

- adatintegritás: a személyes adatoknak azokra a célokra kell vonatkoznia, amelyre azt fel kívánják használni, kizárólag a puszta gyűjtés céljaival vagy az egyén által a későbbiekben engedélyezett célokkal összeegyeztethetetlen módon adatkezelés nem történhet, megfelelő lépéseket kell tenni annak biztosítására, hogy az adatok a tervezett felhasználás szempontjából megbízhatók, pontosak, teljesek és időszerűek legyenek.

DOI: 10.14750/ME.2019.022

- hozzáférés: az érintett számára biztosítani kell, hogy hozzáférhessen a vállalkozás birtokában lévő, rá vonatkozó személyes adatokhoz, biztosítani kell továbbá a helyesbítéshez, módosításhoz és törléshez való jogát. Kivétel ezen jogok gyakorlása alól, ha az adott esetben a hozzáférés biztosításának terhe vagy költsége nem állna arányban az egyén adatvédelmi jogának korlátozásával, vagy ha ezzel más személy jogait érné sérelem.

- végrehajtás, kikényszerítés: az elvek betartását biztosító mechanizmusokat, a jogorvoslati jogot kell biztosítani, kellően szigorú szankciórendszerrel.

Megállapítható, hogy a fenti elvek tartalmuk szerint *egybeesnek* az Adatvédelmi Irányelv által deklarált alapelvekkel, tehát a vállalkozások a tanúsítással azt vállalták, hogy betartják az európai elveket, amelyre tekintettel az Európai Unió elismeri a rendszer és a csatlakozó vállalkozások által biztosított adatvédelmi szintet megfelelőként.

X.1.2. Gyakran Felvetődő Kérdések

A Gyakran Felvetődő Kérdések (a továbbiakban: GYFK), amelyeknek kötelező ereje volt, olyan kérdésekkel foglalkoztak, amelyeket a határozatban foglalt válaszok szerint kell megoldani. Ilyenek például a mögöttes felelősség kérdése vagy a hozzáférési elv tényleges tartalma és korlátai. A Safe Harbor szerinti tanúsításhoz két konjunktív feltételt írt elő a határozat. Az 1. cikk (2) bekezdése értelmében az adatokat fogadó szervezetnek egyértelműen és nyilvánosan ki kell nyilvánítania a GYFK-val összhangban bevezetett elvek teljesítésére vonatkozó kötelezettségvállalását. Továbbá a vállalkozásnak valamely, a Safe Harbor határozatban felsorolt egyesült államokbeli kormányzati szervnek a törvényben meghatározott hatásköre alá kell tartoznia.

DOI: 10.14750/ME.2019.022

A kormányzati szerint így jogosulttá vált az elvek be nem tartása esetén az érintettek által benyújtott panaszok kivizsgálására, valamint a vállalkozást a tisztességtelen vagy megtévesztő gyakorlata miatt kártérítésre kötelezni.

A Safe Harbor szerinti tanúsítás önkéntes, tehát a vállalkozások szabadon dönthettek arról, hogy csatlakoznak-e a keretrendszerhez. 2015 év közepéig több, mint 5500 vállalkozás vállalta, hogy biztosítja a megfelelő védelmi szintet a Safe Harbor elvek betartásával,[312] például az Apple Inc., a Hewlett Packard Enterprise Company és amerikai leányvállalatai és a Facebook Inc. is.

A Szövetségi Kereskedelmi Bizottság (Federal Trade Commission, a továbbiakban: FTC) hatásköre volt, hogy gondoskodjon a beérkező panaszok elbírálásáról, hogy megtiltson bizonyos tevékenységeket. Azonban a keretrendszer leginkább csak deklaratív és önkéntes jellege miatt az elvek tényleges betartása és a vállalkozások olykor átláthatatlan adatkezelési tevékenysége aggályokat vetett fel. Első hivatalos kritikák csak 2013 júliusában jelentek meg,[313] ám már azok egyértelművé tették, hogy az amerikai adatvédelmi standardok elmaradnak az európaitól, ezért Reding[314] alelnök arra hívta fel az Európai Bizottságot, hogy még abban az évben vizsgálja meg a Safe Harbor működését. A viták során kibontakozott legfőbb érvek arról szóltak, hogy az amerikai állami szervek a PRIMS hírszerző programmal olyan adatokhoz férhetnek hozzá tömegesen és korlátok nélkül, amelyek gyűjtésére és tárolására nem volt megfelelő jogalapjuk és a megfigyelés aránytalan mértékű volt. Megjegyzem, a magánszférához való jog nem vonatkozott a kormányzattal szembeni jogérvényesítésre,[315] azt az USA alkotmánya sem tartalmazza.

[312] https://safeharbor.export.gov/list.aspx [2015. június 15.]
[313] Európai Bizottság: Informal Justice Council in Vilnius – Memo http://europa.eu/rapid/press-release_MEMO-13-710_en.htm [2017. november 20.]
[314] Az Európai Bizottság alelnöke, uniós jogérvényesülési biztos.
[315] SIMON (2007) p. 41.

DOI: 10.14750/ME.2019.022

Tehát a nemzetbiztonsági és bűnüldözési indokok mellett az alapvető elvi megfontolás sem mondott ellent a kialakult gyakorlatnak.

A Safe Harbor nem vonatkozott az állami szervek adatgyűjtési tevékenységére, a vállalkozások felé irányuló adatkéréssel – és azok a vállalkozások általi teljesítésével – pedig az elvek érvényesülésének teljes ellehetetlenülését érték el. A vállalkozások sorozatosan mulasztották el egyébként is az elvek betartását, az uniós polgárok pedig nem élveztek az amerikaiakéval azonos jogokat és eljárási biztosítékokat.

Az Európai Bizottság közleményeiben[316] hivatalosan is megállapította ezen aggályokat, és amellett, hogy rögzíti, hogy az új kérdéseket meg kell válaszolni, a meggyengült bizalmat helyre kell állítani, sőt kimondja, hogy a Safe Harbor alapvető kérdései felülvizsgálatra szorulnak, a tényleges reformok szükségessége ellenére, amelyekre egyébként a határozat 4. cikke értelmében – „ez a határozat bármikor kiigazítható a végrehajtásával kapcsolatos tapasztalat fényében" – bármikor lehetősége lett volna, mégsem tett erőteljesebb lépéseket. Az Európai Unió Állampolgári Jogi, Bel- és Igazságügyi Bizottsága[317] még ugyanebben az évben megfogalmazta, hogy „ragaszkodik a szükséges reformok elvégzéséhez és az európaiak számára tényleges garanciák nyújtásához annak biztosítására, hogy a külföldi hírszerzési célokat szolgáló megfigyelés és adatfeldolgozás arányos legyen".[318] Felszólította a tagállamokat arra, hogy tiltsák be vagy függesszék fel a harmadik országokba irányuló, többek között BCR-n alapuló adattovábbításokat is, ha azok teljesítése esetén várható, hogy a címzett adatkezelőre vagy adatfeldolgozóra irányadó jog olyan követelményeket támaszt, amelyek túllépik a demokratikus társadalomban szigorúan szükséges, megfelelő és arányos korlátozásokat."

[316] Communication COM(2013) 846 final, Communication COM(2013) 847 final
[317] Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, (2013/2188(INI))
[318] i.m. 116. pont.

DOI: 10.14750/ME.2019.022

Ugyanakkor a jelentés azt is kiemeli, hogy „még ha megerősítést is nyernek egyes hibák vagy jogellenes tevékenységek, azokat egyensúlyba kell hozni az USA és Európa közötti különleges kapcsolat fenntartásának szükségességével.” Az alapjogi aggályok és a pozitív jogi teendők politikai színezetet kaptak. Az FTC a bírálatok hatására intenzív ellenőrzésekben kezdett, számos hiányosságot, félrevezető adatkezelői magatartásokat tárt fel, amely vizsgálatok bírságolással és adatvédelmi kötelezettségek kötelező vállalását tartalmazó egyezségekkel zárultak.[319]

X.2. A Schrems-ítéletről

A fejezet eddigi része tulajdonképpen már a jogtörténeti bemutatás része is lehetne, tekintettel arra, hogy az Európai Unió Bírósága a C-362/14 számú ügyben hozott határozatával (a továbbiakban: Ítélet) a Safe Harbor rendszert deklaráló Európai Bizottsági határozat érvénytelenségét állapította meg.

X.2.1. Az ügy tényei, a pertörténet

Egy Ausztriában élő osztrák állampolgár panaszt nyújtott be a tagállami adatvédelmi biztoshoz, amelyben kérte, hogy tiltsa meg a Facebook Ireland számára a személyes adatai továbbítását az Egyesült Államokba. Hivatkozott arra, hogy az USA mint harmadik ország hatályos joga és gyakorlata nem biztosít megfelelő védelmet a hatóságok által folytatott megfigyelési tevékenységekkel szemben. Az adatvédelmi biztos úgy ítélte meg, hogy nem köteles a panaszban megjelölt tényeket kivizsgálni, ezért elutasította azt mint jogilag megalapozatlant, mivel az aggályokat a panaszos nem bizonyította. A határozattal szemben a panaszos bírósághoz fordult, amely megállapította, hogy az adattovábbítások elektronikus megfigyelése és lehallgatása szükségszerű és alapvető közérdekű célokat szolgált.

[319] DOMONKOS-POLEFKÓ (2015) p. 124-125.

DOI: 10.14750/ME.2019.022

Azonban megállapította azt is, az uniós polgárok nem rendelkeznek tényleges jogorvoslati joggal e körben. Az ítéletben rögzítette a bíróság, hogy az ír jog tiltja a személyes adatok államterületen kívüli továbbítását, kivéve ha az adott harmadik ország megfelelő szintű védelmet biztosít. A személyes adatokhoz való tömeges és válogatás nélküli hozzáférés - ahogyan az USA is eljárt - nyilvánvalóan ellentétes az arányosság elvével és az ír alkotmány által védelemben részesített alapvető értékekkel. Az eljáró bíróság rámutatott, hogy a panaszos a keresetében valójában a Safe Harbor határozattal létrehozott rendszer jogszerűségét vitatja, ezért előzetes döntéshozatal céljából az Európai Unió Bíróságához fordul. Tehát noha a Safe Harbor határozatot formálisan nem tette vitássá a panaszos, mégis az volt az alapkérdés, hogy a tagállami felügyelő hatóságok – legyen az akár hatósági formában működő, akár ombudsman-like szerv vagy személy – saját nyomozása alapján jogosult-e megállapítani azt, hogy egy harmadik ország nem biztosítja a megfelelő védelmi szintet akkor, ha egyébként arra uniós jogforrás – Európai Bizottsági határozat – van hatályban.

X.2.2. A döntés

Az alapvetés az, hogy az adatvédelmi rendelkezéseket szükségszerűen az Alapjogi Chartában biztosított alapvető jogok fényében kell értelmezni. Azonban "amíg a Bíróság nem állapítja meg a Bizottság határozatának érvénytelenségét,[320] a tagállamok és a szerveik, köztük a független felügyelő hatóságaik, kétségkívül nem fogadhatnak el e határozattal ellentétes olyan intézkedéseket, mint az annak kötelező erejű megállapítására irányuló jogi aktusok, hogy az a harmadik ország, amelyre az említett határozat vonatkozik, nem biztosít megfelelő védelmi szintet."[321]

[320] Az érvénytelenség megállapítására kizárólag az Európai Unió bírósága jogosult (Ítélet 61. pont)
[321] Ítélet 52. pont

DOI: 10.14750/ME.2019.022

Ugyanakkor "a nemzeti felügyelő hatóságoknak jogosultnak kell lenniük arra, hogy teljes függetlenséggel megvizsgálják, hogy ezen adattovábbítás tiszteletben tartja-e az említett irányelvben támasztott követelményeket"[322] és azt, hogy a "harmadik országban hatályos jog és gyakorlatok nem biztosítanak megfelelő védelmi szintet."[323]

Az Ítélet kiemeli azt is, hogy a Safe Harbor elvek I. mellékletének negyedik bekezdése értelmében korlátozhatók, különösen a „nemzetbiztonság, a közérdek vagy a bűnüldözés követelményei" érdekében, amelyek megelőzik az érintett személyes adatai védelméhez fűződő jogát.

Az Európai Bizottság korábbi értékeléséből idézi az Ítélet, hogy az érintetteknek nem volt sem hatósági, sem bírói jogorvoslati lehetőségük az állami megfigyeléssel szemben, noha a személyes adatokat a továbbításuk céljaival össze nem egyeztethető módon, valamint a nemzetbiztonság védelméhez feltétlenül szükséges és azzal arányos mértéket meghaladóan kezelhették az amerikai hatóságok. Az Európai Unió Bírósága tartalmában nem is vizsgálta a Safe Harbor elveket, azok érvénytelenségét mondta ki.

X.2.3. A döntés hatása

A döntés fontos következményekkel járt. *Egyrészt* minden olyan az USA-ba irányuló adattovábbítás, amely a Safe Harbor határozat alapján tanúsított vállalkozásokhoz irányult, ezentúl *nem volt jogszerű*, mert a megfelelő védelmi szint nem volt biztosítottnak tekinthető.

Másrészt az Ítélet azt is kimondta, hogy *a tagállami adatvédelmi felügyelő hatóságok jogosultak vizsgálni az olyan adattovábbítások esetén is* a harmadik ország megfelelő védelmi szintjét, amely államok vonatkozásában

[322] Ítélet 57. pont
[323] Ítélet 66. pont

DOI: 10.14750/ME.2019.022

megfelelőségi határozat van hatályban. Ennek következtében, az eddig legerősebbnek ítélt garancia – a megfelelőségi határozat – *elveszítette „sérthetetlen" jellegét*. Álláspontom szerint ez a döntés erősítette meg azt a vállalkozói magatartást is, amely a jövőben az adattovábbításai jogszerűségének biztosítását és megítélését saját egyedi jogi eszközt alkalmazásával éri el, és nem a jogalkotótól és a politikai viszonyoktól függő megoldásra alapít.

Harmadrészt a döntésből implicite az is következik, hogy az adattovábbítás jogszerűségét - az Adatvédelmi Irányelv 26. cikk (1) bekezdésében foglalt kivételeken túl - a jövőre nézve a modellklauzulák és a BCR biztosíthatta a vállalkozáscsoportok számára, azonban ezek megfelelőségét is az USA jogi környezetére tekintettel megkérdőjelezhetőnek találták.[324] Így az ítélet az európai vállalkozások helyzetét nehezítette meg, mert felül kellett vizsgálniuk valamennyi adatkezelési, felhő-alapú szolgáltatásra igénybe vételére irányuló vagy adatfeldolgozásra irányuló szerződésüket és szerződéses partnerükre, és mára a GDPR hatására is tekintettel szerver-telepítésekbe is kezdtek az uniós tagállamokban.[325]

Az ítéletet követően az Európai Bizottság,[326] a 29. cikk szerinti adatvédelmi munkacsoport[327] és a tagállami adatvédelmi hatóságok[328] sorra hozták

[324] DOMONKOS-POLEFKÓ (2015) p. 131.
[325] BAUER-LEE-MAKIYAMA-VAN DER MAREL-VERSCHELDE (2016) Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, Erik van der Marel: Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, European Centre for International Political Economy, No. 03/2016, http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf [2018. június 01.]
[326] A Bizottság Közleménye az Európai Parlamentnek és a Tanácsnak a 95/46/Ek Irányelv alapján, az Európai Bíróság C-362/14. Sz. (Schrems-) ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52015DC0566&from=EN
[2017. november 10.]
[327] Statement of the Article 29 Working Party http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf,
Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf
[2017. november 10.];

DOI: 10.14750/ME.2019.022

nyilvánosságra álláspontjukat, az azonban közös volt mindegyikben, hogy a mielőbbi megoldás megalkotására sürgették az uniós jogalkotót. Az ítélet kapcsán is felmerül az az alapvető kérdés is, hogy az Európai Unió Bírósága helyesen járt-e el akkor, amikor olyan döntést hozott, ami "már nem jogalkalmazói, hanem inkább jogalkotói felelősség kérdése"[329] és nem lett volna-e helyesebb, ha az évekkel korábban megfogalmazott komoly aggályok feloldására az érintett szakpolitikai szervek vagy az Európai Bizottság *kezdeményezte volna a Safe Harbor felülvizsgálatát*. Megjegyzem, ekkor már az európai adatvédelmi reform és a GDPR megalkotása is folyamatban volt, tehát okszerűen kezdeményezhető lett volna a szabályok újragondolása.

Domonkos és Polfekó[330] azon az álláspontonvolt, hogy az adattovábbítások esetén célszerű volna az egyedi, konkrét adatkezeléseket megvizsgálni, mindemellett a BCR-k alapján történő adattovábbításokat megkérdőjelezhetőnek vélik. Az én álláspontom szerint, ha egyetértünk azzal, hogy a konkrét adatkezelések vizsgálata során a jogszerűség megállapítható, akkor a BCR-n alapuló adattovábbítás esetében is el kell azt fogadnunk.

Ugyanis a BCR, amelyet előzetesen a tagállami hatóságok jóváhagytak, minden egyes egyedi adattovábbításra szabályozást állít fel. Ha azon az alapon kérdőjelezzük meg az adattovábbítás jogszerűségét, hogy a harmadik ország nemzeti joga kollízióba kerül a BCR szabályaival és a vállalkozás a BCR-rel ellentétesen a nemzeti jog szerint jár el, akkor a *BCR ugyanúgy hatástalan, mint bármely más jogi eszköz*.

Azt azonban meg kell jegyezni, hogy egyre több vállalkozás tagadja meg az adatok kiadását állami adatkérések esetén arra hivatkozással, hogy az európai jogszabályok, belső szabályzataik, tanúsításaik vagy éppen üzletpolitikájuk

[328] Többek között a portugál, a spanyol, az Egyesült Királyság-beli, és a magyar NAIH is.
[329] DOMONKOS-POLEFKÓ (2015) p. 126.
[330] DOMONKOS-POLEFKÓ (2015) p. 131.

DOI: 10.14750/ME.2019.022

elveivel volna az ellentétes.[331] Ez pedig felveti annak a kérdését, hogy az állam vajon jogosult-e olyan szabályozás kialakítására vagy olyan jogalkalmazási gyakorlat bevezetésére, hogy bizonyos szektorok szereplői, például a kommunikációs eszközök gyártói kötelesek lesznek „hátsó ajtót", azaz hozzáférést biztosítani az eszközeikhez, például bűnmegelőzési vagy bűnüldözési célból. Ha igen, akkor pedig adódik a kérdés, hogy meddig terjedhet az állami hozzáférés arányos és szükséges mértéke. [332]

X.3. A Privacy Shield napjainkban

Az uniós jogalkotó megtalálta a megoldást az égető problémára még 2016-ban, megszületett az adatvédelmi pajzs[333] (a továbbiakban: Adatvédelmi Pajzs), amely olyan tanúsítási rendszer, amelyben az USA-ban működő vállalkozások kötelezettséget vállalnak arra nézve, hogy betartják az adatvédelmi keret- és kiegészítő elveket.

Az Egyesült Államok Kereskedelmi Minisztériuma bocsátotta ki azokat az elveket, amelyeket az Európai Bizottság jóváhagyott, és amelyek betartásával a megfelelő védelmi szint biztosítható. Az elvek egyik csoportja tartalmazza az általános, minden adatkezelőre kiterjedő szabályokat, míg a kiegészítő elvek szektorális vagy részletkérdésekről rendelkeznek.

[331] Az egyik legismertebb esetben az Apple Inc. az IPhone gyártója tagadta meg a FBI felhívását arra, hogy hozzáférést biztosító szoftvert készítsen egy bűncselekményt elkövető személy telefonjához. Az FBI végül egy harmadik személy által kifejlesztett szoftvert használt fel. Az eset jogi megítéléséről részletesen: Muzamil Riffat: Legal Aspects of Privacy and Security: A CaseStudy of Apple versus FBI Arguments, SANS Institute InfoSec Reading Room, https://www.sans.org/reading-room/whitepapers/legal/legal-aspects-privacy-security-case-study-apple-fbi-arguments-37037 [2018. június 23.]

[332] RIFFAT (2018)

[333] A Bizottság (Eu) 2016/1250 Végrehajtási Határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről HL L 207., 2016.8.1., 1—112. o.

DOI: 10.14750/ME.2019.022

X.3.1. Az alapelvek

Az általános alapelveket az alábbiak szerint deklarálja az Adatvédelmi Pajzs:

- **tájékoztatás:** a vállalkozások kötelesek az érintetteket a személyes adataik kezelésével kapcsolatos lényeges elemekről tájékoztatni, kötelesek nyilvánosságra hozni adatvédelmi szabályzatukat, a Kereskedelmi Minisztérium weboldalán elérhető listájára és egy megfelelő alternatív vitarendezési szolgáltatóra mutató linket is közzé kell tenniük.

- **választási lehetőség**: opt out jogot kell biztosítani az érintettnek arra az esetre, ha személyes adatait az eredetitől eltérő célja kívánják felhasználni.

- **elszámoltathatóság a harmadik fél részére történő adattovábbításért**: harmadik fél részére történő adattovábbításra meghatározott célokból, szerződés alapján kerülhet sor, ha a szerződés azonos szintű védelmet biztosít akként, hogy az tiszteletben tartandó elvek csak nemzetbiztonsági, bűnüldözési és egyéb közérdekű célok eléréséhez szükséges mértékben korlátozhatók. Az azonos szintű védelem biztosításának kötelezettsége valamennyi harmadik félre vonatkozik, függetlenül attól, hogy az az USA-ban vagy más harmadik országban működik-e.

- **biztonság**: a vállalkozásoknak „indokolt és megfelelő” biztonsági intézkedéseket kell hozniuk az adatbiztonság kérdésében.

- **adatok sértetlensége és célhoz kötöttség**: megerősíti az adatminimalizálás és az adatminőség elvét, azaz az adatkezeléssel érintett személyes adatok körét az adatkezelés célja szempontjából releváns mértékre kell korlátozni, az adatoknak megbízhatónak, pontosnak, teljesnek és időszerűnek kell lenniük.

DOI: 10.14750/ME.2019.022

A személyes adatok az érintettel összekapcsolható módon csak addig őrizhetők meg, amíg az eredeti célból kezelik őket, vagy amely célokat utóbb engedélyezett az érintett.

- **hozzáférés**: az érintettnek joga van arra, hogy indokolási kötelezettség nélkül és ésszerű díj ellenében megismerhesse, hogy az adott vállalkozás kezel-e rá vonatkozó személyes adatokat, és az adatkezelés tényét valamint az adatokat ésszerű időn belül kell közölni az érintettel. E jog korlátozása csak kivételes körülmények között engedhető meg. Az érintettnek joga van kérni adatai helyesbítését, módosítását illetve törlését is.

- **jogorvoslat, végrehajtás és felelősség**: szigorú mechanizmusokat kell biztosítani annak érdekében, hogy a vállalkozások megfeleljenek az elveknek és hatékony jogorvoslati lehetőséget biztosítsanak az érintetteknek. Rögzíteni kell, hogy az FTC, a Közlekedési Minisztérium vagy bármely más, erre feljogosított egyesült államokbeli állami szerv vizsgálati és jogalkalmazási hatáskörébe tartozik az adatkezelő. Önként vállalhatják az együttműködést az uniós adatvédelmi hatóságokkal, de bizonyos esetekben ez kötelező is, például HR adatbázisok kezelése esetén.

A *kiegészítő elvek* körében részletezi az Adatvédelmi Pajzs például a különleges adatok kezelése körében alkalmazható kivételek, az újságírói kivételeket, a internetszolgáltatók és a távközlési szolgáltatók mögöttes felelősségének kizárását, a nyilvánosan működő részvénytársaságok és a zártkörű részvénytársaságok rendszeres átvilágítását és auditálását, az adatvédelmi hatóságok szerepét és a fokozott együttműködési kötelezettséget, az öntanúsítás módját és lépéseit, a hozzáférési jog működését a gyakorlatban, a panasztételi, vitarendezési és végrehajtási eljárások részleteit.

DOI: 10.14750/ME.2019.022

X.3.2. Konklúziók a megfelelő védelmi szint biztosításáról

Megállapítható, hogy az új rezsim *alapkoncepciója megegyezik* elődje, a Safe Harbor rendszerével, ezért felmerül a kérdés, hogy miben lesz más, miért lesz jobb az Adatvédelmi Pajzs.

Az alap- és kiegészítő elvek részletesebb iránymutatást adnak és pontosabb megfelelést is várnak el a csatlakozó vállalkozásoktól.

Az Adatvédelmi Pajzs *hatálya* kiterjed a vállalkozások mellett a nemzetbiztonsági megfigyeléseket végző szervekre is. Az állami szervek hozzáférési joga vonatkozásában bevezet korlátozásokat és biztosítékokat, amelyeket a VI. mellékletben foglaltak szerint az Egyesült Államok kormánya a nemzeti hírszerzés igazgatójának hivatala által dolgozott ki, továbbá a VII. mellékletben szerepelnek az Egyesült Államok Igazságügyi Minisztériuma által rögzített korlátozások és biztosítékok. Ilyen például, hogy a jelfelderítési adatgyűjtésnek törvényen vagy elnöki engedélyen kell alapulnia, és az Egyesült Államok alkotmányának - különösen a negyedik alkotmánykiegészítésnek - és törvényeinek megfelelően kell azt végezni, valamennyi személyt méltósággal és tisztelettel kell kezelni, függetlenül az állampolgárságától és lakóhelyétől.[334] Az Adatvédelmi Pajzs (70) bekezdése rögzíti, hogy a "jelfelderítési adatok gyűjtése kizárólag nemzeti vagy minisztériumi megbízatás támogatására irányuló külföldi hírszerzési vagy kémelhárítási célból végezhető, nem pedig bármely egyéb célból (például azért, hogy versenyelőnyt biztosítsanak az Egyesült Államok vállalatainak)." Az adatgyűjtéseknek „a lehető legcélzottabbnak kell lennie", azokat a lehetőségekhez mérten kell leszűkíteni, fókuszálni, és konkrétan felsorolt nemzetbiztonsági célra kell korlátozni az adatok felhasználását**.**

[334] Adatvédelmi Pajzs (69) a)

DOI: 10.14750/ME.2019.022

Az Adatvédelmi Pajzs működtetése az FTC és a Kereskedelmi Minisztérium hatáskörébe tartozik majd, ugyanúgy, mint a Safe Harbor volt. A Kereskedelmi Minisztérium e célra létrehozott külön weboldalán közzéteszi az adatvédelmi pajzsban részt vevő szervezetek listáját és a tanúsítási beadványokat. A szervezeteknek évente újra kell tanúsítaniuk magukat a Kereskedelmi Minisztériumnál, ennek hiányában nem kezelhetnek jogszerűen az EU-ból származó személyes adatokat, valamint kötelező beszámolási rendszert is bevezetnek, az átláthatóság jegyében.

Az érintett nyújthat be panaszt az adatkezelőnek vagy közvetlenül az uniós vagy az amerikai felügyeleti és vitarendező szervnek is. Ingyenes független vitarendezési lehetőséget is kell biztosítani az érintettek számára, első körben az adatkezelőnek, amely során 45 napon belül válaszolni kell a panaszosnak. Ezen túl biztosítani kell, hogy az adatkezelővel szemben az FTC és a Közlekedési Minisztérium is jogosult legyen eljárni, legalább akként, hogy a tanúsított szervezet elismeri a fenti állami szervek joghatóságát saját tevékenysége felett. Az Adatvédelmi Pajzs létrehoz egy 20 bíróból álló *adatvédelmi pajzzsal foglalkozó testületet,* amely kötelező erejű döntést hozó kvázi választott bírósági eljárását is igénybe veheti az érintett. A III. mellékletében az Egyesült Államok kormánya kötelezettséget vállalt arra továbbá, hogy létrehoz egy új, a hírszerzéstől független, a nemzetbiztonsági megfigyeléssel foglalkozó felügyeleti mechanizmust, az adatvédelmi ombudsmant. Az Adatvédelmi Pajzs 90 napos határidőt rögzít arra vonatkozóan, hogy a Kereskedelmi Minisztérium bármely uniós tagállami hatóság megkeresése esetén tájékoztatást adjon az aktuális helyzetről.

Fontos és garanciális újítás, hogy az Európai Bizottság egy éven belül és azt követően évente helyzetértékelést végez az összes rendelkezésre álló információ alapján, így elkerülhető a Safe Harbor esetében bekövetkezett

DOI: 10.14750/ME.2019.022

helyzet megismétlődése. Az első éves értékelés[335] során az Európai Bizottság megállapította, hogy az amerikai hatóságok a legtöbb szükséges strukturális intézkedést megtették, amelyek az Adatvédelmi Pajzs működtetéséhez szükségesek, azonban az ombudsman kijelölése ekkor még csak folyamatban volt a kormányváltás miatt, bár a létrehozáshoz szükséges mechanizmus már rendelkezésre állt.[336] A Gazdasági növekedésért, energiaügyért és a környezetügyértért felelős államtitkárság látja el ma az ombudsman szerepét, a delegált személy 2019 februárjában Manisha Singh.[337]

A felülvizsgálat idejére már több, mint 2400 vállalkozás csatlakozott a rendszerhez. Az Európai Bizottságot arról tájékoztatták, hogy a tömeges és korlátlan megfigyelést biztosító U.S. Foreign Intelligence Surveillance Act (FISA) 702. cikkét 2017. december 31. napján hatályon kívül fogják helyezni, azonban 2018. januárjában újabb hat évre hatályában tartotta azt amerikai jogalkotó, az amerikai elnök nyilatkozata szerint a nemzet biztonságának megőrzése és a nemzetközi terrorizmus megakadályozása érdekében.[338] Beépítettek új garanciákat, a megfigyelés bírói engedélyhez kötött lesz és a törvény más, az átláthatóságra vonatkozó rendelkezéseivel jobban megóvható a személyek magánszférája, de csak amerikai állampolgároké, a garanciák más államok állampolgárai esetén nem alkalmazandók főszabály szerint.

Ez olyan központi eleme lehet a következő, 2018. évi felülvizsgálatnak, amely az adattovábbítások korlátozásához is vezethet vagy a jelenlegi beszámolási rendszer és a megfigyelés korlátozására vonatkozó elvek és szabályok szigorítását eredményezheti.

[335] Európai Bizottság: Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, {SWD(2017) 344 final}, Brussels, 18.10.2017 COM(2017) 611 final
[336] https://www.state.gov/documents/organization/275257.pdf [2018. június 10.]
[337] https://www.state.gov/e/privacyshield/ombud/ [2019. február 24.]
[338] https://www.whitehouse.gov/briefings-statements/statement-president-fisa-amendments-reauthorization-act-2017/ [2018. május 30.]

DOI: 10.14750/ME.2019.022

Összességében az Európai Bizottság az éves felülvizsgálat során megállapítja, hogy az *Adatvédelmi Pajzs keretei között a megfelelő védelmi szint biztosítottnak tekintendő*. A működéssel kapcsolatos fejlesztések érdekében tíz ajánlást is megfogalmazott az Európai Bizottság:

- a vállalkozások csak a tanúsítási folyamat lezárultával hivatkozhatnának nyilvánosan az Adatvédelmi Pajzs szerinti megfelelésükre, ezzel párhuzamosan
- a Kereskedelmi Minisztériumnak rendszeresen és proaktív módon kellene vizsgálnia a félrevezető, hamis kérelmeket és
- a megfelelés folyamatos monitoringozását kellene bevezetni, például kérdőívek rendszeres kiküldésével és értékelésével,
- szükség volna a tudatosság növelésre, különösen az uniós polgárok körében a jogérvényesítési lehetőségek kapcsán és
- a jogalkalmazó szervek közötti szorosabb együttműködés is kívánatos előrelépés.
- az értékelés kiemelt tárgyköre lesz az automatizált döntéshozatal kérdése, és kiemelt ajánlási pont volt a
- a fentebb hivatkozott FISA 702. cikkének reformja, valamint
- az ombudsman kijelölése, amely idő közben már megtörtént,
- az Adatvédelmi Pajzs további szervezeti követelményeinek kialakítása és személyi kijelölések valamint
- a határidőben történő, átfogó jelentési kötelezettség teljesítésére is figyelemhívás történt az Európai Bizottság részéről.

Formálisan a Safe Harborhoz hasonló, de kiterjesztett rendszer jött létre, azonban az első éves értékelésből még nem látható, hogy valóban hatékonyabb-e a működése. Az mindenesetre kedvező előrelépés, hogy a jogorvoslati és felügyeleti kérdésekben kötelező előírások születtek, azonban, különösen a FISA rendelkezés hatályában fenntartásával, azok következetes alkalmazásának kialakulásáig nem lesz előnyösebb az érintettek helyzete. A rendszer tehát nem tökéletes, van-e ennél kedvezőbb megoldás?

DOI: 10.14750/ME.2019.022

X.4. BCR vagy tanúsítás

A BCR jogi elismeréséhez szintén hosszas fejlődési folyamat vezetett, és a jogérvényesítésre vonatkozó ugyancsak hiányzó jogalkalmazói gyakorlat nem szolgál meggyőzőbb indokokkal alkalmazása mellett érintetti szempontból, azonban az adatkezelő vállalkozások számára kedvezőbb jogi eszköz lehet. Az alábbiakban előbb táblázatos formában, majd az egyes szempontok kiemelésével bemutatom, hogy a két tanúsítási rendszer és a BCR miben hasonlóak, és mik a mérlegelendő eltérések.

A GDPR 4. cikk 20. pontjában a BCR fogalma azt sugallja, hogy az alapvető elvek és érvényesíthető jogok szabályzata, azonban a BCR ennél jóval komplexebb dokumentum.[339] Alternatívát biztosít valamennyi olyan jogi eszköz, köztük az Adatvédelmi Pajzs szerinti tanúsításra is, amely a megfelelő védelmi szint biztosítására szolgál, azonban azt, hogy jobb vagy hatékonyabb alternatíva lehet-e, azt az adatkezelő vállalkozásnak kell eldöntenie. A szempontokat az alábbiak szerint lehet összevetni az alapvető és az egyedi különbözőségek megállapítása érdekében:

<table>
<tr><th></th><th>BCR</th><th>Safe Harbor</th><th>Adatvédelmi Pajzs</th></tr>
<tr><td rowspan="2">Jogi természet</td><td colspan="3">- önkéntes alkalmazás
- kötelező erejű szabályok
- állami együttműködés és felügyelet jellemzi
- kötelezettségvállalás arra vonatkozóan, hogy tiszteli és betartja az adatvédelmi szabályokat
- biztosítja a megfelelő védelmi szintet a gazdasági szereplő (vállalkozáscsoport) számára (de
- nem a harmadik ország egésze számára)</td></tr>
<tr><td>magánjogi jogi eszköz hatósági jóváhagyással</td><td>együttszabályozási eszköz (az Európai Bizottság határozata a vállalkozások kötelezettségvállalásával)</td><td>együttszabályozási eszköz (az Európai Bizottság határozata a vállalkozások kötelezettségvállalásával)</td></tr>
</table>

[339] A BCR tartalmáról részletesen lásd a VIII. fejezetben.

DOI: 10.14750/ME.2019.022

	vállalkozáscsoport belső szabályzata hatósági jóváhagyással	tanúsítási mechanizmus, a vállalkozás belső szabályzatot köteles alkotni	tanúsítás mechanizmus, a vállalkozás belső szabályzatot köteles alkotni
	személyi hatálya állampolgárságtól függetlenül mindenkire kiterjed	személyi hatálya csak az uniós polgárokra terjedt ki	személyi hatálya csak az uniós polgárokra terjed ki
	alkalmazhatóságához a vállalkozás(csoport) és az állami szerv tevékenysége (jóváhagyás, monitoring) együttesen szükséges		
Jóváhagyás, felülvizsgálat	az érintett tagállam(ok) nemzeti adatvédelmi felügyelő hatósága(i)	szövetségi szinten a Szövetségi Kereskedelmi Bizottság (FTC)	szövetségi szinten a Kereskedelmi Minisztérium
	a jóváhagyásra irányuló eljárás kérelem alapján indul és felülvizsgálat kizárólag a BCR-t alkalmazó vállalkozáscsoport kérelmére indul	a csatlakozásra/tanúsításra irányuló eljárás kérelem alapján indul és felülvizsgálat kizárólag kérelemre történik	a csatlakozásra/tanúsításra irányuló eljárás kérelem alapján indul és felülvizsgálat saját önértékelés keretén belül, rendszeresen, és a Kereskedelmi Minisztérium rendszeres felülvizsgálata alapján történik és évente tanúsítási kötelezettség áll fenn

DOI: 10.14750/ME.2019.022

	de elvben az érintetti igényérvényesítés során a BCR (felül)vizsgálata megtörténhet		de elvben az érintetti igényérvényesítés során a tanúsítás érvényességének (felül)vizsgálata megtörténhet
Szükséges teendők az alkalmazását megelőzően	- BCR tervezet elkészítése - BCR jóváhagyása a vezető hatóság és az érintett hatóságok által - az eljárási díj megfizetése - a BCR folyamatos frissítése a jogi és/vagy strukturális és/vagy technológiai környezet változása esetén - a módosítások bejelentése a vezető hatóság felé - díjfizetés	- kötelezettségvállalás az elvek, a szabályok és a GYFK szerinti válaszok betartására - a kötelezettségvállalás nyilvántartásba vétele és bejelentése a Szövetségi Kereskedelmi Bizottság (FTC) felé	- kötelezettségvállalás az elvek betartására - adatvédelmi szabályzat elkészítése és közzététele - kérelem benyújtása a Kereskedelmi Minisztériumnak - a Kereskedelmi Minisztérium honlapjára mutató link közzététele - az adatvédelmi pajzs weboldalára vezető hiperlink, valamint a megoldatlan panaszok kivizsgálására a független jogorvoslati mechanizmus weboldalára vagy panasz benyújtására szolgáló formanyomtatványára mutató hivatkozás közzététele - díjfizetés

DOI: 10.14750/ME.2019.022

Tartalom jellege	a vállalkozáscsoport struktúrája, alaptevékenysége, adatkezelési és adattovábbítási tevékenysége szerint kialakított szabályrendszer	általános elvek és a GYFK körében adott válaszok, függetlenül az öntanúsításban résztvevő gazdasági szereplő jellemzőitől illetve egyedi igényeitől	általános és kiegészítő elvek tiszteletben tartása, szervezeten belüli vagy kívüli kapcsolattartó pont, független panaszkezelő mechanizmusok, adatvédelmi szabályzat
	a vállalkozáscsoporton belül és a harmadik országban működő tagok esetén megfelelő védelmi szintet biztosít	az USA-ban működő gazdasági szereplő vonatkozásában igazolta a megfelelő védelmi szintet	az USA-ban működő gazdasági szereplő vonatkozásában igazolja a megfelelő védelmi szintet

2. ábra: BCR, a Safe Harbor határozat és az Adatvédelmi Pajzs összehasonlítása

Mindhárom jogi eszköz elsődleges célja, hogy alkalmazásával az adatkezelő biztosítsa a megfelelő védelmi szintet, BCR esetében ez bármely harmadik ország, míg a Safe Harbor és az Adatvédelmi Pajzs esetén csak az USA vonatozásában. Közkeletű, de téves álláspont az, amely szerint az Adatvédelmi Pajzs minden az USA-ba irányuló adattovábbítás vonatkozásában biztosítja a megfelelő védelmi szintet.

Mivel, noha az Adavédelmi Pajzs az USA minden államára kiterjedő jogi eszköz, mégsem azok megfelelőségét deklarálja, hanem csak azoknak a vállalkozásoknak a tevékenysége minősül annak, akik részt vettek a tanúsításban. Tehát összességében mindegyik vizsgált jogi eszköz csak az adott adatkezelő megfelelőségét biztosítja. Így ha a vállalkozáscsoport nemcsak az USA-ba kíván személyes adatot továbbítani, úgy a BCR a javasolt jogi megoldás. Ezen túl a BCR a vállalkozáscsoport egészének megfelelését biztosítja. Amennyiben egy vállalkozáscsoport külön-külön tanúsítani kényszerül egyes amerikai tagjait, úgy komplexitásának ellenére hosszú távon biztosabbnak látszik a BCR alkalmazása.

DOI: 10.14750/ME.2019.022

A továbbiakban elsődlegesen a két hatályos eszközt hasonlítom össze, a Safe Harbor sajátosságaira csak akkor térek ki, ha az különösen előnyös vagy hátrányos jellemzője miatt jelentősen eltér az Adatvédelmi Pajzstól.

Mindkét megoldás önkéntesen alkalmazható, de amennyiben az adatkezelő bármelyik alkalmazása mellett dönt, annak szabályai kötelezők, megsértésük kártérítési felelősséget vagy hatósági bírságot is vonhat maga után. Kiemelendő, hogy a BCR szignifikáns befelé irányuló kötelező erővel is bír, így az adatkezelő működése során a munkatársak megfelelési hajlandósága erősebb. Azt persze a tanúsítási rendszerek sem zárják ki, hogy belső szabályzatban az adatkezelő a *belső megfelelésre* vonatkozó szabályokat kössön ki. A *kifelé irányuló kötelező erő*, tehát az érintetti jogérvényesítés mind a BCR, mint az Adatvédelmi Pajzs vonatkozásában egyelőre még tapasztalatok nélküli terület, az azonban elmondható, hogy az elvi lehetőség fennáll az érintetti igények érvényesítésére. Mindkét esetben egy in-house adatkezelői panaszkezelési módszert kell biztosítani. Ezen túl míg a BCR esetén az érintett akár a kijelölt vállalkozáscsoporti tag, akár lakóhelye szerinti hatóság vagy bíróság eljárását is kezdeményezheti, addig az Adatvédelmi Pajzs esetén kijelölt, központi, nemrég létrehozott szervek (*adatvédelmi pajzzsal foglalkozó testületet, ombusdman)* új eljárásait kell kezdeményezni. Míg a BCR esetén van egy kijelölt vállalkozáscsoporti tag, amelyre hárul a bizonyítási teher és a kártérítési kötelezettség teljesítése, addig az Adatvédelmi Pajzs szerint tanúsított vállalkozás esetében ilyen kijelölési kötelezettség nincs, ami persze nem jelenti, hogy ne járhatna el hasonlóan.

A BCR alapvetően *magánjogi* eszköz, egy belső szabályzat, a vállalkozáscsoport egyoldalú kötelezettségvállalása, amelyet a nemzeti hatóságok jóváhagynak. Ezzel szemben az Adatvédelmi Pajzs egy *állami tanúsítási rendszer, egy együttszabályozási keretrendszer*, amelyet az FTC és a Kereskedelmi Minisztérium működtet.

DOI: 10.14750/ME.2019.022

Az Európai Bizottság határozatában elfogadta a megfelelő védelmi szint biztosításának igazolásául, hogy az Adatvédelmi Pajzs elveit betartó tanúsított vállalkozások részére jogszerűen történhet az adattovábbítás az USA-ba. Tehát a két jogi eszköz alapvető eltérést mutat.

A BCR alapvetően egy *szabályzat-típusú* megfelelés, míg az Adatvédelmi Pajzs egy *tanúsítási-típusú* megfelelés keretrendszere. Közös jellemzőjük, hogy részben társ-szabályozási eszköznek tekinthetők, hiszen a vállalkozás és az állami szerv együttműködése szükséges alkalmazásukhoz. Míg az állami szerv a jogi környezetnek történő megfelelését vizsgálja, a vállalkozásnak adatvédelmi politikáját és gyakorlatát kell ki- vagy átalakítania a számára legmegfelelőbb formára. Igaz ugyan, hogy akár egy évet is igénybe vehet a BCR első jóváhagyása és a vállalkozáscsoport működése során bekövetkező változásoknak megfelelően annak módosítására és frissítésére is szükség lehet, azonban az Adatvédelmi Pajzs szerinti tanúsítás évente kötelezően felülvizsgálandó, amely sokszoros többlet terhet ró az adatkezelőre.

Alapvető eltérés azonosítható a BCR és az Adatvédelmi Pajzs személyi hatálya kapcsán. A BCR szabályai állampolgárságtól függetlenül kiterjednek mindenkire, aki a hatálya alá tartozik, tehát az uniós polgárokra és minden harmadik ország állampolgáraira is. Az Adatvédelmi Pajzs tanúsítási rendszere csak az uniós polgárok személyes adatainak kezelésére vonatkozó szabályokat állapít meg. Így megállapítható, hogy összességében a BCR szélesebb körű védelmet biztosít egy vállalkozáscsoport szintjén, mint az Adatvédelmi Pajzs szerinti tanúsítás, amely azért is különösen értékes szempont, mert a GDRP tárgyi hatálya nemcsak az uniós polgárok személyes adatinak kezelésére terjed ki, hanem az Európai Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett és az Európai Unióban tartózkodó érintettek személyes adatainak kezelésére is.

DOI: 10.14750/ME.2019.022

Míg a BCR nagy előnye, hogy szabályait a vállalkozáscsoport tevékenységére és struktúrájára lehet igazítani, addig az Adatvédelmi Pajzs szerinti tanúsítás az előre meghatározott elvek kötelező betartását követeli meg. Mivel az USA-ban nincs a GDPR-hoz hasonló átfogó, általános adatvédelmi jogi környezet, így az Adatvédelmi Pajzs, ahogyan a Safe Harbor is, megalkotta az európai szabályok és az alapelvek rövidített, tömörített summáját, amely szükségszerűen nem fogja az azonos szintű védelmet eredményezni. Egy BCR kötelező tartalmi elemei és a jóváhagyása során benyújtandó mellékletek vizsgálata alapján az eljáró hatóságok részleteiben is megismerik a vállalkozáscsoport adatkezelési tevékenységeit, és így valószínűsíthetően megalapozottan lehet a BCR megfelelőségéről és alkalmazhatóságáról dönteni, a megfelelő védelmi szint biztosítását jóváhagyni. Az Adatvédelmi Pajzs szerinti tanúsítás alkalmával az elvek betartására szóló kötelezettségvállalást kell tenni, de a vállalkozás adatvédelmi szabályzata alapján nem biztos, hogy kellő alapossággal bemutatja a vállalkozás adatvédelmi és adatkezelési tevékenységét.

Azt is meg kell állapítani azonban, hogy a BCR nem minden országban ismert és elismert jogi eszköz. A GDPR hatályba lépésével az Európai Unió tagállamai körében közvetlenül alkalmazható jogi eszköz, azonban korábban több tagállamban a vonatkozó jogi környezet nem rendelkezett róla, 2015 októberéig hazánkban sem. Tehát egy olyan harmadik ország esetén, amelyben a BCR az adott harmadik országban nem jelent tényleges védelmet és garanciát, valószínűleg nem lesz megfelelő jogi eszköz az érintettek jogvédelme szempontjából. Ezért az adatkezelőn is nagy a felelősség, hogy a vállalkozáscsoport tagját mely harmadik országba telepítse vagy úgy alakítsa az adatkezelési mechanizmusait, hogy az adott harmadik országba nem továbbít személyes adatokat. Az Adatvédelmi Pajzs esetén ilyen dilemma nem merül fel, mert az EU-USA relációban elismert rendszer, azonban nem

DOI: 10.14750/ME.2019.022

elhanyagolható erős (aktuál) politikai[340] befolyásoltsága sem. Adódik tehát a kérdés, hogy egy vállalkozáscsoport inkább a tisztán jogi alapokon álló, a vonatkozó jogi környezet tervezhetően állandó és statikus szabályai valamint az idővel lassan kialakuló hatósági gyakorlatra alapítottan alkalmazzon egy számára megfelelő rendszerű BCR-t, vagy egy politikai megoldásként aposztrofált, egyelőre hiányos rendszerű tanúsítási mechanizmusban vegyen részt.

2015 év közepén az európai adatvédelmi reform kapcsán egyes szerzők még úgy fogalmaztak, hogy a Safe Harbor rendszert várhatóan drámai változtatás nélkül fogják fenntartani.[341] Ma már tudjuk, hogy a jóslat nem igazolódott be. Az Adatvédelmi Pajzs a Safe Habor utódjaként látja el megerősített jogérvényesítési és felügyeleti funkciókkal az USA-ba irányuló adattovábbítások megfelelőségért felelős rendszer szerepét. A rendszert évente fogja vizsgálni az Európai Bizottság, és a legvitatottabb aggály vonatkozásában - az USA nemzetbiztonsági szerveinek megfigyelési jogosítványain - az USA érdemben nem változtatott, így a 2018. évi, második felülvizsgálat érdekes következményeket hozhat. Azok a vállalkozások, amelyek el kívánják kerülni a Safe Harbor érvénytelenítése idejéből ismert bizonytalanságot, alternatív megoldásokat kereshetnek. Az egyik ilyen növekvő népszerűségnek örvendő megoldás a BCR lehet, amely számos ponton ki tudja küszöbölni az Adatvédelmi Pajzs negatív jellemzőit. Mindemellett megállapítható, hogy az USA adatvédelmi gyakorlata és vonatkozó jogi környezete *alapjaiban tér el az európai hozzáállástól*, és a nemzetbiztonsági kockázatok növekedése és a technológia fejlődése mégsem az egyén magánszférájának erősítése irányába ösztönzi a jogalkotót és az adatkezelőket sem.

[340] SCHUBAUER (2016) p. 135.
[341] PELTZ-STEELE (2015) p. 21.

DOI: 10.14750/ME.2019.022

XI. FEJEZET
CBPR – AVAGY AZ APEC TAGÁLLAMOK ADATVÉDELMI MEGFELELŐSÉGÉRŐL

Az APEC tagállamok[342] 2004-ben fogadták el az Adatvédelmi Keretrendszert[343] (a továbbiakban: Keretrendszer), amelynek funkciója, hogy a tagállamok közötti adatáramlás során a személyes adatok védelmét biztosítsa. Megalkotásának célja elsősorban az elektronikus kereskedelem iránti bizalom növelése és az online közegben egyre gyakrabban előforduló adatvédelmi incidensek kiküszöbölése volt. Alapul szolgáltak az OECD adatvédelmi alapelvek (a célhoz kötöttséget, a nyíltság elvét, a korlátozott adatgyűjtés elvét, az adatminőség elvét az adat integritásaként) és kiegészítették azokat specifikus elemekkel, így például a károkozás megelőzésének elvével. A tagállamok szabad kezet kaptak abban, hogy a Keretrendszer szabályait hogyan ültetik át nemzeti jogukba.

Érdekes tény, hogy a Keretrendszer az adatkezelés jogalapjául az érintett hozzájárulása mellett főszabályként rögzíti az érintett kezdeményezésére nyújtott szolgáltatások nyújtásához szükséges esetet is. Az európai adatvédelmi jogban ezt a jogalapot a GDPR 6. cikk (1) bekezdés b) pontja deklarálja, régen várt megoldásként.

A Keretrendszer a határon átnyúló adatvédelmi szabályok rendszerét (a továbbiakban: CBPR - az angol nyelvű elnevezés szerinti Cross-Border Privacy Rules), mint önkéntesen alkalmazható szabályrendszer létrehozását is ösztönzi.

[342] Ázsiai-Csendes-óceáni Gazdasági Együttműködés, amely alapvetően a tagok konszenzusán és önkéntességen alapuló, kötelező szabályozás nélküli együttműködés a nemzetközi szervezetektől elkülönülten.
[343] APEC Privacy Framework, APEC Secretariat, 35 Heng Mui Keng Terrace, Singapore 119616, ISBN 981-05-4471-5

DOI: 10.14750/ME.2019.022

A CBPR elsődleges célja az, hogy a rendszerhez csatlakozó tagállamokban a rendszer szabályait alkalmazó vállalkozások *adatvédelmi megfelelését biztosítsa a letelepedésük szerinti ország nemzeti joga és a többi, a CBPR-hoz csatlakozott APEC tagállam joga szerint is*, további adminisztratív követelmények beiktatása nélkül. A rendszert egyes szerzők[344] a Privacy Shield rendszeréhez hasonlítják, hiszen mindkettő olyan az önszabályozás elvén nyugvó, tanúsításon alapuló megfelelési és felülvizsgálati mechanizmusokat biztosít, amelyekhez vitarendezési és hatósági jogalkalmazó fórumokat kapcsol. A CBPR nem helyettesíti a nemzeti jogi előírásokat, pusztán egy minimum szintet rögzít olyan esetekre, amelyekre nincs nemzeti jogi előírás. Azok a vállalkozások, amelyek vállalják, hogy betartják a CBRP rendszer előírásait, a nemzeti jogi kötelezettségeiken túl vállalnak többletkötelezettségeket a megfelelés érdekében. Olyan esetekben, amelyekben a nemzeti jog szigorúbb a CBPR szabályoknál, a nemzeti jog alkalmazandó.

XI.1. A CBPR kialakulása és szerkezete

Az APEC tagállamok miniszterei 2007-ben a Data Privacy Pathfinder projektek (a továbbiakban: projektek) létrehozásával kívánták a Keretrendszer olyan irányú reformját elvégezni, hogy a meglévő szabályok ne a szabad adatáramlás gátját képezzék, hanem valóban adatvédelmi célokat szolgáljanak. Ehhez a tagállamok kölcsönös elismerési eljárások kialakításába és fejlesztésébe kezdtek. Céltételezésként a projektek fókuszában egy egységes és könnyen átlátható rendszer létrehozása állt, amely a tagállamok közötti személyes adatok szabad áramlását szolgálja.[345] Tekintettel arra, hogy a tagállamok nemzeti szabályai között nagy volt az eltérés, így végül tizenhat állam részvételével kezdődött meg az egységesítési folyamat.[346]

[344] WALL (2017)
[345] APEC Data Privacy Pathfinder
[346] Ausztrália, Kanada, Chile, Kína, Hong Kong, Japán, Dél Korea, Mexikó, Új-Zéland, Peru, Fülöp-szigetek, Szingapúr, Taipei, Thaiföld, az USA és Vietnam.

DOI: 10.14750/ME.2019.022

A projektek során a CBPR rendszerét és főbb szabályait kívánták létre hozni. A cél az volt, hogy a csatlakozó tagállamok egy olyan önként alkalmazható nemzeti *tanúsítási rendszert alkossanak*, amely a cégek számára lehetőséget biztosít arra, hogy alkalmazásával nemcsak betarthatják a vonatkozó jogi előírásokat, hanem a fogyasztók, az adatalanyok bizalmát is elnyerhetik. A projektek során fontos volt láttatni azt, hogy a CBPR létrehozása a vállalat és az érintett számára is előnyös. A vállalkozások jogi megfelelését biztosítja, kialakítja a vállalkozásnál a külföldi adattovábbítások mechanizmusát, így elszámoltathatóságát is demonstrálhatja, ezzel növelve a fogyasztók bizalmát. A vállalkozáscsoport a tanúsítás eredményeként kialakuló adatvédelmi szabályrendszere képes egységesíteni a vállalkozáscsoport adatvédelmi politikáját, amely az önszabályozás eredményességét és hatékonyságát is megalapozza. A CBPR a tagállamok szintjén segíti az együttműködést a felügyeleti hatóságok között, amely kooperáció a jogszabályok eredményesebb kikényszerítését eredményezheti.

A projektek során létre kívánták hozni az „*elszámoltathatósági megbízottak*” (accountability agent; a továbbiakban: megbízott) körét, amely szervezetek kvázi adatvédelmi biztosként illetve a felügyeleti hatóság egyfajta pótlékaként felügyelik a cégek megfelelő működését és választottbíróságként is eljárhatnak vitás helyzetekben. A megbízottak olyan tagállami szervezetek, amelyek a vállalkozások tanúsítását is elvégzik.

A projektek során a CBPR számos tisztázatlan kérdése várt még rendezésre: ilyen a CBPR nemzeti elismerése olyan tagállamokban is, ahol már van nemzeti adatvédelmi szabályozás; a CBPR keretei közötti önértékelési és tanúsítási mechanizmusok kialakítása; már működő CBPR-hoz hasonló rendszerek fejlesztésének módszertana. Egyértelmű keretrendszert kellett kiépíteni a megbízottak és a tanúsítási mechanizmusok működésére valamint a CBPR megfelelőségi felülvizsgálatának szempontjaira.

DOI: 10.14750/ME.2019.022

A nyilvánosság érdekében létre kellett hozni azt az *információs és irányítási rendszert,* amely a CBPR hatálya alá tartozó tagállamok és tanúsított vállalatok jegyzékét is tartalmazza. A projektek során a nemzeti adatvédelmi felügyelő hatóságok működésének és együttműködésének összehangolására létre kívántak hozni *egy közös Adatvédelmi Hatóságot* és a *nemzeti kapcsolattartó személyek elérhetőségének jegyzékét*, valamint be kívántak vezetni egy általános panaszkezelési nyomtatványt, amelyet minden érintett hatóság elfogad és felhasznál a gyors és hatékony együttműködés érdekében. Tisztázni kellett a CBPR hatályára vonatkozó részleteket és tényleges alkalmazási körét. Mindezen részfeladatok mellett elindult egy *CBPR-teszt projekt*, amely a rendszer bevezetését és fejlesztését az összes többi projekt eredményeinek ismeretében és felhasználásával igyekezett elérni.

2017-ben huszonegy résztvevő tagállamra kiterjedő helyzetelemzés[347] készült el. A CBPR rendszerhez addig – és napjainkig – négy állam csatlakozott: az USA, Kanada, Mexikó és Japán. Egy évtized alatt az APEC tagállamok háromnegyedében fogadtak el adat- és magánéletvédelmi törvényt, és a helyzetelemzésben szereplők közül mindössze három tagállamban nincs még adatvédelmi törvénytervezet sem.
Az viszont megállapítható, hogy ahol van szabályozás, az megfelel a Keretrendszer szabályainak. Ez persze *nem jelenti azt, hogy az adatvédelem szintje lényegesen közelítene az európai megfelelő védelmi szinthez* minden csatlakozott tagállamban, csupán annyit, hogy maga a Keretrendszer sem teszi magasra a mércét. Kizárólag Kína és Malajzia nem tervezi azt, hogy CBPR rendszerhez csatlakozik, mindemellett a Brunei Szultanátus, Kína, Indonézia, Pápua Új-Guinea és Thaiföld nemzeti adatvédelmi jogi szabályozás - ami tehát alapkövetelmény - hiányában nem is tudna csatlakozni.

[347] APEC Electronic Commerce Steering Group - Hang Bui: Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs - Final Report, 2017. január

DOI: 10.14750/ME.2019.022

Hét tagállamban nincs felügyelő hatóság és tizenegy tagállamban nincs tanúsító szervezet, amely komoly akadályát jelenti annak, hogy az adott harmadik ország - vagy a CBPR elveit és szabályait önkéntes jogkövetéssel betartó magatartás hiányában az országban működő vállalat - a személyes adatok védelmének a megfelelőhöz akár csak közeli szintjét biztosítani tudja.

Megállapítható azonban az is, hogy a projektek eredményeként a tervezett rendszer az *eredeti elképzeléseket megvalósítva jött létre*. A CBPR rendszer négy pilléres szerkezete az alábbiak szerint épül fel: az *első pillérbe* tartoznak azok a követelmények, amelyeknek azoknak a szervezeteknek kell eleget tenniük, amelyek megbízottként kívánnak részt venni a rendszer működésében; a *második pillér* egy kérdéssor, amelyet azoknak a szervezeteknek kell megválaszolniuk, amelyek tanúsítást követően részt kívánnak venni a CBPR rendszerben; *harmadik pillér* a tanúsítás során alkalmazandó értékelési kritériumrendszer és információs felület; végül a *negyedik pillér* egy együttműködési megállapodás, amelyet a tagállamok adatvédelmi hatóságai, jelenleg nyolc tagállamból huszonöt tag, kötöttek annak érdekében, hogy a CBPR rendszer előírásainak kikényszerítését biztosítsák a résztvevő APEC tagállamokban. A kezdeti időkben jellemzően nem a CBPR kikényszerítése körében zajlott az együttműködés, hanem további, a rendszertől független, jellemzően a nemzeti adatvédelmi jogi kérdéseket is megvitattak.

Az első pillérbe tartoznak mindazok a követelmények, amelyek teljesítése esetén egy szervezet megbízottként járhat el. Vizsgálat alá vonják a megbízottnak jelentkező szervezet tanúsítási programját, vitarendezési mechanizmusát, az összeférhetetlenséget elkerülő eljárásait, a felülvizsgálati és nyomon követési rendszerét valamint kikényszerítési eljárásait. A megbízotti minőség elnyeréséért anonimizált esetleírásokat és statisztikákat kell közzétenniük. Vállalniuk kell továbbá, hogy a panaszkezelési eljárások során együttműködnek a tagállami hatóságokkal és a többi megbízottal is.

DOI: 10.14750/ME.2019.022

A megbízott a tanúsítás során olyan értékelési módszert köteles alkalmazni, hogy a CBPR elveinek és minimumelőírásainak való megfelelést vizsgálja, és azok sztenderdje alá eső vállalkozások tanúsítást nem kaphatnak.

A második pillért képező kérdéssor megválaszolása és a hozzá csatolt dokumentáció benyújtása a tanúsítási folyamat első lépése. A szervezet válaszait a megbízott értékeli. A csatlakozni kívánó szervezet azt a megbízottat köteles felkérni tanúsításra, amely a szervezet székhelye szerinti tagállamban működik. A megbízott további felvilágosítást kérhet a benyújtott iratok vonatkozásában, illetve további követelményeket írhat elő. Azok a szerveztek, amelyek a megfelelnek a CBPR rendszer előírásainak, tanúsítást kapnak és e minőségüket az APEC honlapján közzéteszi, amely a harmadik pillér törzsét képezi, egyben az átlátható adatvédelmi működést elősegíti.

A CBPR szabályainak betartását a negyedik pillérben a megbízottak és az adatvédelmi hatóságok kényszerítik ki. A megbízott szerződés vagy jogszabály alapján jogosult fellépni a szabályok be nem tartása esetén, míg a hatóságok hatósági eljárás formájában látják el jogalkalmazó felügyeleti szerepüket. A hatóságok az együttműködési megállapodás körében szorosan együttműködnek és nemcsak információcsere útján, hanem konkrét eljárási cselekmény lefolytatása körében is, mindezt mérlegelési jogkörben elhatározva, nem kötelező jelleggel.

A CBPR elvei az egyszerűség, átláthatóság, az alacsony költségvonzat és a tagállamok elszámoltathatósága. A rendszer továbbá magában foglalja az APEC tagállamok számára önkéntes, egységes, konszenzuson alapuló döntéshozatali formában működő és rugalmas adatvédelmi keretrendszert is.

DOI: 10.14750/ME.2019.022

XI.2. Csatlakozás a CBPR rendszerhez

XI.2.1. Tagállam csatlakozása

A CBPR rendszerhez többlépcsős csatlakozási mechanizmust dolgoztak ki. Amennyiben egy tagállam csatlakozni kíván, a tagállam kormánya által kijelölt delegált személy benyújtja a tagállam csatlakozási szándékát tartalmazó kérelmet és megerősíti legalább egy megbízott kijelölését a tagállamon belül. A delegáltnak be kell mutatnia a tagállamában alkalmazandó adatvédelmi jogi környezetet valamint a CBPR rendszer szabályainak kikényszerítését biztosító végrehajtási mechanizmust.

A csatlakozását kérő tagállamban az adatvédelmi felügyeleti hatóságnak jeleznie kell az együttműködési megállapodásban részes hatóságok felé részvételi szándékát, amelyben megerősíti, hogy megfelel a végrehajtás körében előírt követelményeknek. Meg kell erősítenie, hogy hatósági formában működik és biztosítania kell egy kapcsolattartási pontot is. Ismertetnie kell a jó gyakorlatokat, a politikákat és feladat- valamint hatásköreit. A felügyeleti hatóság együttműködési szándékát a negyedik pillér szerinti együttműködési megállapodás hivatalnokai bírálják el.

A tagállamban legalább egy szervezetnek jelölés vagy bejelentkezés alapján jelentkeznie kell megbízottnak. Előfordulhat az a helyzet is, hogy a tagállami adatvédelmi hatóság megbízotti minőségben is eljár, továbbá felmerülhet az az eset is, hogy egy tagállam más tagállam megbízottját jelöli meg a csatlakozáshoz. Ez utóbbi esetben a tagállamnak azt is be kell mutatnia, hogy a megbízott milyen joghatósági és nemzeti jogi szabályok szerint lesz jogosult eljárni a kérelmező tagállamban.

DOI: 10.14750/ME.2019.022

A megbízottnak jelentkezésében meg kell adnia, hogy mely tagállam megbízottja vagy legalábbis melyik tagállam joghatósága alá tartozik, valamint be kell mutatnia, hogy hogyan felel meg az előírt követelményeknek. Ismertetnie kell tanúsítási és felülvizsgálati mechanizmusait, és amennyiben az APEC formulától eltérő tanúsítási nyomtatványt alkalmaz, úgy annak tervezetét is be kell nyújtania. A megbízott kérelme a Közös Felügyeleti Testülethez, onnan pedig a többi részes tagállamhoz kerül. A 2017-es felmérés szerint is *mindössze öt ilyen megbízott működik*, mind az öt amerikai cég, a további tizennégy potenciális jelentkező évek óta vár a bejelentkezéssel. Tehát, a fentiek szerint a tagállam csatlakozását végülis nem gátolja meg, ha nincs a tagállamban ténylegesen működő megbízott illetve következik a fentiekből is az, hogy az egyik tagállam megbízottja tanúsíthat más tagállamban működő szervezetet.

A megbízott működésének felügyeletét a CBPR kormányzásáért felelős Közös Felügyeleti Testület látja el. A megbízotti minősítés egy évre szól, amelyet meg lehet újítani. A tagállam tagságának megszűnése vagy felfüggesztése esetén a megbízott működése és elismertsége is függővé válik.

XI.2.2. Szervezet csatlakozása és tanúsítása

Azoknak a szervezeteknek illetve vállalkozásoknak, amelyeknek a CBRP rendszerhez csatlakozott tagállamban van a székhelyük vagy ott működnek, tanúsítás keretében csatlakozhatnak a rendszerhez. E körben kötelező és kikényszeríthető adatvédelmi elveket és jó gyakorlatokat kell bevezetniük és alkalmazniuk. A megfelelőséget a megbízott értékeli a szervezet tanúsításával. A csatlakozási szándékról az APEC Elektronikus Kereskedelem Vezetéséért felelő Csoport tanácsa, az Adatvédelmi Csoport tanácsa és a CBPR kormányzásáért felelős Közös Felügyeleti Testület dönt.

DOI: 10.14750/ME.2019.022

A tagállam tagságát felfüggesztik vagy megszüntetik abban az esetben, ha a nemzeti jog módosítása következtében a CBPR rendszerrel össze nem egyeztethető jogi környezet jön létre. Ebben az esetben a megbízott sem végezheti tovább tevékenységét, és ebben esetben a tanúsított vállalkozás megfelelősége is megszűnik.

XI.3. A CBPR megítélése

Egyes szerzők[348] szerint a CBPR az interoperabilitás jegyében egy olyan globális rendszerben, ahol az adatvédelmi rezsimek közös megállapodás útján létre jött keretrendszerek alapján együttműködnek, kisebb egységként, regionális keretrendszer tud működni.

A CBPR kezdeti nehézségeit a „tyúk vagy a tojás" dilemma árnyalta tovább,[349] azaz a vállalkozások további tagállamok csatlakozását várták, mielőtt tanúsításukat kérték, a tagállamok pedig a nagyobb piaci érdeklődés esetére tartogatták csatlakozási szándékuk előterjesztését. A BCR esetén ez a jelenség szintén azonosítható volt. Amíg a tagállamok többségében nem vált jogilag elismert jogintézménnyé, addig jellemzően más jogi eszközök alkalmazására voltak kényszerítve a vállalkozáscsoportok.
A BCR elismertségének elterjedésével, igaz lassú ütemben, de növekszik az azt alkalmazó vállalkozáscsoportok köre és a bevont tagok száma is.

XI.4. A BCR a CBPR európai uniós megfelelője?

A 29. cikk szerinti Adatvédelmi Munkacsoport és az APEC tagállamok Adatvédelmi Alcsoportja közös álláspontja szerint a BCR a CBPR európai megfelelője.[350]

[348] HEYDER (2014) (1)
[349] HEYDER (2014) (2)
[350] Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection

DOI: 10.14750/ME.2019.022

Felmerültek a BCR-rel való párhuzamosságok erősítését célzó gondolatok, azonban mint tapasztaljuk, ezek megvalósítása napjainkig elmaradt.

A BCR és a CBPR *közös alapértékei, hogy önkéntes alapú, de kötelező erejű és kikényszeríthető mechanizmusok*. Minkét esetben az adatvédelmi politikát egységesítő célzattal hoznak létre olyan szabályrendszereket, amelyekkel különböző jogi védelmi szinttel bíró országokba lehet jogszerűen személyes adatokat továbbítani, így *biztosítva az elvárt garanciákat*. További közös jellemző, hogy egy külső, harmadik személy - hatóság vagy megbízott - bírálja el a szabályok megfelelőségét. Ezen túl azonban mintha az almát a körtével hasonlítanánk össze, a különbségek nem egymás megfelelői.

Az első kiemelendő tény, hogy a CBPR rendszerben csak olyan vállalkozás kérheti tanúsítását, amely letelepedése szerint ország már csatlakozott a CBPR rendszerhez. Ez a követelmény az uniós jogban olyan formában jelenik meg, hogy csak olyan tagállamban alkalmazható a BCR a megfelelő védelmi szint garanciájaként, ahol azt a nemzeti jogba már bevezették. Azonban ez a nemzeti jogalkotó kompetenciája és döntése, míg a CBPR-hoz történő csatlakozás egy tagállam teljes jogi környezetének egy külső szervezet általi vizsgálatának feltétele. Tehát míg a BCR bevezetését jogalkotással lehet megtenni, addig egy tagállam csatlakozása a CBPR rendszerhez több más tagállam megítélésétől függ, amely jelentős politikai és gazdasági befolyásoltságot hordoz. Továbbá a GDPR hatálya alatt nemzeti jogalkotás hiányában is alkalmazhatók lesznek a BCR-re vonatkozó szabályok, így a tagállamok körében semmilyen további akadálya nem lehet a BCR alkalmazásának 2018. május 25. napja után. Az uniós adatvédelmi jog számos egyéb jogi lehetőséget is biztosít a megfelelő védelmi szint garantálására, többek között említhetem az Európai Bizottság a harmadik ország vonatkozásában meghozott megfelelőségi határozatát, amely inkább

Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents

DOI: 10.14750/ME.2019.022

hasonlítható a CBPR tagállami csatlakozási mechanizmusának eredményeként előálló státuszra. Azonban amíg megfelelőségi határozat birtokában a megfelelő védelmi szint biztosítása nem igényel további intézkedést a vállalkozások részéről az adott harmadik országban, addig a CBPR rendszerben a már a rendszerhez csatlakozott ország tanúsított vállalkozása kerül csak hasonló jogi helyzetbe. *Ezért a CBPR rendszere inkább hasonlítható a már érvénytelen Safe Harbor mechanizmusra, amelyben az USA-ban letelepedett vállalkozások csatlakozhattak önként az adatvédelmi rendszerhez. Az Adatvédelmi Pajzs szintén hasonló elven működik, így még mindig közelebb áll a CBPR rendszerhez, mint a BCR.*

Fontos jellemző, hogy a BCR esetén a harmadik ország nem, csak az azt alkalmazó vállalkozáscsoport tagjai közötti adatáramlás során biztosítja a megfelelő védelmi szintet. A CBPR rendszerhez csatlakozó tagállam esetén - valószínűsíthetően - a tagállam jogrendszere is eléri az elvárt védelmi szintet.

Hasonló viszont az ön- illetve társszabályozási jelleg a CBPR és a BCR esetében is. A BCR-t a tagállami adatvédelmi felügyelő hatóságok vizsgálják meg és hagyják jóvá, a CBPR rendszerben viszont megbízottak - akik lehetnek szervezetek vagy a tagállami hatóság is - állapítják meg a megfelelőséget. Azonban míg a BCR inkább mutatja az önszabályozás jegyeit, addig a CBPR formálisan is tanúsításról rendelkezik, a két módszer pedig eltér egymástól, bár eredményét tekintve hasonló hatásúak.

Mindkét rendszer elsődlegesen az adattovábbítások jogszerűségét hivatott biztosítani, egységességi, hatékonysági alapon és a teljes megfelelésre való törekvésre hivatkozással érdemes valamennyi adatkezelésre kiterjeszteni a szabályaik alkalmazását. Azonban a BCR kifejezetten olyan harmadik országokban biztosítja a megfelelő védelmi szintet, amelyek nem rendelkeznek megfelelőségi tanúsítvánnyal, míg a CBPR rendszere elsődlegesen az APEC tagállamok köréből a rendszerhez csatlakozó államokat

DOI: 10.14750/ME.2019.022

érinti. Tehát míg a BCR alapvetően egy, az adatvédelmi politikát az Európai Unión kívül bárhova exportáló jogintézmény, addig a CBPR egy olyan rendszer, amely az APEC tagállamok körében kívánja az adatvédelmi politikát egységesíteni.

Noha a BCR kifelé irányuló kötelező erejének érvényesülésére, tehát az érintettek igényérvényesítési lehetőségeire és eredményeire még nincs gyakorlati tapasztalat, a CBPR rendszerben a szabályok a nemzeti jog ellenében is kikényszeríthetők, ennek érdekében a tagállami adatvédelmi hatóságok jogosultak eljárni.

Míg a BCR-ban egyértelműen meg kell jelölni a felelősséget vállaló vállalkozáscsoporti tagot, amely nem feltétlenül kell, hogy a vállalkozás székhelye szerinti tag legyen, sőt tipikusan nem az, a CBPR esetén csak tanúsított szervezet lehet, és a tagállami felelősségre vonás is megtörténhet a jogellenesen eljáró taggal szemben.

A BCR esetén változásbejelentési kötelezettség áll fenn, azonban nincs egyértelmű gyakorlat a hatósági felülvizsgálat folyamatára, és az éves gyakoriságú bejelentés mellett sem indul újra a jóváhagyási folyamat. Elvárás azonban egy felelős személy kijelölése, aki hatósági felhívás esetén bármikor kész az aktuális helyzetet bemutatni. Ezzel szemben a CBPR rendszerben változás esetén a tanúsító megbízott egy felülvizsgálati folyamatot folytat le és a szervezeteknek nyilatkozniuk kell aktuális helyzetükről.

Az elemzés több szempont alapján is rávilágít arra, hogy a CBPR rendszer sok jellemzője hasonlít ugyan a BCR jogintézményére, de az igazán közös jellemzője csak annyi, hogy az adatvédelem megfelelő szintjét a vállalkozások illetve szervezetek önkéntes alapon vállalt adatvédelmi többletkötelezettségek vállalása útján biztosítja. A CBPR a tagállamok rendszere, amelyben a tanúsítással érhető el a vállalkozások számára a megfelelés, míg a BCR egy

DOI: 10.14750/ME.2019.022

vállalkozáscsoport önkéntesen alkalmazható jogi eszköze. Tehát ismét arra a konklúzióra lehet jutni, hogy próbálunk párhuzamot találni két különböző alapon álló, egyébként hasonló elven működő, céljaiban azonos jogi keretrendszer között.

XI.5. A GDPR és a CBPR közös jellemzői

Ha elfogadjuk a fenti álláspontot, hogy a CBPR a 2004-ben létrehozott Keretendszer egy alrendszere, akkor érdemes azt inkább az Európai Unió adatvédelmi „rendszerével", a GDPR által meghatározott jogi keretrendszerrel összehasonlítani.

Alapvető különbség, hogy míg a GDPR közvetlenül alkalmazandó szabályokat tartalmaz, addig a CBPR rendszer elvei és szabályai nem élveznek prioritást a tagállami nemzeti joggal szemben. Amelyik tagállamban nincs adatvédelmi jogi környezet, ott a CBPR mintegy minimumkövetelmény-rendszerként funkcionál. Míg a GDPR alkalmazandó olyan nem az unióban letelepedett adatkezelőkre is, akik uniós polgár adatait kezeli, addig a CBPR területi hatálya a tagállamok joghatóságával egyezik meg.

Fontos különbség továbbá, hogy a CBPR rendszer kizárólag az adatkezelőkre terjed ki, a GDPR ezzel szemben az adatfeldolgozók szerepét és helyzetét is szabályozza. Ezzel teljes körű védelmi rendszert épít ki. Adatfeldolgozókra vonatkozó szabályok nélkül ugyanis a szabályozás az önkéntes jogkövetés hiányában az érintett számára nem jelent magas szintű védelmet, hiszen az adatfeldolgozási tevékenység kiszervezésével a szabályok már nem alkalmazandók. Ezen túl a CBPR nem tartalmazza az adatvédelmi incidens fogalmát sem. A GDPR további erőssége, míg a CBPR rendszerben csak önkéntesen alkalmazandó, az adatvédelmi incidens jelentésére vonatkozó kötelezettség bevezetése.

DOI: 10.14750/ME.2019.022

A fenti különbözőségeken túl a két adatvédelmi rezsim azonos elvekkel, célokkal és koncepciókkal operál, azonban még a 29. cikk szerinti Adatvédelmi Munkacsoport és az APEC tagállamok Adatvédelmi Alcsoportjának közös álláspontja szerint egyetlen, már jóváhagyott BCR sem eredményezi azt, hogy a vállalkozás adatvédelmi politikája automatikus tanúsítást kaphatna a CBPR rendszerben.

Értékes együttműködés fejlődhetne ki a két rendszer között, ha a CBPR rendszerben tanúsított vállalkozáscsoportot (vagy vállalkozást) ex lege olyannak lehetne tekinteni a GDPR hatálya alatt, mint amely a GDPR 43. cikk szerinti tanúsító szervet bevonásával a 42. cikk szerint elismert tanúsítási mechanizmus alapján a 46. cikk (2) bekezdés f) pontja szerint a felügyeleti hatóság külön engedélye nélkül biztosítaná a megfelelő garanciákat a személyes adatokat harmadik országba vagy nemzetközi szervezet részére történő továbbításakor. Ehhez persze a CBPR rendszer működésének olyan gyakorlati egységesítésére és szigorú folyamatos monitoringozására volna szükség, amely elkerülhetővé tenné a Safe Harbor érvénytelenítéséhez vezető helyzet kialakulását. Ugyanakkor mivel a CBPR szabályai nem élveznek elsőbbséget a tagállami nemzeti joggal szemben, így a vállalkozásra irányadó APEC tagállami nemzeti jog vizsgálata is előfeltétele kellene, hogy legyen az elismerésnek. Ezt elkerülendő érdemesebb BCR alkalmazása mellett dönteni.

DOI: 10.14750/ME.2019.022

XII. FEJEZET
JOGÁGI ÉS JOGTERÜLETI KITEKINTÉS

A személyes adatok védelmének tárgykörét érdemes több nézőpontból megvizsgálni, mert míg az érintettek többsége marginális jogterületként, a folyamatok gátjaként és felesleges többletkötelezettségként tekint rá, a személyes adatok kezelésének korlátok közé szorítása minden érintett érdeke. Hiszen fordított helyzetben az adatkezelők oldalán eljáró személy érintett adatalannyá válik, és saját példáján érezheti meg a jogellenes adatkezelésből eredő kényelmetlenséget, adott esetben kárt vagy személyiségi jogi jogsérelmet. Az értekezés középpontjában egy, az adatkezelők által alkalmazott jogi eszköz sokszempontú elemzése áll, de teljes képet akkor kapunk róla, ha feltérképezzük azt is, hogy miért is fontos az adatkezelőnek a jogi megfelelés a bírság elkerülésén túl. Jelen fejezetben arra helyezem a hangsúlyt, hogy a személyes adat a gazdasági folyamatokban valójában nagyobb érték az adatkezelőnek, mint az érintettnek.

Az adatkezelők személyében is érdekes eltolódás figyelhető meg. A gazdasági szereplők adatkezelési tevékenysége már-már érzékenyebben érintik az adatalanyok magánszféráját, mint az állam adatgyűjtési tevékenysége, amellyel szemben az adatvédelmi szabályozást a kialakulásának kezdetén meghatározni kívánták. Solove[351] a személyes adatok védelmére vonatkozó legsúlyosabb veszélyként már 2001-ben is azt azonosította, hogy a szabályozási környezet kiforratlan és nem biztosít valós kontrollt az adatok gyűjtése, kezelése és továbbítása során. Rátapint arra is, hogy az állam és a közigazgatás adatgyűjtésén túl a „kistestvérek", a gazdasági szereplők egyre veszélyesebb tényezők. Jellemzően az érintett érdekének, a szolgáltatás jobbításának céljával igyekeznek igazolni a sok esetben indokolatlan volumenű adatgyűjtést és adatkezelést, azonban a profitszerzés érdeke valójában hangsúlyosabban jelenik meg.

[351] SOLOVE (2001)

DOI: 10.14750/ME.2019.022

A személyes adat a XXI. század olaja.[352] Egyszerűen belátható, hogy az adatok, kiemelten a személyes adatok, korunk egyik legértékesebb javainak tekinthetők. Az adatok sokcélú felhasználása az információs társadalomban mindennapos gyakorlat.

Az álláspontom azonban az, hogy az *adatalany éppúgy felelős a privacy paradoxon*[353] *kialakulásáért és térnyeréséért, mint az adatkezelő*. Jelen fejeztben arra vállalkozom, hogy a személyes adatokat mint gazdasági javakat a középpontba állítva igazoljam, hogy az adatvédelmi jogi szabályozásra szükség van, az önszabályozás és így a BCR kiegészítő eszköz lehet az érintettek helyzetének megerősítése körében. Az előző fejezetekben az adattovábbítások jogi környezete és a BCR állt a kutatás fókuszában, ebben a fejezetben rövid kitekintés teszek annak érdekében, hogy a személyes adatok jelentőségét elméleti szemptonú megközelítés útján mutassam be. A fejezet ténylegesen rövid és kitekintő jellegű, hiszen noha témája releváns, a hazai szakirodalomban kevéssé lelhető fel és valamennyi aspektusa jelen sorokban nem mutatható be, azonban fontosnak találom, hogy a tételes jog elemzésének szükségességét és helyességét elméleti megalapozás is támogassa.

XII.1. Pareto-hatékony-e az adatvédelem?

A jog gazdasági szemléletű elemzésének irányzatát alkalmazom az adatvédelmi jogi környezet jogelméleti vizsgálatához.

A vizsgálat tárgyának azonosításához a jogterület kezdeti fő fogalmát, a magánélet védelmét tekintve elsősorban a common law jogrendben gyökerező privacy fogalmának tisztázását tartom szükségesnek azzal a fenntartással,

[352] The Economist: Regulating the internet giants - The world's most valuable resource is no longer oil, but data, https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [2017. október 29.]
[353] BART - JONG (2017) p. 1039.

DOI: 10.14750/ME.2019.022

hogy „tárgyát körülírás nélkül, egyetlen magyar szó használatával meghatározni […] nem lehetséges”,[354] pedig „egy fogalom meghatározására irányuló bármely kísérletnek annak a szónak a köznyelvi használatát kell kiindulópontnak vennie, mely a kérdéses fogalmat jelöli.”[355] Talán éppen ezen ellentét adja a megoldást, hogy az angol terminológiát nem tudjuk magyarra fordítani, amely szakértők vitáinak sokaságát kerülné el, miszerint a magyar köznyelvi szóhasználatban a privacy szó tulajdonképpen nincs jelen, így lehetetlen vállalkozás fogalmának meghatározása. Talán az is állítható, hogy rossz maga a törekvés, hogy egyetlen szóval akarjuk a fogalmat helyettesíteni. Azt állíthatjuk, hogy „a magánélet védelmének […] egyik leghatékonyabb jogi eszköze a személyes adatok védelméhez való jog garantálása. […] A háborítatlan magánélethez való, ennél mindenképpen tágabb jog általános elismerése a tizenkilencedik század végén az amerikai jogrendszer fejlődésének eredménye volt, azonban amelyeket a magyar Alkotmánybíróság azonos fogalmaknak tekint.”[356]

A sokszor idézett személyi-szám határozatként ismertté vált 15/1991. (IV.13.) AB határozat pontosan körülírja azokat a garanciális feltételeket, amelyek megléte esetén az alkotmányos alapjogként deklarált személyes adatok védelméhez való jog érvényre juthat az egyes adatkezelések, adatfeldolgozások során. Az idő előrehaladtával e garanciák a technológia fejlődésével mindinkább mindennapjaink részévé váltak és könnyebben megvalósíthatók. Ugyanakkor számos új tényező jelent meg, amelyek ugyancsak a technológia fejlődésével nagyobb volumenű és más típusú kockázatot jelentenek.

[354] SZABÓ (2005) p. 44.
[355] KELSEN (1945) p. 4.
[356] SZABÓ (2005) p. 44.

DOI: 10.14750/ME.2019.022

Ahogy gazdagodik az elérhető – anyagi és szellemi – javak köre, úgy alakulnak ki az emberben új, immár tisztán kulturális eredetű igények. Összességükből az önrendelkezés fogalma bontakozik ki, az információs önrendelkezésre pedig ennek a része. Adatvédelmi szempontból a privacy az információs önrendelkezéshez áll a legközelebb: mindenki maga dönt arról, hogy milyen információt oszt meg másokkal magáról illetve milyen információt nem tár a nyilvánosság elé. Azaz az egyénnek joga van ahhoz, hogy magáról döntsön, amely kiegészül az egyénre vonatkozó ismeretekre is, hiszen az egyént egyre inkább adatok (pl. ügyfélkódokhoz, szerződésszámokhoz, belépő azonosító számokhoz, e-mail címekhez kapcsolt adatsorok) határozzák meg mások számára. Így a „személyiség virtualizálódik", azonban az emberekre vonatkozó információk sem szabad forgalmú javak.[357] Mindamellett, hogy egyetértek az állítás értékítéletével, számos hétköznapi példa bizonyítja, hogy személyes adataink önmagukban és mások adataival listába szedve mégis kereskedelmi forgalom tárgyát képezik. A direkt marketerek listákat adnak-vesznek, felhasználóként számos olyan ingyenes szolgáltatást, például az internetes tárhelyeket veszünk igénybe, amelyért valójában adataink további felhasználásra történő rendelkezésre bocsátásával fizetünk. A különböző szolgáltatások által létrejövő adatcsomagok megnövelik ugyan az adatvédelem sikertelenségének kockázatát,[358] ugyanakkor a létrehozó szolgáltató számára jelentős adatvagyonnak minősül. A privacy-paradoxon[359] fogalma is erre utal, mely szerint az érintettek elvárják személyes adataik védelmét, azonban erre nem hajlandók (anyagi) javakat áldozni, és akár csekély előnyökért is szolgáltatják különleges adataikat is.

[357] SZABÓ (2005). p. 46-47
[358] BÖRÖCZ (2014) p. 155.
[359] ACQUISTI (2013) p. 16.

DOI: 10.14750/ME.2019.022

Az adatvédelem jogelméleti megközelítésének elemzésére megfelelő irányzat a jog gazdasági jellegű elemzése. A *benthami utilitarizmusban* gyökerező irányzat az 1980-as évekre, leginkább a common law jogrend országaiban vált népszerűvé, azonban a hasznosság elvéből kiinduló megközelítés mindkét klasszikus jogcsaládban egyaránt megjelenik.

Luhmann „*elvárás-biztonság*" koncepcióját az adatvédelemre alkalmazva a következő példát kapjuk: az érintett elvárása, hogy az adatkezelőnek önként megadott adatait az az ismertetett célnak megfelelően, a szükséges időtartamban és a megfelelő műveletekkel jogszerűen kezelje. Elvárja az érintett azt is, hogy amennyiben az adatkezelő nem így cselekszik, igényével bírói úton léphessen fel az adatkezelővel szemben. Az elvárásokban a jövőt tételezzük föl, amely magában hordozza a „csalódás" lehetőségét, példánkban a jogellenes adatkezelés esetét, amely következtében újabb elvárásaink lesznek, például az igény peresítésének lehetősége. A magatartás minták normaként tételezettek, garanciát állítva a jog által tételezett elvárásaink mellett.[360]

A *gazdaságosság* igénye azonban számos ponton áttöri az elvárásaink által állított kereteket: az adatkezelő mindaddig birtokában kívánja tartani adatainkat, ameddig esélyét látja, hogy azt felhasználva profitra tud szert tenni. Az adatkezelő szeretne minél több adatot kezelni, amelyekből személyiségprofilt alkotna rólunk. Az adatkezelő esetleg visszterhes ügylet keretén belül tovább is adná adatainkat. Más célokra is felhasználná adatainkat, mint azt eredetileg közölte velünk, amelyből további előnyt szerezhetne. A gazdaságossági megfontolásokat azonban felülírják jogszabályok, amelyek a fenti magatartások egyikét sem engedik. Adódik a kérdés, hogy *a gazdasági racionalitáshoz igazodik-e a jog*?

[360] Részletesen lásd: LUHMANN Niklas: A jog pozitivitása mint a modern társadalom feltétele In: Jog és szociológia, Válogatott tanulmányok KJK, Budapest 1979. p. 123-142.

DOI: 10.14750/ME.2019.022

A gazdasági jogelmélet szűkebb értelemben az a racionális mérlegelés, amely mint Posner is, mindent pénzbeli kifejezésre összpontosít. A joggazdaságtani elemzésének „emberképe szerint az embernek vannak koherens, önellentmondás-mentes preferenciái, és mindig minden helyzetben azt a megoldást választja, amely az ő preferenciái alapján jobbnak tűnik."[361] Két ellenérdekű fél viszonyában ugyanaz az ok (adatvédelmi intézkedések betartása) az egyik fél számára kedvező (például a vevő személyes adatainak maximális védelme), míg a másik fél számára kedvezőtlen változást eredményez (például az eladó számára nagyobb költség, kisebb profit), ám ha az érintett szubjektív jólétérzete, elégedettsége nagyobb lesz, mint az adatkezelő elégedetlensége, összességében az össztársadalmi jólét növekedéséhez járul hozzá.[362] A normatív joggazdaságtan kiindulópontja a Pareto-hatékonyság elve, amelynek jelentése, hogy vagy mindkét fél helyzete javul, vagy egyikük helyzete úgy javul, hogy a másikét nem rontja. *A fenti hipotetikus eset tehát Pareto-hatékonynak bizonyulhat.*

A gazdasági szereplők saját anyagi érdekből vállalják a személyes adatok és a magánszféra *(belső) szabályzat* deklarálásával történő tiszteletben tartását. Az adatvédelmi intézkedésekkel minimalizálják a jogsértés kockázatát és a bírság lehetőségét, továbbá növelik a fogyasztói bizalmat. A fenti gondolatot kiterjesztve arra juthatunk, hogy nem alkalmazni adat- és magánszféra-védelmi szabályokat költségesebb, de legalábbis kevésbe nyereséges, mint alkalmazni azokat, de hangsúlyosan csak hosszú távon. *Laudon* arra az álláspontra helyezkedik, hogy nem jogszabály vagy intézményes védelem a megoldás a privacy paradoxon helyzetre, hanem egy erős *információs piac* létrehozása, amelyben kiegyenlítettek az érintett és az adatkezelő jogai és érdekei valamint profit-orientált magatartása is.[363]

[361] SZALAI (2013) p. 1-71.
[362] TÓTH (2004)
[363] LAUDON (1993) p. 1-31. (részletesen jelen dolgozat további fejezeteiben)

DOI: 10.14750/ME.2019.022

A jog feladata az, hogy az emberi szükségleteket kielégítse, minél igazságosabb módon, azaz a jognak társadalmilag hasznosnak kell lennie.[364] A jog jogi jellegének és a gazdasági jellegének tehát közelebb kell esnie egymáshoz a magatartásszabályok vonatkozásában. Ennek egyik lehetősége a gazdaság önszabályozása. Az adatvédelem GDPR-beli uniós vívmányai is ezt a módszert erősítik. A jog szabályait és garanciáit a gazdasági szereplők magukra szabva alkotják újra saját szabályrendszerként, így alkalmazhatóbbá, életszerűbbé teszik azok kötelező betartását. Ennek eszköze lehet a BCR is, hiszen kötelező normaként fejti ki hatását a vállalkozáscsoportok igazgatására és eljárásaira jogalkotói aktus nélkül is, hatósági jóváhagyás és a bírói kikényszeríthetőség mellett.

XII.2. Eltérő érdekállások

A posneri felfogás[365] szerint a privacy olyan *fogyasztási cikk*, mely félkész, de igen hasznos gazdasági jószág, melyeket jólétünk és bevételeink érdekében használunk fel. Sajátos analógiát állít fel a személyes adatok védelme és a közgazdaságtan, kereskedelem vonatkozásában. Úgy véli, hogy az emberek termékekhez hasonlóan adják el magukat, és amennyiben bizonyos jellemzőiket eltitkolják – azaz személyes adataik egy részét nem tárják a nyilvánosság elé – túl jó színben tüntetik fel magukat, eltitkolva a „termék" valós tulajdonságait. Posner arra a konklúzióra jut, hogy egyenesen elítéli, hogy jogszabály biztosít jogosultságot arra, hogy az egyén információt titkolhat el magáról, mert az torzítja, megtéveszti a piacot. Jellemző esete, ha egy állásinterjún a jelentkező valótlan képet mutat magáról, akkor a leendő munkáltató nem a legmegfelelőbb jelentkezőt fogja alkalmazni, amely következtében a hasznossági tényező nem lesz kielégítő a munkáltató számára.

[364] TÓTH (2004)
[365] POSNER (1978) p. 393-422.

DOI: 10.14750/ME.2019.022

Mindemellett Posner is elismeri, hogy a hátrányos üzleti tranzakcióktól csak úgy lehet az egyénnek megóvnia önmagát - amihez természetesen joga van -, hogy nyilvánosságra nem hozott magánszférájának jellemzőit mások nem kutathatják fel. Az adatvédelmi szabályozás azonban alapvetően nem az érintett „titkolózásához" való jogának biztosításán alapul, hanem a jogszerű adatkezelés kötelezettségét írják elő. Az egyik legfrissebb felmérésben[366] arról kérdezték az uniós polgárokat, hogy mennyire bíznak a különböző gazdasági társaságok és nemzeti hatóságok adatkezelési módszereiben.
A megkérdezettek az interneten szolgáltatásokat nyújtó cégek adatvédelem terén nyújtott biztosítékaiban kételkednek leginkább – megjegyzem, hogy a gyakorlat azonban nem tükrözi ezt az aggodalmat, hiszen az internetes szolgáltatások igénybe vétele napról-napra növekszik -, a legbiztonságosabbnak pedig az egészségügyi intézményeket, valamint a bankokat tartják. Hasonló jó arányban bíznak a nemzeti hatóságok és az uniós szervek adatkezelésében, míg a telefonos értékesítési tevékenységgel foglalkozó cégekbe vetett bizalom jóval elmarad ettől. A pénzügyi helyzetre vonatkozó adatok, majd az egészségügyi adatok, a személyi azonosító számok, ezeket követik az ujjlenyomat és a lakcím azon a listán, amelyen az érintettek a számukra legféltettebb adatokat sorolják. Legkevésbé féltett személyes jellegű adat a személyes vélemény, a nemzetiség, a szabadidős tevékenységekre vonatkozó adatok és végül a weboldalak látogatása. Téves azonban az elképzelés, hogy pénzügyi viszonyaink a legfontosabbak a szolgáltatók, a kereskedelem számára. Ismét a direkt marketer példáját említem, aki a látogatott weboldalak, a cookie-k alkalmazásával, a kereséseink elemzésével kínálja számunkra a „legmegfelelőbb" termékeket és szolgáltatásokat megvásárlásra.

[366] Európai Bizottság: Social Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union, 2011, Brüsszel, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [2015. május 25.]

DOI: 10.14750/ME.2019.022

A szükséges rossz jellemzően megjelenik bizonyos *szolgáltatások, például online tárhelyszolgáltatás igénybe vétele esetén* is. A tárhely használatának feltétele, hogy levelezésünk teljes tartalma és a hozzá kapcsolódó metaadatok is a szolgáltató rendelkezésére állnak. Itt az a mérlegelendő helyzet, hogy az érintett számára ér-e annyit az igénybe vehető szolgáltatás annál, hogy a fenti adatkezelésbe beleegyezzen. Elegendő azonban az interneten böngészni, vagy a legnagyobb keresőmotorokat használni, amelyek aztán webtracking és a cookiek alkalmazásával hamar viselkedés-alapú hirdetéseket fognak generálni a felhasználó számítógépén. Az adatainkat, sok esetben magánéletünk egy teljes szeletét - személyes adatainkat, földrajzi helyzetünket, preferenciánkat, keresési előzményeinket, vásárlási szokásainkra vonatkozó ismétlődő adatsorokként - adjuk át fizetségként azokért a szolgáltatásokért, amelyeket „ingyenes" igénybe vehetünk. A fogyasztók mindig felülértékelik az olyan javakat, szolgáltatásokat, amelyek ingyen vannak, és ingyenesnek tekintenek minden olyat is, amelyért személyes adataikkal „fizetnek". Így a szolgáltatók számára nemcsak fogyasztókká, hanem egyidejűleg termékké is válunk. Posner elmélete szerint az érintett adatai közbenső javak, amelyeket az érintett anyagi javak, más előnyök vagy hasznos eredmény létrejöttéhez használ.[367]

XII.3. Szerződéstani megközelítés[368]

A *kereslet és a kínálat* egymást feltételezik. Természetes közvetett termékként jön létre például a fogyasztói adat bármely vásárlás, internetes tranzakció, bármely interakció alkalmával.[369] Ha pontosan ismerjük a felek preferenciáit, könnyebbé válik a jogügyleteket sikerre vinni. Ha az eladó részletes információk birtokában volna vevője céljáról és anyagi helyzetéről, akkor a szerződéskötést megelőzően felmerülő költségeket és a haszontalansági tényezőket redukálni lehetne, így növelve a megtakarítást és a *hasznot*.

[367] POSNER (1978) (2) p. 19.
[368] VARIAN (1996)
[369] HUANG (1998) p. 7.

DOI: 10.14750/ME.2019.022

Az egyénre szabott, „perszonalizált reklámoknak gazdaságélénkítő hatásuk van, mert sokkal nagyobb a valószínősége annak, hogy a felhasználó rákattint arra a hirdetésre, amely érdeklődési körével megegyezik."[370] Ugyanakkor súlyosan hátrányos lehet bizonyos szerződések esetén, ha a szerződő fél olyan információt ismerne meg a másik félről, amely befolyásolja a szerződés lényeges elemeit. Az *életbiztosítás*i szerződés megkötése során kiemelt fontosságú a biztosított magánéletét érintő kérdések, például a dohányzás, genetikai betegségek előfordulása a családban, amelyek jelentősen befolyásolják a biztosítót a díj megállapításában. A felek között eltérő az információigény, információs aszimmetria áll be, és ezen különbség kielégítése szükségszerűen járhat a magánszféra sérelmével, de legalábbis a személyes adatok mint javak iránti igény megnövekedésével.

Varian azt állítja, hogy a magánszférához fűződő bizonyos jogokat, például a személyes adatok kezelését, felhasználását bérbe lehet adni különböző célokra, például gyűjteni lehet egy levelező listán, azonban ezek továbbadása csakis az érintett kifejezett hozzájárulásával történhet meg. Kérdéses azonban, hogy az érintett kifejezett hozzájárulásával létrehozott listák mennyiben tekinthetők a listák készítőinek szellemi tulajdonának, azok képezhetik-e visszterhes adásvételi, bérleti, használati … stb. szerződés közvetett tárgyát, azaz eladhatják-e azokat, bérbe adhatják-e azokat, és amennyiben igen, hogyan érinti ez az érintettek információs önrendelkezését. Ezt megelőzi az előkérdés is, hogy a személyes adatokkal miként rendelkezhet, rendelkezhet-e tulajdonjog tárgyaként az érintett?

A személyes adatokat mint tulajdonjog tárgyait Westin nagy hatású 1967. évi cikke[371] óta vita övezi. Egyes szerzők már - különösen az USA-ban – régóta létező jelenségként írják le azt, hogy a személyes adatok áruvá

[370] BÖRÖCZ (2014) p. 150.

[371] WESTIN (1967) p. 114-115.

DOI: 10.14750/ME.2019.022

válnak, információs javak[372], a piacon mérhető értékkel bírnak, így azok el is adhatók. Az USA-ban attól, hogy a személyes adatot egyre inkább tulajdonjog tárgyaként azonosították,[373] azt várták, hogy áthidalható a jogi szabályozás hiánya és az érintetti kontroll tudatos növelésével a védelem szintje is emelhető, az adatvédelmi incidensek visszaszoríthatók azáltal, hogy a beépített adatvédelem elvén az adatkezelők tudatosan alkalmaznak adatvédelmi intézkedéseket. Amennyiben elfogadjuk, hogy a személyes adat tulajdonjog tárgya lehet, másszóval rendelkezni lehet róla, úgy kérdés, hogy az az érintett vagy az adatkezelő tulajdona-e, és mi az alapszabály – ha van egyáltalán – a továbbítására, esetleg eladására vonatkozóan. *Három érvcsoport* köré gyűjthető össze a szemlélet támogatóinak köre.

Az *első*, például Murphy[374] vagy Lessig[375], aki szerint a tulajdonjogi szemlélet lényege abban áll, hogy a személyes adat nyilvánosságra hozataláról – vagy titokban tartásáról – az adat tulajdonosa dönthet, aki lehet akár az érintett, akár az adatkezelő is.

A *második* érvcsoport Bergelson[376] tollából az, hogy a tulajdonjogi szemlélettel bírói úton kikényszeríthető, a jogsértést megelőző jellegű felelősségi szabály alakítható ki, amely az érintett számára kártérítést biztosít jogellenesség esetére.

A *harmadik* érvcsoport képviselője Cohen,[377] aki szerint a jog, a technológia és a piac hármasa olyan feltételeket képes teremtetni az érintett számára, amelyek a szerzői joghoz hasonlóan biztosítanak az érintett számára lehetőséget arra, hogy meghatározza személyes adatainak sorsát. Ehhez persze arra is szükség volna, hogy legyenek alapvető szabályok az adatok

[372] REICHMAN – SAMUELSON (1997) p. 51-166.
[373] Bár az alapelv még mindig az, hogy a személyes adat egyetlen ember tulajdona sem lehet.
[374] MURPHY (1996) p. 2383-2384.
[375] LESSIG (2002) p. 247.
[376] BERGELSON (2003) p. 430. Vera Bergelson: It's Personal, but Is It Mine? Toward Property Rights in Personal Information, U.C. Davis Law Review 37, 379, 2003, p. 430
[377] COHEN (2000) p. 1437-1438.

DOI: 10.14750/ME.2019.022

„kereskedelmére", akár szerződéstani megközelítésűek is. Azonban, ahogy Purtova[378] is kiemeli, ez a szemlélet az amerikai tulajdon-felfogásban, az amerikai - gyenge - adatvédelmi jogi környezetben alakulhatott ki, és ott terjedhetett el. Az európai olvasó számára Purtova üzenete az, hogy amennyiben a tulajdonjogi szemléletet az európai jogrendszerekbe is be kívánják vezetni, úgy vegyék fontolóra annak piaci, és a piacon túli, védelmi funkcióját is. Ezt az amerikaiak elmulasztották megtenni, álláspontja szerint.

Az adat a gazdasági növekedés elengedhetetlen eleme lett, különösen a negyedik ipai forradalomban, amelyet az okos eszközök és az adat-vezérelt digitális környezet ural. A személyes adat tulajdonjogi megközelítésének elfogadása az érintett számára lehet igazán előnyös, hiszen a szerződéses láncolatban visszanyerheti az adatai feletti tényleges kontrollt. Purtova[379] a földtulajdonhoz hasonló szabályozási és jogosultsági szintek mentén kezelné az adatok helyzetét is: nem korlátozhatatlan, de legszélesebb rendelkezési jog illetné meg az érintettet, aki jogosult az adatai továbbítására és átadására, ellenszolgáltatás fejében, míg az adatkezelő csak a bérlő mintájára bizonyos korlátos használati jogokkal bírna csupán, amelyeket a célhoz kötöttség vagy a cél eléréséhez szükséges időtartam szorítana keretek közé. A kritikus tényező az, hogy milyen körülmények között, meddig minősül személyes adatnak az adott ismeret, tehát a beazonosíthatóság, azaz az érintett és az adat összekapcsolhatósága az adat gazdasági értékét is befolyásolja. Egy statisztika, egy anonimizált ismeret kevésbé lesz értékes, mint egy az érintett maga által vagy megfigyeléséből keletkező, egy adott érintettről szóló ismeret. Ezen a ponton pedig megállapítható az is, hogy az adathalmaz, legyen az bármekkora is, értéke azon múlik, hogy az egyes egyének beazonosíthatók-e. Tehát valódi értéket mégsem az adatok összegyűjtött halmaza, hanem egy-egy, az érintettel összekapcsolt adat hordoz, az adatösszesség csupán értéknövelő tényező, de nem az érték eredője.

[378] PURTOVA (2009) (1) p. 507-521.
[379] PURTOVA (2017) (2)

DOI: 10.14750/ME.2019.022

Schwartz[380] szerint az elektronikus adathalamazok és ezek metaadatai a legnagyobb magánéletre és személyes adatok védelmére gyakorolt hatása az, hogy valójában titkos adatgyűjtés zajlik, mert az érintett ténylegesen nem tudhatja, hogy róla milyen adatokat, milyen célból és meddig tárolnak. Súlyosbítja a helyzetet az, hogy nem lehet kitérni az adatgyűjtés útjából.

Helyesen állapítja meg, hogy a technológia alakítja értékes áruvá a személyes adatot. Az áruvá vált adatoknak pedig különböző köreit azonosítja: az első azoknak a listája, akik áruba bocsátották személyes adataikat, a második az ő érdeklődési körük és a nekik szánt célzott hirdetések alapjául szolgáló adatok, a harmadik kör ezen érintettek tranzakcióihoz és szerződéseikhez kapcsolódó adatok valamint a negyedik az ezekhez kapcsolódó metaadatok, a különböző körökbe tartozó adatok értéke a piac aktuális helyzetétől és az adatkezelő személyétől függ.

A magánszférához való jog gazdasági elemzésének első sarok köveit letevő S. D. Warren és L. D. Brandeis[381] az „egyedül hagyáshoz való jogot" a tulajdon fogalmának kibővüléséből eredezteti. A nem kézzelfogható tulajdonformák kialakulása oda vezetett, hogy a birtokháborítás és az emberi *test fizikai védelme is átalakult*, és a személyiség sérthetetlensége az „érzelmek tiszteletben tartására is kiterjedt, az élet jogi fogalmának részévé vált a családi viszonyok, érzelmi kötelékek" köre is. A *becsületsértés és rágalmazás* cselekményével állították párhuzamba a magánélet elleni támadásokat, melyek elsődleges elkövetőjének a sajtót találták. Állították, hogy a magánszféra fenntartásához való általános jog alkalmazására volna szükség, amely egyfajta tulajdonjog érvényesítése, amelyet a publikálatlan művek a szerző, alkotó engedélye nélkül történő nyilvánosságra hozatalával hasonlítottak össze. A dolog, amely védelem alatt áll, a „*magántermészetű esemény*" (domestic occurence).

[380] SCHWARTZ (2004) p. 2055-2128.

[381] WARREN-BRANDEIS (1980) p. 193-220.

DOI: 10.14750/ME.2019.022

A *szellemi tulajdon védelméhez* hasonlóan nem a fizikai eltulajdonítás ellen szükséges a védelem, hanem a nyilvánosságra hozatal ellen, amely nem a magántulajdon, hanem a személyiség sérthetetlenségéből ered. Így a magánszféravédelem és az adatvédelem több a tulajdonjognál, de mára kevesebb is annál.[382]

A személyes adat tulajdonképpen az érintett és az adatkezelő viszonyában keletkező termék. A személyes adatot nem az érintett hozza létre, hanem leginkább az adatkezelő, többnyire az összekapcsolás illetve a következtetések levonása révén. A személyes adat értelmezhető akként is, hogy az az adatkezelő által létrehozott szellemi termék, amellyel aztán szabadon rendelkezhet. Ez persze a legkevésbé támogatott álláspont.

XII.4. Szabad piac, mintsem a túlszabályozás – egy megoldási javaslat

Egy *másodlagos (adat) piac* jön létre, amelynek javai a személyes adatok. Felhasználásuk profitot eredményez az adatok kezelőinek hosszú távon, az érintett számára jellemzően rövidtávon. Hosszú távon az érintett adatai korlátlan kiadásával kiszolgáltatottá[383] válik az adatkezelőknek, szubjektív sérelem, ha az érintett immár „megfigyeltnek" érzi magát, [384] és az ellenőrzés lehetőségét is elveszíti személyes adatainak útja felett. Solove[385] rámutat arra, hogy az érintettek információs önrendelkezése – Solove self-management-tnek nevezi - nem jelent tényleges kontrollt az adatok felett, ennek okaiként pedig az egyén személyes kognitív képességeinek - informáltság, döntésképesség, időtényező - hiányát, az adatkezelők sokaságát mint strukturális porblémát és az általuk aggregált adatösszességek létrehozásának tényét azonosítja. Azt is állítja, hogy az adatvédelmi költségek és hasznok az egyén szintén kevésbé,

[382] Schermer (2015)
[383] Mindennapi példa az árdiszkrimináció jelensége.
[384] ACQUISTI (2010) p. 15.
[385] SOLOVE (2013) p. 1880. Solove, Daniel, J. (2013): Introduction: Privacy Self-Management and the Consent Dilemma, Harward Law Review, 7.sz. pp. 1880-1903. http://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma [2019.02.25.)

DOI: 10.14750/ME.2019.022

inkább kummuláltan és holisztikusan értelmezhető igazán. Az adatvédelmi szabályozásnak új irányt kell vennie, szerinte egy nem túlzottan paternatilisztikus, de bizonyos alapvető normákat pontosan határolt módon megfogalmazó, következetes szabályozás kialakítása volna kívánatos.

A *kitöltetlen csekk* metaforájával él Acquisti: eszerint amikor az érintett személyes adatait rendelkezésre bocsátja egy kitöltetlen csekket ad ki. Lehetséges, hogy a csekket sosem váltják be. Meglehet, hogy egy „kisebb összeggel töltik ki és váltják be", például kéretlen levelekhez, direkt marketing hívások bonyolításához használják fel az adatokat. Egy „nagyobb összeg" például a teljes személyiség lopás.

A személyes adatoknak óriási ma a piaca, és ezeken a javakon a tulajdonjogot nem az egyes érintettek, hanem azok gyakorolják, akik ezeket az adatokat összegyűjtik, rendszerezik, majd az egyes szempontok szerint elkészült összeállítást visszterhesen eladják például a direkt marketernek, írja Varian, és a laudoni *Nemzeti Információs Piac* létrejöttét vizualizálja lehetséges jövőképként.

Laudon Nemzeti Információs Piacának elképzelése a korábban már vázolt, a gazdaságban jelen lévő információs asszimmetria feloldásának kínál úttörő megoldást. Kiemeli, hogy nem a technológia fejlődése a hibás az egyre gyakoribb privacy-t sértő folyamatokban, hanem a helyzet, amit mi magunk alakítottunk ki. Elveti a szabályozásra és állami hatósági felügyeletre hagyatkozó nézeteket, és egy piaci alapú, profitorientált megoldást kínál, amely szerinte a társadalmi elfogadhatóság határán belül marad, ugyanakkor hatékonyan szolgálja ki a piaci igényeket úgy, hogy minden résztvevő nyertesnek érzi magát.[386]

[386]Posner idézett műveiben azt állítja, hogy a jogszabályi védelem csupán a tranzakciós költségeket növeli meg és lehetővé teszi a megtévesztést is, bizonyos adatok eltitkolásának lehetőségét biztosítva. Posner (1978) p. 22.

DOI: 10.14750/ME.2019.022

Elképzelése szerint az érintett szolgáltatja adatait és a Piacon belül egy központi irányító vállalat azokat mindig ahhoz a csoporthoz rendeli, amelyben hasonló tulajdonságú vagy preferenciájú személyek adatai vannak. Aki az egyes csoportoknak kínálna terméket vagy szolgáltatást, megveszi az adott adathalmazt, amelynek az árából osztaléknak nevezett hányadot kap az adatait szolgáltató érintett. Aki ezt az összeget, nevezzük a „zavarás árának" alacsonyabbnak értékeli, mint amennyit a „zavartalansága" érne meg számára, eltávolíttathatja nevét a listákról.

Az érintetteknek saját fiókja volna egyedi azonosító kóddal és jelszóval, így az információáramlás teljes felügyeletük alatt állna. Nyomon követnék, hogy a Piacon rendelkezésre bocsátott adataikat hányan, kik vásárolják meg, és ezen tranzakciók után bizonyos osztalékban részesülnek, amelynek volna egy rögzített minimuma, azonban felső határa nincs. A fiók blokkolásának jogával az érintett megtilthatná adatai további „forgalmazását". Ügynökök is működnének a Piacon, akik bizományos módjára járnának el a rájuk bízott adatok értékesítése során. A közigazgatási szerveknek főszabály szerint nem kellene fizetnie az adatokért.

Éles kritika illeti az elképzelést,[387] amelyek szerint a folyamat önmagát gerjesztené és az adatvédelmi incidensek száma tovább nőne. Az érintettek között diszkrimináció állna be anyagi körülményeik alapján, a növekvő érintetti ellenőrzés mellett is kevésbé maradhatna titkos a magánélet. Laudon állítja, hogy a Piac az egyetlen hatékony jogi megoldás az egyének személyes adatainak másodlagos célra történő további felhasználására. [388]

Az információs piac álláspontom szerint *létezik*, de nem a fentiek szerint intézményesült formában, az érintettek tudatos adatszolgáltatása és az adat-vásárlók által fizetett osztalék nélkül.

[387]LAUDON (1993) p. 21.
[388] LAUDON (1993) p. 18.

DOI: 10.14750/ME.2019.022

Az adatkezelők hatalmi helyzetben vannak, az érintettek számára pozitívumként kell értékelni, ha a kötelezően szolgáltatandó adatok körét bizonyos korlátok közé lehet majd szorítani. Érintettként - sajnos - nem vagyunk alkupozícióban. Kétséges, hogy nemzeti szinten hatékony volna-e a Piac működése, nemzetközi szintre vagy nemzetközi elemmel bővítve pedig a joghatósági, az alkalmazandó jog és adatvédelmi standardok, devizaárfolyamok, pénzügyi tranzakciók kérdéseit kell megválaszolni. Már 2005-ben egy teljes személyes adatokra épülő iparágat azonosítanak az amerikai gazdaságban,[389] amely a számítógépek elterjedésével és az IT iparággal párhuzamosan fejlődik és növekszik, hiszen az adatokat könnyedén és szinte mennyiségi korlátok nélkül lehet digitalizálni, tárolni, majd az így létre jött adatbázisokat szűrni vagy éppen eladni. Az iparág szereplői kiemelik a technológiai eszközök nyújtotta előnyöket, ugyanakkor a már szokásjogi alapon kialakult piaci gyakorlat formális szabályozását elkerülnék. Somogy két hírhedt adatvédelmi incidens[390] bemutatásával igazolja, hogy a rohamosan növekvő bevételekkel gazdálkodó piaci szereplők egy szabályozatlan környezetben többnyire az érintett tudta nélkül gazdálkodnak az összegyűjtött személyes adatokkal, amely helyzetet csakis a jogi keretek kialakításával lehet a helyes mederbe szorítani. A Személyes adatvédelmi modell rezsim 2.0. (Model Regime of Privacy Protection v. 2.0) jogi keretrendszert alkotta meg Solove és Hoofnagle[391] azzal, hogy a Laudon féle elmélethez képest több ponton további garanciákat vezettek be. Az egyik, hogy „egyablakos" rendszerben volna lehetősége az érintettnek, hogy jogait érvényesítse, többek között azt is, hogy az adataihoz minden egyes hozzáférés igénylést egyedileg bíráljon el, és adott esetben tagadjon meg. Egybeesik a GDPR szellemiségével és szabályozásával a modell rezsim azon jellemzője, hogy működtetni kell benne egy olyan mechanizmust, amellyel az érintett tudomást szerez a megtörtént adatvédelmi incidensekről. A modell rezsim a magánnyomozók

[389] SOMOGY (2012) p. 901
[390] A ChoicePoint és a LexisNexis amerikai adatbrókerektól hekkerek összesen közel 800 000 amerikai személyes adait, köztük különleges adatokat, biztosítási adatokat és vezetői engedélyek adait, lopták el.
[391] SOLOVE-HOOFNAGLE (2005)

DOI: 10.14750/ME.2019.022

elszámoltathatóságára is hangsúlyt fektetne, és korlátozná az állami szervek vásárlási lehetőségeit is, tekintettel arra, hogy a harmadik személytől, például a vevőtől megvett adatok az eladó tevékenységére nézve is szolgáltatnak adatot. Az állami adatbányászat felett bírói kontroll és a nyilvános elszámoltathatóság állna.

XII.5. Jogelméleti összegezés

A személyes adatok védelméhez való jog a gazdaságosság szempontjából több nézőpontból vizsgálható. Ha a szabadságjog oldaláról közelítjük, nincs relevanciája. Ha a titkolózáshoz való jogként tekintünk rá, akkor csekély, de gazdaságilag releváns javakként értékelhetők a személyes adatok. Ha a személyes adatok rendelkezésre bocsátásának lehetőségeként vizsgáljuk, akkor a hasznossági mutatók fókuszába kerülhet. Egy amerikai állampolgár például 29 dollárt hajlandó fizetni személyes adatai védelemért, és mindössze 50 centtel fizetne többet egy olyan termékért, amelyet a személyes adatok védelmére intézkedést tett kereskedő kínál.[392]

A jog legyen akár eszköztár, akár érvényességi forrás, az önszabályozás egy további megoldás a gazdaság számára az adatvédelmi szabályok betartására. Az önszabályozás alapját és mintáját azonban a jog biztosítja és szolgáltatja, így a hatékony önszabályozás is csak megfelelő jogi környezetben tud kialakulni, majd érvényesülni. Ennek a következtetésnek egyik gyakorlati példája a BCR is. A jogi környezethez képest olyan önként vállalt többletkötelezettségeket alapít, amelyek a jog mellett kikényszeríthető módon érvényesülnek. Úgy alakíthatók ki a szabályai, ahogyan a vállalkozáscsoport tevékenységének és struktúrájának a legmegfelelőbb, így a megfelelés színvonala és hatékonysága erősíthető meg. A fejezet konklúziója és egyben üzenete is, hogy a személyes adatok ne csak az érintettnek legyenek személyesek, fontosak és értékesek!

[392]ACQUISTI (2013) p. 16.

DOI: 10.14750/ME.2019.022

ÖSSZEGEZÉS

Az értekezés alapvető célkitűzése az, hogy bemutassa a GDPR alkalmazásával előtérbe került új adatvédelmi jogi eszközt, a BCR-t, és a jogterületi reform fényében rávilágítson annak hazai bevezetésének és alkalmazásának folyamataira, nehézségeire, előnyeire a jogalkotó és a jogalkalmazó előtt álló kihívások mentén, az egyes adatkezelők és az érintettek szintjén is. Valamennyi vizsgálati és elemzési terület kutatása során megalkotott konklúzió a fejezetek végén olvasható. Megtartva az értekezés többfunkciós jellegét, az eredményeket jelent fejezetben meg nem ismételve foglalom össze a kutatás ívét és logikai rendjét, egyúttal utalok a kiinduló kérdések és hipotézisek által határolt vizsgálati területekre is. Ezzel a szerkezeti és tartalmi tagolással célom, hogy az olvasó már az egyes fejezetek végén koherens végkövetkeztetéseket kapjon, jelen fejezettel kezdve az értekezés olvasását pedig hamar rátalálhasson az őt valóban foglalkoztató kérdésekre, sorokra.

A kutatás egyik alapvető kérdése volt, hogy a GDPR a szükséges mértékben és módon formálta-e át a jogi környezetet? A jogharmonizációs folyamat bemutatásával tetten érhető az a tendencia, hogy hazánk adatvédelmi jogi környezete példaértékűen szigorú volt európai viszonylatban, a GDPR közvetlen hatálya révén azonban ez típusú eltérés jellemzően megszűnik, noha azokon a területeken, ahol arra a GDPR felhatalmazást ad, a tagállamok alkothatnak részletező, megszorító, végrehajtási jellegű intézkedéseket. Hazánk kivételes adatvédelmi jogi környezetét is az jellemezte, hogy még a GDPR kötelező alkalmazása előtt bevezette a BCR jogintézményét 2015 októberében az Infotv. által meghatározott, a harmadik országba irányuló adattovábbításokra vonatkozó rendszerbe, megelőzve számos másik Európai Uniós tagállam jogalkotását. Megerősítést nyert az az alapvetés is, hogy a BCR a GDPR-ban kiemelt szerepet nyert. Bevezetése a gazdasági szereplőktől már a jogalkotási eljárás során is jelentős támogatást kapott. Beigazolódott, hogy a piaci igényekre szabott új jogintézmény, amely illeszkedik az

DOI: 10.14750/ME.2019.022

adatvédelmi jog reformjának tendenciájába: egy hibrid ön- illetve társszabályozási eszköz, amely a megfelelő védelmi szintet mintegy a beépített adatvédelem körében biztosítja egy vállalkozáscsoport minden tagjának, függetlenül azok letelepedésének helyétől, az érintettek állampolgárságától vagy a vállalkozáscsoport tevékenységétől. A BCR jogi elismerésének folyamata egyértelműen pozitív hozzáállást mutat a jogalkotó részéről: az Adatvédelmi Irányelvben csak rejtett, implicite megoldás, a magyar jogalkotó megelőzve a GDPR közvetlen alkalmazásának időpontját léptette hatályba a jogintézményt, a GDPR- ban pedig egyértelműen támogatott jogintézmény a megfelelő védelmi szint biztosítására. Mindezek mellett a BCR-t alkalmazók száma lassan növekszik ugyan hazánkban is, de az elvárható nagyobb volumenű, nemzetközi szinten is fellépő érdeklődés elmaradt. Ennek több oka is azonosítható, legfőbb valószínűleg jogi természetének bizonytalansága és megalkotásának költségessége.

Ismerve a BCR bevezetésének előzményeit és indokait, a fogalom egyes elemeit vizsgáltam. Már a jogintézmény magyar elnevezése vonatkozásában módosító javaslatot fogalmaztam meg. A jogbiztonságot erősítendő érdemes lett volna átvenni ugyanis az uniós terminológiákat: a vállalkozáscsoport és a kötelező erejű vállalati szabályok elnevezéseket. Megjegyzem a kötelező jelző félrevezető az uniós elnevezésben is. Javaslatom a „vállalkozáscsoporti adatvédelmi kódex” kifejezés bevezetése, mely jobb, mint az angol kifejezés tükörfordítása, indokolását pedig a BCR fogalmi elemzésére vonatkozó fejezetben adom meg. A fogalmat persze hatályon kívül kellett helyezni, amely a terminológiai problémát véglegesen feloldotta. A fogalom további elemei kapcsán nem egyértelmű az alkalmazására jogosultak köre, a felelősségi kérdések, a kötelező jelleg értelmezése a BCR mint belső szabályzat, mint egyoldalú kötelezettségvállalás szempontjából. Ezek helyes értelmezésére adok egy-egy megoldási javaslatot a BCR fogalmi elemzésére vonatkozó fejezetben, azonban a nemzeti szintű értelmezési módok helyett támogatandó volna egy uniós szintű állásfoglalás a még nyitott pontokról.

DOI: 10.14750/ME.2019.022

A BCR hatósági jóváhagyására - álláspontom szerint helyesen engedélyezésére - nincs nemzeti eljárásjogi környezet, soft law jellegű jogforrás áll a nemzeti hatóság rendelkezésére. Javaslatot teszek a vonatkozó jogi környezet megalkotásra akként, hogy annak lépéseire, a BCR-re vonatkozó különleges eljárási cselekményekre a BCR jóváhagyására vonatkozó eljárásról szóló fejezetben egy modell-eljárás menetét alkotom meg és elemzem. Ebben a fejezetben arra a konklúzióra jutottam, hogy a BCR első jóváhagyása során valamennyi Európai Uniós tagállam nemzeti hatóságát be kellene vonni, amelyre tekintettel az egyes nemzeti eljárások lefolytatása okafogyottá válna.

A BCR megalkotása nem egyszerűen szabályzatkészítés, nem csupán a vállalkozáscsoport adatkezelési gyakorlatának leírása. A BCR megalkotása egy vállalkozáscsoport üzletstratégiájának fontos eleme, amely az érintetti jogok biztosításának különféle módozatainak kialakításán túl adatbiztonsági, felelősségi, szervezeti, személyi, audit tevékenységre vonatkozó és képzési kérdéseket is magában foglal. A tartalmi elemzés körében már jóváhagyott BCR-k törzsszövegét vizsgáltam annak érdekében, hogy egy modell struktúrára felépítve mutassam be a BCR kötelező tartalmi elemeinek jelentőségét, helyét a BCR rendszerében.

A vállalkozáscsoportok számos tényezőt vesznek figyelembe akkor, amikor adatkezelési tevékenységeiket kialakítják. A SWOT analízis arra szolgál, hogy a jogtudományi szempontú vizsgálat során a BCR előnyeit, hátrányait, az alkalmazásában rejlő lehetőségeket és veszélyeket strukturáltan mutathassam be és a tényezők számszerű összesítésén túl értékeljem a tényezők tartalmi jellemzőit. Az, hogy melyik rovat hány darab jellemzőt tartalmaz, nem irányadó a BCR megítélésében. Nem mondhatjuk, hogy több a hátrány, mint az előny, tehát a BCR rossz. Azt sem mondhatjuk ki egyértelműen, hogy sok fejlesztési lehetőség kínálkozik, ezért várni kell még a BCR alkalmazásával.

DOI: 10.14750/ME.2019.022

A legtöbb szempont ugyanis esetenként, vállalkozáscsoportonként mérlegelendő.

Az értekezésben két párhuzamosan működő rendszert is bemutatok, az egyik az USA-ba irányuló adattovábbításokra vonatkozik, a másik az APEC tagállamok adatvédelmi tanúsítási rendszerét mutatja be és hasonlítja össze a BCR-rel. Az analízis eredménye, hogy a BCR tulajdonképpen egyikhez sem hasonlítható, eltérő jogi alapon nyugszik, egyediesíthető jellemzői valószínűleg a BCR javára billentik a képzeletbeli mérleg nyelvét.

A személyes adataink, nem meglepő módon, a vállalkozáscsoportoknak éppolyan értékesek, mint saját magunknak, azonban profitot jellemzően mégis a cégek szereznek belőlük. Az értekezés utolsó, kitekintő fejezetében arra a jogelméleti megközelítésre hívom fel a figyelmet, amely a személyes adatokat tulajdonjog tárgyaként, értékkel bíró javakként azonosítja azokat a gazdaságban. A meglepő, egyben elgondolkodtató állapot mindenkit érint, ezért fontos, hogy személyes adataink védelme érdekében tudatosan járjunk el, előzzük meg a jogsértést, olyan adatkezelőben bízzunk, aki elkötelezett a személyes adatok védelme mellett, akár BCR alkalmazásával is.

DOI: 10.14750/ME.2019.022

SUMMARY

The priority objective of this dissertation is to examine the BCR, the newly introduced legal instrument of the GDPR. In the dissertation the emphasis is laid on the process of the domestic implementation, the difficulties and the advantages of the application of BCR within the framework of the lately reformed legal surrounding of personal data protection. These factors are evaluated not only from the point of the legislator and the authorities but also from certain data processors and the data subjects as well.

The Hungarian law concerning personal data protection has been exemplary strict and comprehensive among the European countries. As GDPR has a direct effect this kind of difference is annulled, however in certain fields in which GDPR entitles the member states to regulate some detailed or restrictive national rules can be enacted. One of the unique features of the Hungarian data protection law is that BCR had been enacted in October 2015, long before the GDPR came into effect on 25th May 2018. With this legislative action, Hungary developed this legal field overtaking many other EU member states.

BCR as a legal instrument plays a key role in the GDPR as its implementation was supported by the economic operators from the first time of the legislation process. It has been justified, that the BCR is created according to the needs of the multinational companies and it fits well to the tendencies of the reform of the data protection law: BCR is a hybrid tool with a combination of elements of self- and co-regulation. It can provide the adequate level of protection for all members of a group of undertakings irrespective of their registered office or their activities and even the nationality of the data subjects.

DOI: 10.14750/ME.2019.022

The enactment of BCR has deemed to be accepted by the legislator as well: while it was only a potential but mostly ignored tool under the era of 95/46/EK Directive, the Hungarian legislator modified the domestic law years to enact it and the GDRP has reformed the rules on data transfers to third countries and recognizes BCR as an important and accepted way of ensuring adequate level of protection.

Knowing the reasons and the steps of introducing BCR, the dissertation contains a detailed conceptual evaluation. A proposal for its Hungarian appellation is made: the terminology of the GDPR was supported to keep or the terminus technicus of „code for data protection of the group of undertakings" should be applied. The reasons for this recommendation is stated in a certain part of the dissertation. Several parts of the concept induce arguments concerning the entitlements, the issues of liability, the interpretation of binding force having the BCR as an internal code or a unilateral commitment. In the part of the conceptual determination, I provide guidance of interpretation.

The approval process of BCR by data protection supervisory authorities is not regulated by the GDPR, nor any domestic statute, and only soft law legal sources give guidance for the requirements. In the next chapter of the dissertation, a proposal is made on the urging need for the creation of procedural rules. My proposal includes the steps and the special actions of a model process of the approval of a BCR. As a conclusion it is also stated that during the first approval of a BCR all of the data protection authorities of the member states shall take part in the process and evaluate the draft of the BCR, referring which the national approval processes can be annulled.

DOI: 10.14750/ME.2019.022

Creating a BCR is not only making another code of conduct for the company. The creation of a BCR is an essential part of the strategy of the group of undertakings including not only the mechanism for the process of personal data but also policies for data security, liability issues, structural and personnel questions, steps and requirements for trainings, audits, and monitoring activities. In that chapter of the dissertation the core texts of approved BCRs are taken into account in order to build up a model structure and emphasise the significance and the role of each element of the content.

Companies take several features into consideration when they create the structure and mechanisms for the processing of personal data they work with. The SWOT analysis aims to introduce and evaluate the strengths, the weaknesses, the opportunities and the threats deriving from the application of BCR. The number of the components of each cell do not show much rather the importance and the relevance of the factors. It cannot be stated that because more weaknesses than strength are listed BCR is unsuitable. The need for and the benefits deriving from its application shall be evaluated case by case to be able to make a deliberated decision.

Two parallel systems are also introduced in the dissertation. One is the system concerning data transfers toward the data processor in the USA, the other is the mechanism of APEC member states. These two approved certification mechanisms are compared to the BCR. The evaluation provided the conclusion that the BCR is grounded on a different legal basis but its biggest advantage derives from its uniqueness.

Our personal data constitute high value not only for us but for the data controller companies as well, although the financial profit goes only to the companies. In the last chapter of the dissertation, a brief outlook is made in order to provide arguments towards theoretical and fundamental rights issues.

DOI: 10.14750/ME.2019.022

In this part a different approach is taken into consideration thus the phenomenon of propertisation and commodification of personal data can be understood better. A thoughtful situation in which we have lived nowadays which results in the spread of the privacy paradox. This concerns everybody so that it is important for every person to be conscious in the questions of personal data protection, the prevention the infringements, even with the support of the application of BCR.

DOI: 10.14750/ME.2019.022

IRODALOMJEGYZÉK ÉS HIVATKOZÁSOK

Szakirodalmi források

ACQUISTI (2013)

Acquisti Alessando: The Economics of Privacy: *Theoretical and Empirical Aspects*, Carnegie Mellon University, September 12, 2013, http://cusp.nyu.edu/wp-content/uploads/2013/09/C03-acquisti-chapter.pdf [2015. június 7.]

ACQUISTI (2010)

Alessando Acquisti: The Economics of Personal Data and the Economics of Privacy, *Background Papaer #3*, OECD, OECDConference Centre, December 1, 2010

BAKER (2006)

Roger K. Baker: Offshore IT Outsourcing and the 8th Data Production Principle - Legal and Regulatory Requirements - with Reference to Financial Services, *International Journal of Law and Information Technology*, Vol. 14, Issue 1 (2006), p. 1-27.

BAKER (2017)

Jennifer Baker: *European Commission eyes an end to data localization in EU*, 2017.01.12. https://iapp.org/news/a/european-commission-eyes-an-end-to-data-localization-in-eu/ [2018. június 23.]

BALOGH-BÖRÖCZ-KISS-POLYÁK-SZŐKE (2017)

Balogh Zsolt György, Böröcz István, Kiss Attila, Polyák Gábor, Szőke Gergely László: Az adatvédelmi hatásvizsgálat módszertana, *Médiakutató: Médiaelméleti Folyóirat* 15: (4) pp. 77-92.

DOI: 10.14750/ME.2019.022

BALOGH – KISS – POLYÁK – SZÁDECZKY – SZŐKE (2014)
Balogh Zsolt György, Kiss Attila, Polyák Gábor, Szádeczky Tamás, Szőke Gergely László: Technológia a jog szolgálatában? – kísérletek az adatvédelem területén, *Pro Futuro 2014/1*., Debrecen, 2014. p. 33-45.

BART - JONG (2017)
Susanne Bart, Menno D.T.de Jong: The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, *Telematics and Informatics,* Vol. 34, Issue 7, November 2017, p. 1038-1058

BÁRTFAI (2018) (1)
Bártfai Zsolt: *A GDPR jogalapjairól – 1. rész*
https://jogaszvilag.hu/rovatok/szakma/a-gdpr-jogalapjairol-1-resz
[2018. június 23.]

BÁRTFAI (2018) (2)
Bártfai Zsolt: *A GDPR jogalapjairól – 2. rész*
https://jogaszvilag.hu/rovatok/szakma/a-gdpr-jogalapjairol-1-resz
[2018. június 23.]

BAUER-LEE-MAKIYAMA-VAN DER MAREL-VERSCHELDE (2016)
Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, Erik van der Marel: *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, European Centre for International Political Economy, No. 03/2016, http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf [2018. június 01.]

DOI: 10.14750/ME.2019.022

BAUER - LEE-MAKIYAMA - VAN DER MAREL – VERSCHELDE (2014)
Matthias Bauer, Hosuk Lee-Makiyama, Erik Van Der Marel, Bert Verschelde: The Costs Of Data Localisation: Friendly Fire On Economic Recovery, *Ecipe Occasional Paper*, No. 3/2014.

BENDER – PONEMON (2006)
David Bender, Larry Ponemon: Binding Corporate Rules for Cross-Border Data Transfer, *Rutgers Journal of Law and Urban Policy*, Vol. 3, Issue 2 (Spring 2006), p. 154-171.

BERMAN-MULLIGAN (1999)
Jerry BERMAN, Deirdre MULLIGAN: Privacy in the Digital Age: Work in Progress, *Nova Law Review*, Volume 23, Issue 2, 1999, p. 552-582.

BERGELSON (2003)
Vera Bergelson: It's Personal, but Is It Mine? Toward Property Rights in Personal Information, *U.C. Davis Law Review 37*, 379, 2003, p. 430.

BÓDIG – GYŐRFI – SZABÓ (2004)
Bódig Mátyás - Győrfi Tamás - Szabó Miklós (szerk.): A Hart utáni jogelmélet alapproblémái, Miskolc, Bíbor Kiadó, 2004. (ISBN: 978-963-9466-03-6)

BOROS – DARÁK (2018)
Dr. habil. Boros Anita, Dr. Darák Péter (szerk.): *Az általános közigazgatási rendtartás szabályai*, NKE, Budapest, 2018

DOI: 10.14750/ME.2019.022

BÖRÖCZ (2014)

Böröcz István: Don’t be evil - A Google adatvédelmi politikája az AdWords szolgáltatás tükrében, *Studia Iuvenum Iurisperitorum*, 2014. 7. szám, http://epa.oszk.hu/02500/02567/00007/pdf/EPA02567_Studia_Iuvenum_Iurisperitorum_7_2014_145-366.pdf [2018. május 12.]

CHANDER-LÊ (2014)

A. CHANDER, U. P. LÊ: Breaking the Web: Data Localization vs. the Global Internet, *Working Paper 2014-1, California International Law Center*, 12.03.2014, https://poseidon01.ssrn.com/delivery.php?ID=478069124110089025103017030005001092030042006012089031090113085070105027104019085087043038022017031001018002102011014064000074110010017028007093092096084124114126058030010086006005106105125031075093078086073008010065067031092098067066073125120003002&EXT=pdf [2017. november 20.]

CASTRO (2011)

Daniel Castro: *Benefits and Limitations of Industry Self-Regulation for Online Behavioural Advertising*, ITIF, 2011 p. 1-3, http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf [2018. január 5.]

COHEN (2000)

Jilue E. Cohen: Examined Lives: Informational Privacy and the Subject as Object, *52 Stanford Law Review 1373*, (2000) p. 1437–1438.

CSINK-MAYER (2012)

Csink Lóránt; Mayer Annamária: *Variációk a szabályozásra - Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban*, Médiatudományi Intézet, 2012.

DOI: 10.14750/ME.2019.022

CZÉKMANN (2015)
CZÉKMANN Zsolt: Az információs társadalom megvalósításának lépései Magyarországon, *Studia Iurisprudentiae Doctorandorum Miskolciensium-Miskolci Doktoranduszok Jogtudományi Tanulmányai* 16. tomus 2015. p. 43-66. (ISSN: 1588-7901)

DOMONKOS-POLEFKÓ (2015)
Domonkos Márton, Polefkó Patrik: Egy bírósági döntés következményei – avagy az Európai Bíróság ún. Schrems döntésének hatásai, a Safe Harbor sorsa és a felmerülő kérdések az adatvédelem területén, *Infokommunikáció és Jog,* XII. évfolyam 64. szám, 2015. december p. 123-132.

FRASER (2016)
Erica Fraser: Data Localisation and the Balkanisation of the Internet, *Scripted*, Vol. 13, Issue 3, December 2016, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/ [2017. december 5.]

GELLMANN (2016)
Robert Gellmann: Failures of Privacy Self-Regulation in the United States, In: Wright, David, De Hert, Paul (Eds.): *Enforcing Privacy, Regulatory, Legal and Technological Approaches*, Springer, 2016, p. 53-77.

HEYDER (2014) (1)
Markus Heyder: *Getting Practical and Thinking Ahead: "Interoperability" Is Gaining Momentum* https://iapp.org/news/a/getting-practical-and-thinking-ahead-interoperability-is-gaining-momentum/ [2018. április 27.]

HEYDER (2014) (2)
The APEC Cross-Border Privacy Rules—Now That We've Built It, Will They Come? https://iapp.org/news/a/the-apec-cross-border-privacy-rules-now-that-weve-built-it-will-they-come/ [2018. április 27.]

DOI: 10.14750/ME.2019.022

HORVÁTH-EGRI (2015)

Horváth-Egri Katalin: A kötelező szervezeti szabályok (Binding Corporate Rules, BCR) és az együttműködési eljárás lehetőségei, *Infokommunikáció és Jog*, XII. évfolyam 64. szám, 2015. december p. 143-146.

HUANG (1998)

P. Huang: *The Law and Economics of Consumer Privacy Versus Data Mining*, University of Pennsylvania, May 27, 1998, p. 1-35. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=94041 [2015. május 21.]

JÓRI (2003)

Dr. Jóri András: Az új magyar adatvédelmi törvény elé, *Jogtudományi Közlöny*, 2003/12. p. 393-408.

JÓRI (2009)

Jóri András: *Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése*, PhD értekezés, Pécs, 2009

JÓRI – SOÓS (2016)

Jóri András; Soós Andrea Klára: *Adatvédelmi Jog*, HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2016

KAMARINOU (2013)

Dimitra Kamarinou: International transfer of personal data and compliance under Directive 95/46/EC, the dratft Regulation and the international community, *Communications Law*, vol. 18, no. 3, 2013

KECSKÉS (2009)

Kecskés László: *EU-JOG és harmonizáció*, HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2009

DOI: 10.14750/ME.2019.022

KELSEN (1945)
Kelsen Hans: *General Theory of Law and State*, New York, Russel and Russel, 1945.

KEMENES (2017)
Kemenes István: A kontraktuális kártérítés egyes kérdései, *Magyar Jog*, 2017/1. p. 1-10.

KOLTAY (2007)
Koltay András: A magánszféra és a sajtó – magyar, angol és európai pillanatkép, *Magyar Jog*, 54. évf. 10. sz. / 2007, p. 616-625.

KUNER (2003)
Christopher Kuner: European Data Privacy Law and Online Business, *Oxford University Press*, New York, 2003

KUNER (2015)
Christopher Kuner: Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law, *University of Cambridge Faculty of Law Research Paper No. 49/2015*, Cambridge, 2015, p. 1-18.

LAUDON (1993)
Kenneth C. Laudon: Market and Privacy, *Woring Paper Series*, STERN IS-93-21, Center for Digital Economy Research, 1993.

LESSIG (2002)
Lawrence Lessig: Privacy as Property, *69 Social Research: An International Quarterly of Social Sciences 1*, 2002, p. 247-269.

DOI: 10.14750/ME.2019.022

LIBER (2011) (1)
Liber Ádám: *New Data Protection Law in Hungary: Binding Corporate Rules and 'ad hoc' contractual arrangements omitted from the list of adequacy instruments*, 2011/09/12, http://www.dataprivacy.hu/?p=730 [2018. február 05.]

LIBER (2011) (2)
Liber Ádám: *Állásfoglalás az alkalmazandó jogról* (8/2010. sz. vélemény) http://www.dataprivacy.hu/?p=462 [2018. április 12.]

LIVINGSTON-GREENLEAF (2016)
Scott Livingston, Graham Greenleaf: Data Localisation in China and Other APEC Jurisdictions, *143 Privacy Laws & Business International Report*, 2016. p. 22-26.

MAJTÉNYI (2003)
Majtényi László: *Információs jogok*. In: Halmai Gábor – Tóth Gábor Attila (szerk.) 2003. Emberi jogok. Budapest, Osiris. p. 577-635.

MAJTÉNYI (2010)
Majtényi László: *Információs és médiajog I.*, Bíbor Kiadó, Miskolc, 2010, (ISBN:978-963-9988-17-0)

MAJTÉNYI – BAYER (2016)
Majtényi László – Bayer Judit: *Információs jog*, 2016., online könyv, http://jogikar.uni-miskolc.hu/informacios-es-mediajogi-tanszek-tansegedletek

MAKSÓ (2015)
Maksó Bianka: Kötelező szervezeti szabályozás – az Infotv. legújabb adatvédelmi eszközének bevezetéséről, *Infokommunikáció és Jog,* XII. évfolyam 64. szám, 2015. december, p. 147-154.

DOI: 10.14750/ME.2019.022

MOEREL (2011)

E. M. L. Moerel: *Binding Corporate Rules - Fixing the Regulatory Patchwork of Data Protection*, PhD értekezés, Amszterdam, (ISBN/EAN 978-90-817726-0-0), Tilburg Institute for Law, Technology, and Society (TILT), 2011. https://pure.uvt.nl/ws/files/1346784/Moerel_binding_19-09-2011.pdf [2018. 06. 23.]

MURPHY (1996)

RS Murphy: Property Rights in Personal Information: An Economic Defence of Privacy, *Georgtown Law Journal 83*, 1996, 2381, p. 2383–2384.

OROS – SZURDAY (2003)

Dr. OROS, Paulina, Dr. SZURDAY, Kinga: Európai Füzetek 35.: *Adatvédelem az Európai Unióban – Szakmai összefoglaló a magyar csatlakozási tárgyalások lezárt fejezeteiből*, A Miniszterelnöki Hivatal Kormányzati Stratégiai Elemző Központ és a Külügyminisztérium közös kiadványa, Budapest, 2003

OSZTOVITS (2012)

Osztovits András (szekr.): *EU-jog*, HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2012

PELTZ-STEELE (2015)

R. J. Peltz-Steele: The pond betwixt: differences in the US-EU data protection /Safe Harbour Negotiation, *Journal of Internetlaw*, vol. 19. no. 1., 2015 July, pp. 15-30.

PFEIFLE (2017)

Sam Pfeifle: *Is the GDPR a data localization law?* https://iapp.org/news/a/is-the-gdpr-a-data-localization-law/ [2017. november 20.]

DOI: 10.14750/ME.2019.022

POSNER (1978) (1)
A. Richard Posner: The Right of Privacy, *Georgia Law Review*, Vol. 12, No. 3 (Spring 1978), p. 393-422.

POSNER (1978) (2)
A. Richard Posner: An Economic Theory of Privacy, *AEI Journal on Govenrment and Society*, Regulation, MAY/JUNE 1978 p. 19-26.

POULLET (2007)
Yves Poullet: *Transborder Data Flows and Extraterritoriality: The European Position*, 2007.
http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/poullet_/poullet_en.pdf [2018. február 05.]

PURTOVA (2017)
Nadezhda Purtova: Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency, Tilburg Law School, *Legal Studies Research Paper Series*, No. 21/2017,
PURTOVA (2009)
Nadezhda Purtova: Property rights in personal data: Learning from the American discourse, *Computer Law & Security Review 25*, 2009, p. 507–521.

REICHMAN – SAMUELSON (1997)
J.H. Reichman, Pamela Samuelson: Intellectual property rights in data, Berkeley Law, Berkeley Law Scholarship Repository, *50 Vanderbilt Law Review*, 49 (1997) p. 51-166.

DOI: 10.14750/ME.2019.022

RIFFAT (2018)
Muzamil Riffat: *Legal Aspects of Privacy and Security: A CaseStudy of Apple versus FBI Arguments, SANS Institute InfoSec Reading Room*, https://www.sans.org/reading-room/whitepapers/legal/legal-aspects-privacy-security-case-study-apple-fbi-arguments-37037 [2018. június 23.]

RYNGAERT (2015)
Cedric Ryngaert: Symposium issue on extraterritoriality and EU data protection, *International Data Privacy Law*, Volume 5, Issue 4, 2015 november 1., p. 221–225. https://doi.org/10.1093/idpl/ipv025 [2017. december 20.]

SAJÓ (1989)
Sajó András: Gazdaság és jog kapcsolata – jogelméleti szempontból, In: *Jogtudományi Értekezések*, (Szerk.: Rácz Lajos) Akadémiai Kiadó, Budapest, 1989, 58 – 72.

SAMUELSON (1999)
Pamela Samuelson: Privacy as Intellectual Property?, Berkeley Law, Berkeley Law Scholarship Repository *52 Stanford Law Review*, 1125 (1999) p. 1125-1173

SÁRI (2006)
Sári János: *Alapjogok, Alkotmánytan II.*, Osiris Kiadó, Budapest, 2006, p. 29-31.

SCHERMER (2015)
Bart Schermer: Privacy and property: do you really own your personal data? *Interdisciplinary Study of the Law*, University of Leiden, 2015. http://leidenlawblog.nl/articles/privacy-and-property-do-you-really-own-your-personal-data [2018. május 12.]

DOI: 10.14750/ME.2019.022

SCHUBAUER (2016)

Schubauer Petra: Privacy Shield, az új biztonságos kikötő, *Jog és Állam*, 21. szám, KRE Állam- és Jogtudományi Kar, 2016, p. 133-140.

SCHWARTZ (2004)

Paul M. Schwartz: Property, Privacy, and Personal Data, Berkeley Law Berkeley Law Scholarship Repository, *117 Harvard Law Review*, 2004, p. 2055 – 2128.

SIMON (2007)

Simon Éva: Egy XIX . századi tanulmány margójára, *Információs Társadalom,* 5. évf. 2. sz. 2005., p. 32-43.

SOLOVE-HOOFNAGLE (2005)

Daniel J. Solove, Chris J. Hoofnagle: A Model Regime of Privacy Protection (Version 2.0), *GWU Legal Studies Research Paper No. 132* (05.04.2005)

SOLOVE (2001)

Solove, D. J. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, 53 (6) p. 1393-1462.

SOLOVE (2013)

Solove, Daniel, J. (2013): Introduction: Privacy Self-Management and the Consent Dilemma, *Harward Law Review*, 7. szám pp. 1880-1903. http://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma [2019. február 28.]

SVANTESSON (2012)

Dan Jerker B. Svantesson: Extraterritoriality In The Context Of Data Privacy Regulation, *Masaryk University Journal of Law and Technology*, Vol 7:1, 2012. p. 87 – 96.

DOI: 10.14750/ME.2019.022

SZABÓ (2005)

Szabó Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, *Információs társadalom*, digitális folyóirat, 2005. V. évfolyam 2. szám, p. 44-54. http://www.infonia.hu/digitalis_folyoirat/2005_2/2005_2_szabo_mate_daniel.pdf [2018. június 20.]

SZÁDECZKY (2010)

Szádeczky Tamás: Pillars of IT Security, In: Balogh, Zsolt György; Chronowski, Nóra; Hornyák, Szabolcs; Nemessányi, Zoltán; Pánovics, Attila; Peres, Zsuzsanna; Szőke, Gergely László (eds.) *Essays of Faculty of Law University of Pécs: Yearbook of 2010*. Pécs: University of Pécs Faculty of Law, 2010. 295 p. HU ISSN 2061-8824 pp. 247-268.Studia iuridica auctoritate Universitatis Pécs publicata; Vol. 147. HU ISSN 0324-5934, 2010.

SZALAI (2013)

Szalai Ákos: A szerződési jog gazdasági elemzésének közgazdaságtani és jogi alapjai, *Pázmány Law Working Papers 2013/08*, http://plwp.eu/docs/wp/2013/2013-08-Szalai.pdf [2015. augusztus 5.]

SZALMA (2015)

Szalma József: Felelősség A Szerződésszegésért, *Publicationes Universitatis Miskolcinensis Sectio Juridica et Politica*, Tomus XXXIII (2015), p. 335–353.

SZÉKELY – BALOGH – JÓRI – FÖLDES (2004)

Székely Iván, Balogh Zsolt György, Jóri András, Földes Ádám: Adatvédelem és információszabadság, *Fundamentum*, 8. évf. 4. szám, p. 44-67.

SZIGETI (2009)

Szigeti Tamás: Az információs hatalom korlátozása tengeren innen és túl, *Infokommunikációs jog,* 2009. évf. 4. szám, p. 159-165.

DOI: 10.14750/ME.2019.022

SZIKLAY (2011)
Sziklay Júlia: *Az információs jogok kialakulása, fejlődése és társadalmi hatása*, PhD értekezés, Pécs, 2011.

SZIKLAY (2010)
Sziklay Júlia: Az információs jogok, mint alkotmányos alapjogok, *Jogelméleti Szemle, 2010/1. sz.*, 2010. http://jesz.ajk.elte.hu/sziklay41.html [2018. június 5.]

SZŐKE (2015)
Szőke Gergely László: *Az európai adatvédelmi jog megújítása – Tendenciák és lehetőségek az önszabályozás területén*, HVG-ORAC Lap- és Könyvkiadó Kft, Budapest, 2015

SZŐKE – POLYÁK (2014)
Szőke Gergely László, Polyák Gábor: Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére, In: Nemeslaki András (szerk.): *E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek*, Budapest, NKE, 2014. p. 65-89.

SZŐKE (2013)
Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése, *Infokommunikáció és jog* 10. p. 107-112.

TORMA – CSÁKI – CZÉKMANN (2011)
Torma András - Csáki Gyula Balázs - Czékmann Zsolt*: E-kormányzati szolgáltatások a gazdasági*, Nemzeti Tankönyvkiadó, Budapest, 2011. (ISBN: 978-963-19-7267-2)

DOI: 10.14750/ME.2019.022

TÓTH (2004)

Tóth J. Zoltán: Richard Posner és a gazdasági jogelmélet, *Jogelméleti Szemle*, 2004/1. szám

VARIAN (1996)

Hal R. Varian: *Economic aspects of Personal Privacy*, UC Berkeley, December 6, 1996, http://people.ischool.berkeley.edu/~hal/Papers/privacy/ [2018. június 23.]

WALL (2017)

Alex Wall: GDPR matchup: *The APEC Privacy Framework and Cross-Border Privacy Rules*, https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/ [2018. április 09.]

WARREN – BRANDEIS (1980)

Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, *Harvard Law Review*, Vol. 4, No. 5 (Dec. 15, 1890), p. 193-220.

WESTIN (1967)

Alan F. Westin: Privacy and Freedom, *Social Work*, Volume 13, Issue 4, 1 October 1968, p. 114–115.

WRIGHT-DE HERT (2016)

Wright David, De Hert Paul (eds.): Enforcing Privacy: Regulatory, Legal and Technological Approaches Law, *Governance and Technology Series*, Volume 25, Springer International Publishing, Switzerland, 2016. p. 13-49.

DOI: 10.14750/ME.2019.022

Jogszabályok jegyzéke

Magyar jogszabályok

Magyarország Alaptörvénye

2011. évi CXII. törvény
az információs önrendelkezési jogról és az információszabadságról

1998. évi VI. törvény
az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről

1992. évi LXIII. törvény
a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

Európai Uniós jogi aktusok

A Bizottság (EU) 2016/1250 Végrehajtási Határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről HL L 207., 2016.8.1., 1—112. o.

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) OJ L 119, 4.5.2016, p. 1–88.

DOI: 10.14750/ME.2019.022

Az Európai Parlament és a Tanács 2010/13/EU Irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv)
OJ L 95, 15.4.2010, p. 1–24.

Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, OJ C 326, 26.10.2012, p. 47–390.

Az Európai Unió Alapjogi Chartája, OJ C 326, 26.10.2012, p. 391–407.

2010/87/EU A Bizottság határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről HL L 39., 2010.2.12., 5—18. o.

2001/497/EK A Bizottság határozata (2001. június 15.) a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről HL L 181., 2001.7.4., 19—31. o., magyar különkiadás fejezet 13 kötet 26 o. 347 – 360.

2004/915/EK A Bizottság határozata (2004. december 27.) a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről HL L 385., 2004.12.29., 74—84. o.

2000/520/EK bizottsági határozat, A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről, Hivatalos Lap L 215, 25/08/2000 0007 – 0047.

DOI: 10.14750/ME.2019.022

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 OJ L 281, 23.11.1995, p. 31–50.

Soft law jellegű jogforrások, esetjog

A NAIH hivatkozott dokumentumai

Ügyszám: NAIH/2017/ …. / Előzmény: NAIH/2016/5859/H.

Ügyszám: NAIH/2018/2069/2/K

Ügyszám: NAIH-510-6/2012/H
Tájékoztató közlemény a személyes adatok védelmére vonatkozóan alkalmazandó előírásokról, továbbá az adatkezelőket, illetve adatfeldolgozókat terhelő bejelentési kötelezettségek teljesítéséről
http://naih.hu/files/2018-05-25-GDPR-koezlemeny.pdf [2018. június 1.]

A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye az Európai Unió Bíróságának a Weltimmo-ügyben hozott ítéletéről https://www.naih.hu/files/2015-10-03-Kozlemeny---Weltimmo-itelet.pdf [2018. június 1.]

Útmutató az EU-USA adatvédelmi pajzshoz
https://www.naih.hu/files/Privacy-Shield-UTMUTATO.pdf [2018. június 1.]

NAIH: Felkészülés az Adatvédelmi Rendelet alkalmazására 12 lépésben
http://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html [2017. december 18.]

DOI: 10.14750/ME.2019.022

Tájékoztató közlemény a személyes adatok védelmére vonatkozóan alkalmazandó előírásokról, továbbá az adatkezelőket, illetve adatfeldolgozókat terhelő bejelentési kötelezettségek teljesítéséről

Állásfoglalás: http://naih.hu/files/2223-2-2013-v.pdf [2018. február 01.]

A 29. cikk szerinti Adatvédelmi Munkacsoport dokumentumai

WP74: Working Document: 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, 11639/02/EN,

WP107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", 05/EN

WP108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 05/EN

WP133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data

WP153: Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, 1271-00-00/08/EN

WP154: Working Document setting up a framework for the structure of Binding Corporate Rules, 1271-00-01/08/EN

WP155 rev.04: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, 1271-04-02/08/EN

DOI: 10.14750/ME.2019.022

WP176: FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC. 00070/2010/EN

WP179 update: Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, 176/16/EN

WP184: Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments, 00683/11/EN

WP187: Opinion 15/2011 on the definition of consent, 01197/11/EN

WP195: Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 00930/12/EN

WP195a: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities

WP204 rev.01: Explanatory Document on the Processor Binding Corporate Rules, 00658/13/EN

WP 242 rev.01.: ‘Guidelines on the right to data portability’, 5 April 2017, 16/EN

WP254: Adequacy Referential (updated) 17/EN

WP259: Guidelines on Consent under Regulation 2016/679, 17/EN

DOI: 10.14750/ME.2019.022

Hivatalos közlemények, jelentések, összefoglalók

APEC Secretariat: APEC Privacy Framework, Singapore 119616, (ISBN: 981-05-4471-5) https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) [2018. június 23.]

APEC Data Privacy Pathfinder https://apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework [2018. június 23.]

APEC Electronic Commerce Steering Group - Hang Bui: Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs - Final Report, 2017. január https://www.apec.org/Publications/2017/01/Survey-on-the-Readiness-for-Joining-Cross-Border-Privacy-Rules-System---CBPRs [2018. június 23.]

Európai Bizottság: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-)ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról, Brüsszel, 2015.11.6., COM(2015) 566 final https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52015DC0566&from=EN [2018. június 23.]

Európai Unió Állampolgári Jogi, Bel- és Igazságügyi Bizottsága: Jelentés az egyesült államokbeli NSA megfigyelési programjáról, a különféle tagállamokban megfigyelést végző szervekről és az uniós polgárok alapvető jogaira gyakorolt hatásukról, valamint a transzatlanti bel- és igazságügyi együttműködésről http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//HU [2018. június 23.]

DOI: 10.14750/ME.2019.022

Európai Bizottság: Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield Brussels, 18.10.2017 COM(2017) 611 final http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619 [2018. június 23.]

Európai Bizottság: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedet vállalatok szempontjából, COM/2013/0847 final https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013DC0847&qid=1530022648852&from=HU [2018. június 23.]

Európai Bizottság: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a bizalom helyreállítása az EU-USA adatáramlások tekintetében https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013DC0846&qid=1530022749769&from=HU [2018. június 23.]

European Commission: Commission Staff Working Paper - Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf [2017. november 20.]

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A személyes adatok Európai Unión belüli védelmének átfogó megközelítése, COM(2010) 609 végleges, Brüsszel, 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf [2018. június 23.]

DOI: 10.14750/ME.2019.022

European Commission: Summary of replies to the public consultation about the future legal framework for protecting personal data, Brussels (2010) http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf [2018. június 23.]

Commission staff working document accompanying the document report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619 [2018. június 23.]

Európai Bizottság: Informal Justice Council in Vilnius – Memo http://europa.eu/rapid/press-release_MEMO-13-710_en.htm [2017. november 20.]

European Commission: Communication on Building a European Data Economy https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy [2018. június 23.]

Európai Bizottság: Social Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union, 2011, Brüsszel, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [2018. június 23.]

Európai Bizottság: Miben fogja az uniós adatvédelmi reform megkönnyíteni a nemzetközi együttműködést? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_hu.pdf [2015. november 5.]

Európai Bizottság: *Commission proposes a comprehensive reform of the data protection rules* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm [2015. november 2.]

DOI: 10.14750/ME.2019.022

Európai Bizottság: *Milyen előnyökkel jár az uniós adatvédelmi reform az európai vállalkozások számára?* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_hu.pdf [2015. július 1.]

Az európai bizottság éves jelentése: Magyarország előrehaladásáról a tagság felé, 2002. www.eski.hu/new3/eucsat/eu/2002/2002hu.doc
[2015. november 2.]

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary OJ L 215 2000.08.25. 4-6. p.

128th Session of the Committee of Ministers, Elsinore, Denmark, 17-18 May 2018, Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e [2018. június 23.]

International Camber of Commerce: Data, https://iccwbo.org/global-issues-trends/digital-growth/data/ [2018. június 23.]

International Camber of Commerce: Trade In The Digital Economy A Primer On Global Data Flows For Policymakers Prepared by the ICC Commission on Trade and Investment Policy and the ICC Commission on the Digital Economy https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf
[2018. június 23.]

DOI: 10.14750/ME.2019.022

Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents

A megfelelő védelmi szintet biztosító országok listája: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm [2017. október 19.]

United States Department Of Justice: Overview Of The Privacy Act Of 1974, 2015 Edition https://www.justice.gov/opcl/file/793026/download [2018. június 23.]

Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, (2013/2188(INI))

Privacy Shield Framework https://www.privacyshield.gov/EU-US-Framework [2018. június 23.]

Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure https://www.state.gov/documents/organization/275257.pdf [2018. június 23.]

Privacy Shield Program - Self-Certification Information https://www.privacyshield.gov/article?id=Self-Certification-Information [2018. június 23.]

DOI: 10.14750/ME.2019.022

The White House: Statement by the President on FISA Amendments Reauthorization Act of 2017 https://www.whitehouse.gov/briefings-statements/statement-president-fisa-amendments-reauthorization-act-2017/ [2018. június 23.]

Statement of the Article 29 Working Party on the consequences of the Schrems judgment Brussels, 3 February 2016, http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf [2018. június 23.]

Statement of the Article 29 Working Party, Brussels, 16 October 2015, http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [2018. június 23.]

The Unites States Department of Justice: Privacy Act of 1974 https://www.justice.gov/opcl/privacy-act-1974 [2018. június 23.]

Yves Bot Főtanácsnok indítványa, az ismertetés napja: 2015. szeptember 23., a C-362/14. sz. ügy Maximillian Schrems kontra Data Protection Commissioner ügyben, ECLI:EU:C:2015:627 https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:62014CC0362&from=HU [2018. június 23.]

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Comments on Chapter V, Brussels, 12 December201, 6723/ 13 REV 5, 2012/0011 (COD)

DOI: 10.14750/ME.2019.022

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206723%202013%20REV%205 [2017. október 19.]

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Comments on Chapter V, Brussels, 23 April 2014, 6723/ 13 REV 6, 2012/0011 (COD) http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206723%202013%20REV%206 [2017. október 19.]

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Chapter V, Brussels, 28 April 2014, 8087/1/14 REV 1, 2012/0011 (COD) http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208087%202014%20REV%201 [2017. október 19.]

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Partial General Approach on Chapter V, Brussels, 28 May 2014, 10349/14, 2012/0011 (COD) http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT [2017. október 19.]

Gazdasági Együttműködési és Fejlesztési Szervezet: Áttekintés OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, 2003 http://www.oecd.org/sti/ieconomy/15590228.pdf [2018. június 23.]

DOI: 10.14750/ME.2019.022

Igazságügyi Minisztérium: Jogharmonizációs ügyek intézése
http://eujog.im.kormany.hu/jogharmonizacios-ugyek-intezese
[2018. június 23.]

A jogharmonizáció Magyarországon
http://www.parlament.hu/biz37/eib/link1/jogharm.htm [2018. június 23.]

Hivatkozott esetjog

C-362/14. sz. ügyben a Bíróság 2015. október 6. napján meghozott ítélete, Maximillian Schrems kontra Data Protection Commissioner; Elektronikus EBHT (Általános EBHT), ECLI:EU:C:2015:650

C-230/14. sz. Weltimmo s.r.o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság, a Kúria (Magyarország) által benyújtott előzetes döntéshozatal iránti eljárásban a Bíróság 2015. október 1-jén meghozott ítélete, Elektronikus EBHT (Általános EBHT) ECLI:EU:C:2015:639

C-131/12. sz. ügyben a Bíróság 2014. május 13. napján meghozott ítélete, Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González; Elektronikus EBHT (Általános EBHT), ECLI:EU:C:2014:317

C-293/12. és C-594/12. sz. egyesített ügyekben a Bíróság 2014. április 8. napján meghozott ítélete, Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai és Kärntner Landesregierung és társai; A High Court (Írország) és a Verfassungsgerichtshof (Ausztria) által benyújtott előzetes döntéshozatal iránti kérelmek, Elektronikus EBHT (Általános EBHT), ECLI:EU:C:2014:238

DOI: 10.14750/ME.2019.022

C-288/12. sz. ügyben a Bíróság 2014. április 8. napján meghozott ítélete, Európai Bizottság kontra Magyarország EBHT (Általános EBHT), ECLI:EU:C:2014:237

C-101/01. sz. Svédországban, Bodil Lindqvist ellen folytatott büntetőeljárás során előzetes döntéshozatali eljárásban a Bíróság 2003. november 6. napján meghozott ítélete, EBHT 2003., I- 12971. p ECLI:EU:C:2003:596

C-2/74. sz. ügyben a Bíróság 1974. június 21. napján meghozott ítélete, Jean Reyners kontra État belge. Letelepedési jog; Elektronikus EBHT (Általános EBHT), ECLI:EU:C:1974:68

A VIII. fejezetben vizsgált BCR-k online elérhetősége

http://www.evosoft.hu/kotelezo-ereju-vallalati-szabalyok-binding-corporate-rules

https://www.ericsson.com/assets/local/legal/processor-binding-corporate-rules/hungarian.pdf

https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf

http://www8.hp.com/hu/hu/binding-corporate-rules.html

A BCR-t alkalmazó vállalkozáscsoportok listája

https://naih.hu/a-bcr-t-magyarorszagon-alkalmazo-adatkezel-k.html
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en#listofcompanies

Az oldalak utolsó felkeresésének dátuma: 2019. március 10.

DOI: 10.14750/ME.2019.022

RÖVIDÍTÉSEK JEGYZÉKE

Adatvédelmi Irányelv	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
Avtv.	1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
BCR	kötelező szervezeti szabályozás, Binding Corporate Rules,
CBRP	Cross-Border Privacy Rules
GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
EAT	Európai Adatvédelmi Testület
FTC	Federal Trade Commission (USA) Szövetségi Kereskedelmi Bizottság
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
WP	A 29. cikk szerinti Adatvédelmi Munkacsoport munkadokumentumai, ajánlásai, magyarázó dokumentumai

DOI: 10.14750/ME.2019.022

A SZERZŐ A TÉMAKÖRHÖZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEI

Maksó Bianka
Binding Corporate Rules as the new concept for data protection in data tarnsfers
In: Bakhoum – Gallego – Mackenrodt – Surlytė-Namavičienė (edit): "Personal Data In Competition, Consumer Protection and Ip Law - Towards a Holistic Approach?
Max Planck Institute for Innovation and Competition
MPI Studeis on Intellectual Property and Competition Law, Volume 28, p. 501-525
Springer, 2018
ISBN: 978-3-662-57645-8

Maksó Bianka
Az APEC tagállamok adatvédelmi keretrendszeréről
Studia Iurisprudentiae Doctorandorum Miskolciensium
Miskolci Doktoranduszok Jogtudományi Tanulmányai 18.
(megjelenése folyamatban)

Maksó Bianka
A BCR szerepe az adatvédelmi jogban
interTalent Unideb 2018 Konferencia – Debreceni Egyetem
Konferencia helye, ideje: Debrecen, Magyarország, 2018.04.27.
(megjelenése folyamatban)

Maksó Bianka
BCR a munkahelyen: avagy a munkavállalók személyes adatai védelmének aktuális kérdéseiről fókuszban napjaink technológiai kihívásaival
Studia Iurisprudentiae Doctorandorum Miskolciensium
Miskolci Doktoranduszok Jogtudományi Tanulmányai 17.
p. 201-222. (2017)

Maksó Bianka
Az adatvédelmi jog reformja és a BCR szerepe
Miskolci Doktorandusz Konferencia Tanulmánykötet
Konferencia helye, ideje: Miskolc, Magyarország, 2017. október 27.
Miskolc, Bíbor Kiadó, 2017. p. 119-130. (ISBN:978 615 5536 56 4)

DOI: 10.14750/ME.2019.022

Maksó Bianka
A kötelező szervezeti szabályozás (BCR) hazai bevezetéséről
In: Miskolczi Bodnár Péter (szerk.)
XII. Jogász Doktoranduszok Országos Szakmai Találkozója. 450 p.
Konferencia helye, ideje: Budapest, Magyarország, 2017.12.06.
Budapest, Patrocinium Kiadó, 2017. p. 252-262.
(Jog és Állam; 22.)

Maksó Bianka
International data transfer with special attention to the conclusions of the invalidity of US Safe Harbour scheme
In: Kékesi Tamás (szerk.)
The Publications of the MultiScience - XXX. microCAD International Multidisciplinary Scientific Conference
Konferencia helye, ideje: Miskolc, Magyarország, 2016.04.21-2016.04.22.
Miskolc: University of Miskolc, 2016. Paper E15.

Maksó Bianka
Certain issues of international transfer of personal data with special attention to the concept of BCR
In: Haffner Tamás, Kis Kelemen Bence, Kovács Áron (szerk.)
Fiatalok EURópában Konferencia 2015: Tanulmánykötet: II.
Pécs, 2015. november 13-14. 401 p.
Pécs, Sopianae Kulturális Egyesület, 2016. p. 153-162.
(ISBN:978-615-80444-0-0)

Maksó Bianka
A hazai adatvédelmi jogi környezet mai állapotához vezető főbb jogharmonizációs lépések, különös tekintettel a külföldi adattovábbítás szabályaira
JURA 2016:(1) p. 239-244. (2016)

Maksó Bianka
Exporting the policy - International data transfer and the role of Binding Corporate Rules for ensuring adequate safeguards
Pécs Journal Of International And European Law (PJIEL) 2016:(2) p. 79-86. (2016)

Maksó Bianka
Regulation of international data transfer in the EU with special attention to the issue of legal harmonisation
In: Szabó Miklós (szerk.)
Doktoranduszok fóruma: Miskolc, 2015. november 19.: Állam- és Jogtudományi Kar Szekciókiadványa. 314 p.
Konferencia helye, ideje: Miskolc, Magyarország, 2015.11.19.
Miskolci Egyetem, 2016. (ISBN:978 963 358 106 3)

DOI: 10.14750/ME.2019.022

Maksó Bianka
Lawmaking in favour of the multinational protection of personal data: procedural rules for authorizating BCR's
In: Bodó László (szerk.)
Jogalkotás és jogalkalmazás a XXI. század Európájában II. 118 p.
Konferencia helye, ideje: Budapest, Magyarország, 2015.05.15 Budapest; Debrecen: Doktoranduszok Országos Szövetsége, 2016.
(ISBN:978-615-5586-06-4)

Maksó Bianka
Kötelező szervezeti szabályozás:
Az Infotv. legújabb adatvédelmi eszközének bevezetéséről
Infokommunikáció és Jog 64. p. 147-154. (2015)

Maksó Bianka
Analysis of a new method of Data protection
In: Róth Erika (szerk.)
Via scientiae iuris: International Conference of PhD Students in Law. 476 p.
Konferencia helye, ideje: Miskolc, Magyarország, 2015.07.02-2015.07.04.
Miskolc: Gazdász Elasztik Kft., 2015. p. 241. (ISBN:978-615-80212-1-0)

Maksó Bianka
A gazdasági szempontok és a magánélet védelme
Studia Iurisprudentiae Doctorandorum Miskolciensium - Miskolci Doktoranduszok Jogtudományi Tanulmányai 16**:** p. 305-323. (2015)

Maksó Bianka
Certain dogmatic issues about the Application of Information Rights as Fundamental Rights
In: Szabó Miklós (szerk.)
Doktoranduszok Fóruma: Állam- és Jogtudományi Kar Szekciókiadványa.
Konferencia helye, ideje: Miskolc, Magyarország, 2014.11.20 Miskolc: Miskolci Egyetem, 2015. p. 185-190. (ISBN:978-963-358-087-5)

Maksó Bianka
A kötelező erejű vállalati szabályok:
Az adatvédelmi önszabályozás új lehetősége
In: Koncz István, Szova Ilona (szerk.)
A Tudomány szolgálatában 2. köt: PEME IX. Ph.D. Konferencia.
Konferencia helye, ideje: Budapest, Magyarország, 2014.10.29 Budapest, Professzorok az Európai Magyarországért Egyesület, 2014. p. 159-170.
2. kötet. (ISBN:978-963-89915-4-6)

DOI: 10.14750/ME.2019.022

SZERZŐSÉGI NYILATKOZAT

Alulírott dr. Maksó Bianka ezennel kijelentem, hogy a doktori fokozat megszerzése céljából benyújtott értekezésem kizárólag saját, önálló munkám. A benne található, másoktól származó, nyilvánosságra hozott vagy közzé nem tett gondolatok és adatok eredeti lelőhelyét a hivatkozásokban (lábjegyzetekben), az irodalomjegyzékben, illetve a felhasznált források között hiánytalanul feltüntettem.

Kijelentem továbbá azt is, hogy a benyújtott értekezéssel azonos tartalmú értekezést más egyetemen nem nyújtottam be tudományos fokozat megszerzése céljából.

E kijelentésemet büntetőjogi felelősségem tudatában tettem.

Miskolc, 2019. március 10.

dr. Maksó Bianka

DOI: 10.14750/ME.2019.022