DOI: 10.38146/BSZ.2017.2.7

SCHUBAUER PETRA

A Safe Harbor határozat érvénytelenítésének hatása az európai adatvédelmi gyakorlatra

2015. október 6-án az Európai Unió Bírósága kimondta a bizottság Safe Harbor határozatának érvénytelenségét, alapjaiban bolygatva meg az Európai Unióban alkalmazott adattovábbítási gyakorlatot.

Az információs társadalmak korában nem újdonság, hogy az információáramlás (és így az adattovábbítás) adja a gazdasági-társadalmi fejlődés alapját, amelynek útjába nem célszerű akadályokat gördíteni.[1]

Az Európai Unió Bizottsága is több alkalommal kifejtette, hogy a személyes adatok továbbítása szerves, egyre nagyobb részét teszi ki a transzatlanti kereskedelmi kapcsolatoknak[2], amelyekbe beletartoznak az egyre növekvő számú digitális vállalkozások, mint például a közösségi média vagy a számítástechnikai felhők.[3]

A külföldre történő adattovábbítás a globalizáció korában megkérdőjelezhetetlenül hasznos gazdaságilag, ezzel összefüggésben azonban egyre gyakrabban jelennek meg olyan helyzetek, amelyekben az érintett adatalany magánszférája veszélybe kerülhet.[4] Az információs önrendelkezési jog jogosultjának szavatolni kell azon jogát, hogy eldönthesse, a hozzá kapcsolódó személyes adatoknak mi legyen a sorsuk.[5] A külföldre történő adattovábbítás ebből a szempontból különösen veszélyes lehet, mivel a személyes adatok határokon átnyúló gyors és észrevétlen továbbításának semmilyen technikai vagy financiális akadálya nincs, és így az adatalany elveszítheti a kontroll lehetőségét, ha személyes adatait egy olyan országba továbbítják,

1 Péterfalvi Attila (szerk.): Adatvédelem és információszabadság a mindennapokban. HVG-ORAC, Budapest, 2012, 119. o.

2 Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America following the Judgement by the Court of Justice in Case C-362/14 (Schrems). http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-usdataflowscommunicationfinal.pdf

3 A főtanácsnok indítványa a C-362/14. sz. ügyben. Maximillian Schrems kontra Data Protection Commissioner. 106/15. sz. sajtóközlemény. Európai Unió Bírósága, Luxemburg, 2015. szeptember 23. curia.europa.eu/jcms/jcms/P174300/fr/

4 Liber Ádám: Személyes adatok nemzetközi továbbítása. Az új adatvédelmi törvény margójára. Infokommunikáció és Jog, 2011/5., 179. o.

5 A főtanácsnok indítványa… i. m.

amely jogrendje nem vagy nem megfelelően nyújt védelmet a személyes adatok számára.[6] Az információs önrendelkezési jog garantálása és az adatok belső piacon történő szabad áramlása közötti konszenzust az unió adatvédelmi irányelve teremtette meg 1998-ban.

A jelenleg hatályos adatvédelmi szabályozás szerint az Európai Gazdasági Térség tagállamain belül történő adattovábbítást belföldi adattovábbításnak kell tekinteni.

Az irányelv az EGT-tagállamokon kívüli, harmadik országok tekintetében két csoportot állít fel: az adatvédelmi szempontból megfelelő védelmet nyújtó, és az adatvédelmi szempontból megfelelő védelmet nem nyújtó országokat. Utóbbiakba az adattovábbítás fő szabály szerint tilos, csak az irányelv által meghatározott kivételes esetekben lehetséges.

A biztonságos országok tekintetében a megfelelő szintű védelemről az úgynevezett megfelelőségi teszt *(Essentially Equivalent Test)* segítségével lehet megbizonyosodni, amely során konkrétan meg kell vizsgálni a továbbítandó adatok jellegét, az adatkezelés célját, időtartamát, az alkalmazandó jogi szabályozást, az adatkezelés átláthatóságát, az adatalany jogait, az adott országban érvényesülő szakmai szabályokat és biztonsági intézkedéseket.[7] E szempontokat figyelembe véve a célországnak gondoskodnia kell az adatvédelmi anyagi szabályok meglétéről, valamint az anyagi szabályok érvényesítéséhez szükséges eljárásjogi eszközökről. Anyagi jogi követelménynek tekinthető egyebek között a célhoz kötöttségnek és a szükségességi–arányossági követelményeknek való megfelelés, az adatkezelés átláthatósága, az adatalanyok jogainak szavatolása, az adattovábbítás korlátozása, valamint a szenzitív személyes adatok esetén többletgaranciák nyújtása. Eljárásjogi követelménynek minősül a független hatósági felügyelet, a hatékony jogérvényesítés lehetőségének és a megfelelő jogorvoslatnak a megteremtése.[8]

A megfelelőségi teszt elvégzése után a végső döntést a bizottság mondja ki határozatában, az adatvédelmi irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (az EU-tagállamok adatvédelmi hatóságaiból álló, úgynevezett 29-es Adatvédelmi Munkacsoport, a továbbiakban: munkacsoport) meghallgatása után. Biztonságos országnak számít jelenleg Andorra, Argentína, Svájc, Guernsey, Man-sziget, Jersey, a Feröer-szigetek, Izrael, Ausztrália és Kanada. Az Egyesült Államok esetében a bizottság két esetben döntött úgy, hogy Amerika garantálja a megfelelő adatvédelmi szintet: az Egyesült Álla-

6 Péterfalvi Attila (szerk.): i. m. 119. o.
7 Uo. 121. o.
8 Liber Ádám: i. m. 180. o.

mok Vámügyi és Határvédelmi Irodájának történő utasnyilvántartási adatok, valamint az úgynevezett Safe Harbor („biztonságos kikötő") listán szereplő vállalatok részére történő személyes adatok továbbítása esetén.[9]

Az Egyesült Államok kereskedelmi minisztériuma 2000. július 21-én az A5-0177/2000.[10] számú állásfoglalása keretében adta ki a Safe Harbor adatvédelmi elveket, amelyek alapján az Európai Unióból az Egyesült Államokba történő adattovábbítás biztonságosnak tekintendő, amennyiben az Amerikában letelepedett vállalkozások az elveknek megfelelő tevékenységet végeznek. A Safe Harbor önszabályozáson alapul, mivel az adatokat fogadó vállalkozásoknak önkéntes alapon egyértelműen és nyilvánosan ki kell jelenteniük az elvek teljesítésére vonatkozó kötelezettségvállalást, erről bejelentés után a kereskedelmi minisztérium bárki számára elérhető nyilvántartást[11] vezet. A Safe Harbor gyakorlati jelentőségét mutatta, hogy a legnagyobb amerikai adatkezelők – így a Facebook, a Yahoo, az eBay, az Amazon és a Google is – a Safe Harbor adatvédelmi elveknek való megfelelőséggel teremtettek jogalapot az adatkezeléseikhez.[12]

2000. július 26-tól 2015. október 6-ig biztonságosnak tekintették az adattovábbítást a Safe Harbor elvek alapján, ezt a nagyjából tizenöt éves gyakorlatot azonban az Európai Unió Bíróságának a *Maximillian Schrems kontra Data Protection Commissioner-ügy*ben hozott határozata megszüntette.

A Maximillian Schrems kontra Data Protection Commissioner-ügy

A döntés alapját a C-362/14. számú ügy adta, amelyben *Maximillian Schrems* a Facebook Ireland Ltd. (a továbbiakban: ír Facebook) ellen 2013. június 25-én panaszt nyújtott be az adatvédelmi biztoshoz *(Data Protection Comissioner)* a Facebook által a felhasználók személyes adatainak az Egyesült Államokban található szervereken történő tárolása miatt. Schrems azzal érvelt, hogy az Egyesült Államok joga és gyakorlata nem garantál az uniós állampolgárok adatai számára megfelelő védelmet az állami felügyelettel szemben, ezt az állítását a Snowden-ügy során kiderült információkkal támasztotta alá.

9 Péterfalvi Attila (szerk.): i. m. 121. o.
10 Jóri András: Adatvédelmi kézikönyv. Osiris Kiadó, Budapest, 2005
11 https://safeharbor.export.gov/list.aspx
12 Liber Ádám: i. m. 181. o.

2013 júniusában *Edward Snowden* felfedte, hogy az amerikai Nemzetbiztonsági Ügynökség *(National Security Agency; NSA)* és további amerikai nemzetbiztonsági szolgálatok a Prism nevű program[13] alkalmazásával tömeges, szabad hozzáférést kaptak az Egyesült Államok szerverein tárolt adatokhoz. Ezeket a szervereket számos, az internet és technológia területén tevékenykedő, a Facebookhoz hasonló vállalkozás birtokolta vagy felügyelte[14], így a szervereken egyebek között az uniós Facebook-felhasználók személyes adatai is megtalálhatók voltak. Bár a Safe Harbor határozat I. mellékletének 4. bekezdése alapján nemzetbiztonsági megfontolások alapján lehetőség van eltérni az elvektől, a Snowden-ügy kapcsán Schrems érvei szerint a Prism hírszerző program megkérdőjelezi a bizottság döntésének érvényességét, amely szerint az Egyesült Államokban a Safe Harbor programban részt vevő vállalkozások esetében garantált a megfelelő adatvédelem[15], mivel a személyes adatok Amerikába való továbbítása után azokhoz az adatok tömeges és válogatás nélküli megfigyelése és lehallgatása útján az NSA és más szövetségi ügynökségek hozzáférhetnek, mindez jelentős túlkapás, és így túlterjeszkedik az I. számú melléklet 4. bekezdése által megengedett határokon.

Az adatvédelmi biztos úgy ítélte meg, hogy a panaszt nem köteles kivizsgálni, mivel az jogilag megalapozatlan. Véleménye szerint nem volt bizonyíték arra, hogy az NSA hozzáférhetett Schrems adataihoz, valamint a bizottság a 2000/520/EK irányelvben kijelentette, hogy a Safe Harbor rendszer megfelelő védelmi szintet nyújt a személyes adatok számára, amelyet adatvédelmi hatóságként az adatvédelmi biztos nem kérdőjelezhet meg, így a panaszt el kell utasítani. Schrems a panaszt elutasító határozat ellen keresetet nyújtott be az ír legfelsőbb bírósághoz.

A ír legfelsőbb bíróság arra a megállapításra jutott, hogy Schrems panasza nem az ír Facebook magatartására, hanem magára a Safe Harbor rendszerre és az Egyesült Államok adatvédelmi jogára és gyakorlatára irányult. Ezek alapján a panasz az uniós jogot közvetlenül érinti, így az ír legfelsőbb bíróság előzetes döntéshozatali eljárásban fordult a bírósághoz azt tudakolva, hogy a nemzeti felügyeleti hatóságok és a bizottság milyen eljárást kövessenek, amikor a Safe Harbor alkalmazása során visszásságokkal találkoznak. Szükséges volt pontosítani a nemzeti felügyeleti hatóságok hatáskörét azokban az esetekben, amikor személyes adatok harmadik országbeli székhelyű

13 http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

14 A főtanácsnok indítványa… i. m.

15 Sam Pfeifle: Safe Harbor "Invalid". Rules ECJ, 2015. https://iapp.org/news/a/first-reactions-to-the-ecj-decision

vállalkozások részére történő továbbítására vonatkozó panaszt kell elbírálniuk, és az e panaszban szereplő állítás szerint a harmadik ország nem garantálja az adatok megfelelő védelmét, noha a bizottság határozatában (jelen esetben a 2000/520/EK határozatban) kimondta, hogy az ország megfelelő szintű védelmet nyújt.

Az előzetes döntéshozatali eljárás során *Yves Bot* főtanácsnok kifogásolta, hogy az uniós Facebook-felhasználókat nem tájékoztatják a regisztráció folyamán arról, hogy a személyes adataikat egy olyan harmadik országba továbbítják, amelyben az adatok az ottani szabályozásnak megfelelően elérhetők lesznek a nemzetbiztonsági ügynökségek számára. Amerika joga és gyakorlata széles körben lehetővé teszi az uniós polgárok személyes adatainak gyűjtését és általános jellegű lehallgatását anélkül, hogy az érintettek hatékony jogi védelmet élveznének, vagyis a Prism nevű program aránytalan és szükségtelen mértékben fér hozzá az uniós polgárok adataihoz: nemcsak azokéihoz, akik veszélyt jelentenek a nemzetbiztonságra, hanem mindenkiéhez, aki a Facebook elektronikus hírközlési szolgáltatását igénybe veszi. Megállapították, hogy az uniós polgároknak nincs tényleges meghallgatási joguk, nincs lehetőségük betekinteni az adatokba, azok helyesbítését, törlését kérni vagy jogorvoslattal élni, valamint nincs megfelelő független felügyeleti szerv, hatóság, amely az adatkezelés jogellenességét vizsgálhatná.

Az említett indokok alapján a főtanácsnok arra az álláspontra jutott, hogy a Safe Harbor határozat nem tartalmaz elegendő garanciát. Véleménye szerint a bizottság által hozott határozat léte nem akadályozhatja meg a nemzeti felügyeleti hatóságokat abban, hogy kivizsgálják azt a panaszt, amely szerint valamely harmadik ország nem kínál megfelelő védelmi szintet a továbbított személyes adatok számára.[16]

A főtanácsnok indítványával összhangban a bíróság meghozta a döntést, miszerint a Safe Harbor elvekről szóló 2000/520/EK határozatot érvénytelennek kell nyilvánítani, mivel az alapvető jogoknak az előbbiekben leírt megsértése miatt nem fogadható el, hogy az e határozat által létrehozott biztonságos kikötő rendszere megfelelő védelmi szintet nyújt az EU-ból az Egyesült Államokba továbbított személyes adatok számára.[17]

16 A főtanácsnok indítványa… i. m.

17 Az Európai Unió Bíróságának döntése a C-362/14. számú ügyben. 2015. http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en

A kialakult helyzet és a külföldi adattovábbításra vonatkozó hatályos szabályozás

A *Maximillian Schrems kontra Data Protection Commissioner-ügy*ben a bíróság egyértelműen elmagyarázta az uniós adatvédelmi hatóságok és a bizottság viszonyát: a hatóságokat köti a bizottság döntése addig, amíg azt a bíróság érvénytelennek nem találja, vissza nem vonja, vagy hatályon kívül nem helyezi[18], így ha a hatóság a bizottság döntésével ellentétes álláspontra jut, először a bírósághoz kell fordulnia. A hatóságoknak fontos szerepük van abban, hogy teljes függetlenséggel, az EU jogszabályainak megfelelően figyelemmel kísérjék az adatkezeléseket, adattovábbításokat, adatfeldolgozásokat az egyének védelme érdekében[19], és így jogosultak – és kötelesek – önállóan[20] vizsgálni a harmadik ország által garantált adatvédelmi szintet a kötelező erejű bizottsági döntéstől függetlenül is.

A kialakult helyzet nyomán az Európai Bizottság 2015. november 6-án közleményében iránymutatást nyújtott a tagállami adatvédelmi hatóságoknak abban a kérdésben, hogyan járjanak el az Amerikába történő adattovábbításokkal kapcsolatos ügyekben. Ezen felül tájékoztatót adott ki a transzatlanti adattovábbítások jogi alapját megteremtő alternatív megoldásokhoz a piaci szereplők számára, valamint szükségszerűen megkezdődött a Safe Harbor program újratárgyalása az Egyesült Államokkal.[21] A tárgyalások eredményeképp létrejött az úgynevezett Privacy Shield („adatvédelmi pajzs") rendszer, amelyet a bizottság 2016. augusztus 1-jén közzétett 2016/1250. számú határozatában. A 29-es Munkacsoport 2015. október 6-i közleményében hangsúlyozta, elengedhetetlen, hogy a tagállami hatóságok erős, kollektív és egységes módon implementálják a bírósági döntést. A munkacsoport sürgette a tárgyalások és az együttműködés megkezdését Amerika és a tagállamok, valamint az EU intézményei között, hogy olyan jogi és technikai megoldásokat találjanak, amelyek lehetővé teszik az adattovábbítást az alapvető adatvédelmi jogok tiszteletben tartása mellett.[22] Akár egy új Safe Harbor keretében – az új szabályozásnak az átláthatóságot, arányosságot, jogorvoslati eljárásokat és adatvédelmi jogokat kell tartalmaznia, amelyek meghatározott eljárá-

18 Communication from the Commission… i. m.

19 Denis Kelleher: The Role of the DPA. 2015. https://iapp.org/news/a/after-safe-harbor-the-role-of-the-dpa/

20 Communication from the Commission… i. m.

21 Denis Kelleher: i. m.

22 Statement of the Article 29 Working Party. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29pressmaterial/2015/20151016wp29statementonschremsjudgement.pdf

sok keretében érvényesíthetők és adatvédelmi hatóságok által ellenőrizhetők. Remélhetőleg ezeknek a követelményeknek a Privacy Shield a jövőbeni gyakorlati alkalmazása során meg tud felelni, és nem kerül sor még egy bírósági eljárásra, amelyben bebizonyosodhat a rendszer gyengesége.

Milyen lehetőségek maradtak az Egyesült Államokba történő adattovábbításra?

Azok az adattovábbítások, amelyek a Safe Harbor programra hivatkozva történnek, a bíróság ítélete szerint jogellenesek. Ennek megfelelően azok az adatkezelők, amelyek kizárólag a Safe Harbor-döntésre hagyatkoztak, és nincs más jogi megoldásuk az adatkezelés jogalapjára, mindenfajta szabályozás nélkül maradtak.[23]

Az adatvédelmi irányelv 26. cikk (2) bekezdése alapján adatvédelmi szempontból nem biztonságos országokba kivételesen továbbíthatók személyes adatok szerződéses alapon is, ha az adatkezelő megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében.[24] Ilyen esetben alkalmazni lehet a bizottság által kidolgozott általános szerződési feltételeket *(Standard Contractual Clauses* vagy *model clauses),* amelyek megfelelő védelmet nyújtanak az adattovábbítások esetére. Az uniós tagállamok az általános szerződési feltételek által nyújtott biztosítékokat kötelesek elfogadni, ugyanakkor a tagállami felügyeleti hatóságok felügyelhetik azok betartását, így ha a felek bármelyike megsérti a megállapodást, a hatóság megtilthatja vagy felfüggesztheti az adattovábbítást. Ezek a szerződések egyedi esetekben megfelelő eszközök lehetnek, de nem nyújthatnak megnyugtató megoldást multinacionális vállalatok szervezeten belüli adatáramoltatására.[25] A bizottság ez idáig négyféle általános szerződésifeltétel-csomagot bocsátott ki: az adatkezelők közötti megállapodás két változatát, valamint az adatkezelő és adatfeldolgozó közötti megállapodás két változatát. Ezek a mintaszerződések tartalmazzák a felek jogait és kötelezettségeit, ezek pontos leírása szükséges, mivel nem lehet előre megállapítani, hogy az az ország, ahová a személyes

23 Kirsten Thompson – Daniel G. C. Glover – Barry Sookman – Keith Rose: Life after Schrems: Think Locally, Act Globally? http://www.canadiancybersecuritylaw.com/2015/10/life-after-schrems-think-locally-act-globally/?utmsource=Mondaq&utmmedium=syndication&utmcampaign=View-Original

24 95/46/EK irányelv

25 Péterfalvi Attila (szerk.): i. m. 122. o.

adatokat továbbítják, megteremti-e az adatok számára a megfelelő szintű védelmet.[26]

Lehetőség van *ad hoc* adatvédelmi megállapodásokra is, ezeket azonban egyenként kell a tagállami adatvédelmi hatóságokkal jóváhagyatni, valamint az engedélyezést be kell jelenteni az Európai Bizottságnál.

A kötelező erejű vállalati szabályozás *(Binding Corporate Rules; BCR)* a vállalaton belüli önszabályozás eszköze, amelynek célja, hogy a különböző államokban található, de egy vállalatcsoportba tartozó vállalatok között a személyes adatok szabadon mozoghassanak. Az ilyen egyoldalú kötelezettségvállalások tartalmára nézve a 29-es Munkacsoport ajánlásokat dolgozott ki, lefektetve az anyagi jogi és eljárásjogi követelményeket.[27] A kötelező erejű vállalati szabályozást végső soron az érintett nemzeti adatvédelmi hatóságok hagyják jóvá az adatvédelmi törvényekben lefektetett eljárások keretében.

A kötelező erejű szervezeti szabályozások 2015. október 1. napjáig Magyarországon nem minősültek elfogadott jogalapnak az adattovábbítások terén, azonban az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (Infotv.) 2015. október 1. napjával történő módosításával bekerült a szabályozásba ez a jogi lehetőség is. 2013. november 8-án *Péterfalvi Attila,* a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) elnöke állásfoglalásában úgy tájékoztatott, hogy a kötelező erejű szervezeti szabályozáson alapuló adattovábbítás nem megengedhető.[28] (Érdekes, hogy az Infotv. hatálybalépését megelőző adatvédelmi törvény tartalmazta, azonban az új szabályozás negligálta a kötelező erejű vállalati szabályok alkalmazásának lehetőségét. Sokan ezt visszalépésnek tekintették a korábbi szabályozáshoz képest.)

Az adatvédelmi irányelvben találhatók meghatározott kivételek, amelyek fennállása esetén lehetőség van személyes adatot olyan harmadik országba továbbítani, amely nem gondoskodik az adatok megfelelő szintű védelméről. Ilyen egyebek között az az eset, amikor az adatalany kifejezett, önkéntes hozzájárulását adta az adattovábbításhoz; az adattovábbítás szerződés teljesítéséhez szükséges; az adattovábbítás fontos közérdekből szükséges; a továbbítás jogok bíróság előtti megállapítása, gyakorlása vagy védelme miatt szükséges; a továbbítás az érintett létfontosságú érdekeinek védelme miatt szükséges;

26 Communication from the Commission… i. m.

27 Working Document setting up a table with the elements and principles to be foundin Binding Corporate Rules. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp153en.pdf

28 NAIH-állásfoglalás, 2013. http://www.naih.hu/files/2223-2-2013-v.pdf

vagy ha a továbbítást olyan nyilvántartásból végzik, amely a nyilvánosság tájékoztatását szolgálja.[29] A munkacsoport korábbi közleményeiben hangsúlyozta, hogy ezeket a kivételeket nem lehet kiterjesztően értelmezni.

A 29-es Adatvédelmi Munkacsoport állásfoglalása szerint az általános szerződési feltételek és a kötelező erejű vállalati szabályozás a továbbiakban is alkalmazható alternatív megoldásként, amíg meg nem születik egy új megállapodás a Safe Harborról. Végezetül az Amerikai Egyesült Államok és az Európai Unió Bizottságának megállapodása eredményeképp létrejött a Privacy Shield rendszer, amely a korábbi Safe Harbor helyébe lépve annak funkcióját remélhetőleg a jövőben is teljes mértékben el tudja látni.

A hatályos magyar szabályozás szerint harmadik országba adatot továbbítani két esetben lehet: egyrészt az érintett kifejezett hozzájárulása alapján, másrészt akár az érintett hozzájárulásának hiányában is, ha az adattovábbításnak van az Infotv. által elismert jogalapja, valamint a célországban az adatok megfelelő szintű védelme biztosított. Az adatok megfelelő szintű védelmét biztosítottnak kell tekinteni, ha azt az Európai Unió kötelező jogi aktusa megállapítja, vagy nemzetközi szerződés van hatályban, illetve ha az adattovábbítás címzettje kötelező szervezeti szabályozásnak megfelelően kezeli a személyes adatokat.[30]

Láthatjuk, hogy a Safe Harbor határozat érvénytelenné nyilvánítása nagymértékben felkavarta a kialakult adatvédelmi gyakorlatot. Bár maradtak eszközök az adattovábbításokra, mégis igény volt egy új Safe Harbor határozat létrehozatalára. Max Schrems, az alapügy felperese szerint rendkívül nehéz lesz olyan megoldással előállni, amely a bíróság által azonosított valamennyi problémára válasz. Az Egyesült Államok kormánya nem valószínű, hogy korlátozni kívánná a titkos információszerzésre vonatkozó jogi szabályozását annak érdekében, hogy az uniós alapjogi chartával összhangba kerüljön. A két fél csak olyan korlátozott adatvédelmi garanciákat tartalmazó megállapodásra juthatna, amely még nagyon messze van attól, hogy a bíróság által megfogalmazott követelményeknek megfeleljen. A következő Safe Harbor programnak tulajdonképpen a 95/46/EK irányelv szó szerinti átvételének kellene lennie, hogy kiállja a bíróság próbáját. Max Schrems meglátása szerint egy „gyors javítás" bizonyosan nem vezet olyan Safe Harbor programhoz, amely szavatolja az adatvédelem megfelelő szintjét.[31] Bár kialakult gyakorla-

29 Liber Ádám: i. m. 182. o.

30 NAIH-állásfoglalás… i. m.

31 Max Schrems: Will We See a "Safe Harbor 2.0." Soon? https://iapp.org/news/a/will-we-see-a-safe-harbor-2-0-soon/

ta nincs még a Privacy Shield rendszernek, az adatvédelemmel foglalkozó jogászok nagy elvárásokkal tekintenek az újításra, amely remélhetőleg megállja a helyét, és akár a bíróság próbáját is kiállja.

Nemzetközi kitekintés

A bíróság érvénytelenséget kimondó döntése óta az uniós adatvédelmi hatóságok nemzeti szinten információs kampányokkal kezelik a kialakult helyzetet: egyrészt közvetlen információt nyújtanak az olyan vállalkozások, piaci szereplők számára, amelyek a Safe Harbort alkalmazták, valamint általános jellegű tájékoztatót tesznek közzé honlapjaikon.[32]

A különböző országok adatvédelmi szervei különböző válaszokat adtak a kialakult helyzetre.

David Smith brit adatvédelmi biztos nyilatkozatában hangsúlyozta, hogy a Safe Harbor érvénytelenítése nem jelenti azt, hogy Nagy-Britannia állampolgárainak adataira egyre növekvő veszélyek leselkednének, valamint az újraszabályozás szükségessége sem újdonság. A brit hatóság tudomásul veszi, hogy jó időbe telhet, mire a Safe Harbort alkalmazó vállalatok felülvizsgálják szerződéseiket, valamint hogy a hatályos jogszabályokkal összhangban lévő, megfelelő adatvédelmi szintű megoldás megtalálásában a hatóság a honlapján közzétett információkkal kíván segítséget nyújtani.[33]

Németország speciális helyzetben van a többi EU-tagállamhoz képest, mivel az adatvédelmi felügyeleti feladatokat nem egyetlen hatóság látja el, hanem tizenhét független adatvédelmi hatóság. A szabályozást tekintve érdekesség, hogy a vállalkozásoknak nincs általános bejelentési kötelezettségük, ha adatokat továbbítanak harmadik országokba (beleértve az Egyesült Államokat is). Közleményében a német *Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder* (Adatvédelmi Hatóságok Adatvédelmi Konferenciája) tájékoztatott, hogy ha a német hatóságok a Safe Harboron alapuló adattovábbítással találkoznak, meg fogják tiltani, és a tilalmat megszegőkkel szemben súlyos pénzbírságot helyeznek kilátásba. A vállalkozásokat felszólítják, hogy haladéktalanul vizsgálják felül az adattováb-

32 Press release of the Article 29 Working Party. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29pressmaterial/2015/20151006wp29pressreleaseonsafeharbor.pdf

33 ICO response to ECJ ruling on personal data to US Safe Harbor. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/

bításra vonatkozó eljárásaikat, hogy a német szabályozásnak megfelelő legyen, valamint a törvényhozó figyelmét felhívják, hogy az ilyen esetekben szükséges pontosan meghatározni az adatvédelmi hatóságok kereseti jogát.[34]

A német adatvédelmi hatóságok többségének jelen álláspontja szerint a BCR és az általános szerződési feltételek alkalmazása mint megoldás szintén megkérdőjelezhető. A német hatóságok pillanatnyilag nem engedélyeznek adattovábbításokat az Egyesült Államokba a BCR vagy az adattovábbítási szerződések alapján. Szigorú kereteken belül az egyetlen jogalapként az érintett beleegyezése fogadható el, azonban a beleegyezésen alapuló adattovábbítás nem lehet ismétlődő, rutinszerű vagy tömegesen előforduló (Schleswig-Holstein adatvédelmi biztosának különvéleménye szerint az érintett beleegyezése sem teremt elegendő jogalapot).

Belgiumban, Hollandiában és Luxemburgban az adatvédelmi hatóság alapvetően osztja a 29-es Munkacsoport állásfoglalását. A BCR és az általános szerződési feltételek alkalmazható ezekben az országokban alternatív megoldásként, azzal a megkötéssel, hogy Luxemburgban az adatvédelmi hatóság előzetes hozzájárulása kell az adattovábbításhoz, még akkor is, ha a vállalkozások a bizottság által elfogadott szerződési feltételek szó szerinti átvételét alkalmazzák.

Svájcban elsődleges megoldásként a Safe Harboron alapuló adattovábbítás helyett a vállalkozások adattovábbítási megállapodásokat kötelesek kötni, amelyekben az adatkezelőknek garantálniuk kell, hogy a megfelelő jogok gyakorlása érdekében az adatalanyokat érthetően tájékoztatták arról: lehetséges, hogy az Egyesült Államok hatóságai hozzáférnek a személyes adataikhoz.

Kelet-Közép-Európa államai közül Bulgáriában, Csehországban, Lengyelországban, Romániában és Szlovákiában nagyjából azonos a helyzet: alternatív megoldásként alkalmazható a kötelező erejű vállalati szabályozás és az általános szerződési feltételek, illetve az érintettek hozzájárulása vagy az adatvédelmi hatóság engedélye a törvényekben meghatározott esetekben.[35]

A Nemzeti Adatvédelmi és Információszabadság Hatóság 2015. október 6-án közzétett közleménye szerint a hatóság üdvözli az Európai Unió Bíróságának döntését, amelynek folyományaképp alapjaiban kell újraszabályozni az Egyesült Államokba irányuló adattovábbításokat. A közlemény utal rá,

34 Positionspapier der Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder. https://www.datenschutz.hessen.de/ft-europa.htm#entry4521

35 Eva Casselino Herrera – Tom De Cortier – Carsten Domke – Márton, Domokos – Caroline Froger-Michon – Christopher Jordan – Loretta Pugh – Christian Runte – Anne-LaureVilledieu: The ECJ's Safe Harbour Decision: Consequences and Practical Guidance for HR. Conference call, Dec. 14, 2015.

hogy a bíróság ítéletében kiemeli, a tagállami adatvédelmi hatóságoknak minden esetben biztosítani kell azon jogát, hogy a külföldre irányuló adattovábbítások esetén vizsgálják, a célország biztosítja-e a megfelelő adatvédelmi szintet. A tagállami hatóságok, így a NAIH is jogosult arra, hogy teljes függetlenséggel vizsgálja a harmadik országokba irányuló adattovábbítások kapcsán az adatvédelmi garanciák meglétét. A NAIH a bírósági ítélet miatt kialakult helyzetben az Európai Unió többi adatvédelmi hatóságával egységes vélemény kidolgozásán munkálkodik.[36] 2015. októberi közleménye óta a magyar adatvédelmi hatóság a kérdésben további nyilatkozatot vagy iránymutatást nem tett, és ez idáig a többi uniós országgal való egységes vélemény kidolgozása is elmaradt.

Összegzés

A tagállamok adatvédelmi hatóságainak gyakorlatai között különbségek mutatkoznak, ez – egyelőre – nem tesz eleget a 29-es Adatvédelmi Munkacsoport által szükségesnek tartott egységes, kollektív implementáció követelményének. Az Európai Unió és az Egyesült Államok közötti adattovábbítás bázisa, a Safe Harbor határozat érvénytelenítésével az eddig kialakult adatvédelmi gyakorlat megroppant, bizonytalanságban hagyva a piaci szereplőket és néha még magukat a tagállami adatvédelmi hatóságokat is. Némi aggodalomra adhat okot a német Adatvédelmi Hatóságok Adatvédelmi Konferenciájának hozzáállása is: véleményük szerint a kötelező erejű vállalati szabályozás és az általános szerződési feltételek is csak megkérdőjelezhető mértékben biztosítják a személyes adatok megfelelő szintű védelmét. E logikából kiindulva akár az a helyzet is előfordulhat, hogy egy előzetes döntéshozatali eljárás során a bíróság érvénytelenné nyilvánítja a bizottság általános szerződési feltételekre vonatkozó határozatait, ami beláthatatlan következményekkel járna a további adatvédelmi gyakorlatra.

Abban egységes álláspont mutatkozik a tagállamok és az Európai Unió között, hogy égető szükség van egy mielőbbi, megújult Safe Harborra, amelyet remélhetőleg a Privacy Shield rendszer megfelelően tud biztosítani.

36 NAIH-közlemény az Európai Unió Bíróságának a Safe Harbor ügyben hozott ítéletéről. http://www.naih.hu/files/2015-10-06-Kozlemeny—-Safe-harbor.pdf