Ajánlások

Translations proofread by EDPB Members.
This language version has not yet been proofread.

01/2020. számú ajánlás az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében kiegészítő intézkedésekről

Elfogadás időpontja: 2020. november 10.

Összefoglaló

Az Európai Unió általános adatvédelmi rendelete kettős célt szolgál: a személyes adatok Európai Unión belüli szabad áramlásának elősegítését az egyének alapvető jogainak és szabadságainak, különösen a személyes adatok védelméhez való jogának egyidejű megőrzése mellett.

Közelmúltbeli „Schrems II" ítéletében (C-311/18) az Európai Unió Bírósága (EUB) arra emlékeztet bennünket, hogy a személyes adatok Európai Gazdasági Térségben (EGT) biztosított védelmét az adatok helyétől függetlenül biztosítani kell. A személyes adatok harmadik országokba történő továbbítása nem alkalmazható az EGT-ben biztosított védelem aláásásának vagy gyengítésének eszközeként. A Bíróság ezt annak egyértelművé tételével is megerősíti, hogy a harmadik országokban biztosított védelmi szintnek nem azonosnak, hanem lényegében azonosnak kell lennie az EGT-ben biztosított védelmi szinttel. A Bíróság fenntartja továbbá az általános szerződési feltételek mint egy olyan adattovábbítási eszköz érvényességét, amely a harmadik országokba továbbított adatok védelmének lényegében azonos szintjét biztosíthatja szerződéses úton.

Az általános szerződési feltételeket és az általános adatvédelmi rendelet 46. cikkében említett egyéb adattovábbítási eszközöket nem vákuum veszi körül. A Bíróság megállapítja, hogy az adatátadóként eljáró adatkezelők vagy adatfeldolgozók feladata, hogy esetről esetre és adott esetben a harmadik országbeli adatátvevővel együttműködve ellenőrizzék, hogy a harmadik ország joga vagy gyakorlata hatással van-e az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközökben foglalt megfelelő garanciák hatékonyságára. Ezekben az esetekben a Bíróság továbbra is nyitva hagyja annak lehetőségét, hogy az adatátadók olyan további intézkedéseket hajtsanak végre, amelyek pótolják a védelem e hiányosságait, és az uniós jog által előírt szintre emelik azt. A Bíróság nem pontosítja, hogy ezek milyen intézkedések lehetnek. A Bíróság hangsúlyozza azonban, hogy az adatátadóknak esetről esetre kell azonosítaniuk azokat. Ez összhangban áll az elszámoltathatóságnak az általános adatvédelmi rendelet 5. cikkének (2) bekezdésében rögzített elvével, amely szerint az adatkezelők felelősek az általános adatvédelmi rendeletben foglalt, a személyes adatok kezelésére vonatkozó elveknek való megfelelésért, továbbá képesnek kell lenniük e megfelelés igazolására.

Annak érdekében, hogy segítséget nyújtson az adatátadóknak (legyenek azok akár az általános adatvédelmi rendelet hatálya alá tartozó személyes adatokat kezelő adatkezelők vagy adatfeldolgozók, akár ilyen adatokat kezelő magánszervezetek vagy közjogi szervek) a harmadik országok értékelésének és szükség esetén a megfelelő további intézkedések azonosításának összetett feladatában, az Európai Adatvédelmi Testület elfogadta ezt az ajánlást. Ez az ajánlás egymás után követendő lépéseket, lehetséges információforrásokat és néhány, lehetséges további intézkedésekre vonatkozó példát kínál az adatátadók számára.

Első lépésként az Európai Adatvédelmi Testület azt tanácsolja Önnek mint adatátadónak, hogy **ismerje saját adattovábbításait**. A harmadik országokba irányuló összes személyesadat-továbbítás feltérképezése nehéz feladat lehet. Annak biztosítása érdekében azonban, hogy a személyes adatok kezelésük helyétől függetlenül lényegében azonos szintű védelmet élvezzenek, tisztában kell lenni azzal, hogy hova kerülnek azok. Azt is ellenőriznie kell, hogy az Ön által továbbított adatok a harmadik országba történő adattovábbítás és a harmadik országbeli adatkezelés céljai szempontjából megfelelőek és relevánsak-e, és a szükségesre korlátozódnak-e.

A **második lépés** annak **ellenőrzése**, hogy az általános adatvédelmi rendelet V. fejezetében felsoroltak közül **melyik adattovábbítási eszközön alapul az Ön által végzett továbbítás**. Ha az Európai Bizottság az általános adatvédelmi rendelet 45. cikke vagy a korábbi 95/46/EK irányelv alapján hozott megfelelőségi határozatainak valamelyikével már megfelelőnek nyilvánította azt az országot, régiót

vagy ágazatot, amelybe Ön az adatokat továbbítja, akkor mindaddig, amíg a határozat hatályban van, Önnek nem kell további lépéseket tennie azon kívül, hogy figyelemmel kíséri a megfelelőségi határozat érvényességét. Megfelelőségi határozat hiányában az általános adatvédelmi rendelet 46. cikkében felsorolt adattovábbítási eszközök valamelyikét kell igénybe vennie a rendszeres és ismétlődő adattovábbításokhoz. Az általános adatvédelmi rendelet 49. cikkében meghatározott eltérésekre csak az alkalmi jellegű és nem ismétlődő adattovábbítás néhány esetében hivatkozhat, ha teljesíti a feltételeket.

A **harmadik lépés** annak **értékelése**, hogy **a harmadik ország joga vagy gyakorlata** bármilyen módon hatást gyakorolhat-e azon adattovábbítási eszközök megfelelő garanciáinak hatékonyságára, amelyeket az adott adattovábbítással összefüggésben igénybe vesz. Az értékelésnek elsősorban az Ön által végzett adattovábbítás és az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköz szempontjából releváns harmadik országbeli jogszabályokra kell összpontosítania, amelyek alááshatják az említett adattovábbítási eszköz által biztosított védelmi szintet. Azon elemek értékelését illetően, amelyeket figyelembe kell venni egy harmadik országnak a hatóságok adatokhoz való megfigyelési célú hozzáférésére vonatkozó jogának értékelése során, kérjük, olvassa el az Európai Adatvédelmi Testület alapvető európai garanciákról szóló ajánlását. Ezt különösen akkor kell gondosan mérlegelni, ha a hatóságok adatokhoz való hozzáférésére vonatkozó jogszabályok nem egyértelműek, vagy nem érhetők el nyilvánosan. Az azon körülményeket szabályozó jogszabályok hiányában, amelyek között a hatóságok hozzáférhetnek a személyes adatokhoz, ha továbbra is folytatni kívánja az adattovábbítást, meg kell vizsgálnia más releváns és objektív tényezőket, és nem támaszkodhat olyan szubjektív tényezőkre, mint például annak valószínűsége, hogy a hatóságok az uniós előírásoknak nem megfelelő módon férnek hozzá az Ön adataihoz. Ezt az értékelést kellő gondossággal kell elvégeznie, és alaposan dokumentálnia kell, mivel elszámoltatható lesz az annak alapján hozott döntésért.

A **negyedik lépés** azon **további intézkedések azonosítása és elfogadása**, amelyek szükségesek ahhoz, hogy a továbbított adatok védelmének szintje megfeleljen a lényegi azonosság uniós követelményének. Erre a lépésre csak akkor van szükség, ha az Ön értékelése azt tárja fel, hogy a harmadik ország jogszabályai hatással vannak az általános adatvédelmi rendelet 46. cikke szerinti, Ön által az adattovábbítással összefüggésben igénybe vett vagy igénybe venni kívánt adattovábbítási eszköz hatékonyságára. A jelen ajánlás (2. melléklete) a további intézkedések példáinak és a hatékonyságukhoz szükséges egyes feltételeknek a nem kimerítő felsorolását tartalmazza. A 46. cikk szerinti adattovábbítási eszközökben foglalt megfelelő garanciákhoz hasonlóan egyes további intézkedések egyes országokban hatékonyak lehetnek, másokban azonban nem feltétlenül. Az Ön feladata értékelni ezen intézkedések hatékonyságát az adattovábbítással összefüggésben, valamint a harmadik ország jogának és az Ön által igénybe vett adattovábbítási eszköznek a fényében, és elszámoltatható lesz az Ön által hozott döntésért. Ehhez több további intézkedés kombinálására is szükség lehet. Végső soron úgy találhatja, hogy egyetlen további intézkedés sem képes lényegében azonos védelmi szintet biztosítani az Ön által végzett konkrét adattovábbítás esetében. Azokban az esetekben, amelyekben egyetlen további intézkedés sem megfelelő, a személyes adatok védelmi szintje veszélyeztetésének elkerülése érdekében Önnek el kell kerülnie, fel kell függesztenie vagy meg kell szüntetnie az adattovábbítást. A további intézkedések ezen értékelését emellett kellő gondossággal kell elvégeznie, és dokumentálnia kell.

Az **ötödik lépés** minden olyan **hivatalos eljárási lépés megtétele**, amelyre az Ön további intézkedésének elfogadásához szükség lehet, az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköztől függően. A jelen ajánlás részletezi ezeket az alakiságokat.

Előfordulhat, hogy az alakiságok némelyikét illetően konzultálnia kell az illetékes felügyeleti hatóságokkal.

A **hatodik és egyben utolsó lépés**, hogy megfelelő időközönként végezze el az Ön által harmadik országokba továbbított adatok védelmi szintjének újraértékelését, és kísérje figyelemmel, hogy történtek-e vagy várhatók-e olyan fejlemények, amelyek hatással lehetnek e védelmi szintre. Az elszámoltathatóság elve megköveteli a személyes adatok védelmi szintjének folyamatos figyelemmel kísérését.

A felügyeleti hatóságok továbbra is ellátják az általános adatvédelmi rendelet alkalmazásának nyomon követésére és kikényszerítésére irányuló feladatukat. A felügyeleti hatóságok kellő figyelmet fordítanak az adatátadók által annak biztosítása érdekében tett intézkedésekre, hogy az általuk továbbított adatok lényegében azonos szintű védelemben részesüljenek. Amint arra a Bíróság emlékeztet, a felügyeleti hatóságok felfüggesztik vagy megtiltják az adattovábbítást azokban az esetekben, amelyekben – a vizsgálatuk végén vagy panasz nyomán – úgy ítélik meg, hogy nem biztosítható lényegében azonos védelmi szint.

A felügyeleti hatóságok az uniós adatvédelmi jog következetes alkalmazásának biztosítása érdekében folytatják útmutatások adatátadók részére történő kidolgozását, és továbbra is összehangolják fellépésüket az Európai Adatvédelmi Testületen belül.

Tartalomjegyzék

Az Európai Adatvédelmi Testület

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával[1] módosított XI. mellékletére és 37. jegyzőkönyvére,

tekintettel eljárási szabályzatának 12. és 22. cikkére,

mivel:

(1) Az Európai Unió Bírósága (EUB) a 2020. július 16-i Data Protection Commissioner kontra Facebook Ireland LTD, Maximillian Schrems ítéletében (C-311/18) arra a következtetésre jutott, hogy az általános adatvédelmi rendelet 46. cikkének (1) bekezdését és 46. cikke (2) bekezdésének c) pontját úgy kell értelmezni, hogy az e rendelkezések által megkövetelt megfelelő garanciáknak, érvényesíthető jogoknak és hatékony jogorvoslati lehetőségeknek biztosítaniuk kell, hogy azon személyek jogai, akiknek a személyes adatait az általános adatvédelmi kikötések alapján továbbítják harmadik országba, olyan védelmi szinttel rendelkezzenek, amely lényegében azonos az Európai Unió Alapjogi Chartája fényében értelmezett e rendelet által az Európai Unióban biztosított védelmi szinttel.[2]

(2) Amint azt a Bíróság hangsúlyozta, a természetes személyek számára biztosított védelmi szintet, amely lényegében azonos a Charta fényében értelmezett, az általános adatvédelmi rendelet által az Európai Unióban biztosított védelmi szinttel, az V. fejezet azon rendelkezésétől függetlenül kell biztosítani, amely alapján a személyes adatokat harmadik országba továbbítják. Az V. fejezet rendelkezéseinek célja e védelem magas szintjének folyamatos fenntartása a személyes adatok harmadik országba irányuló továbbítása esetén.[3]

(3) Az általános adatvédelmi rendelet (108) preambulumbekezdése és 46. cikkének (1) bekezdése értelmében uniós megfelelőségi határozat hiányában az adatkezelő vagy az adatfeldolgozó a megfelelő garanciák érintett számára való biztosítása útján gondoskodik az adatvédelem harmadik országbeli hiányosságainak ellensúlyozásáról. Az adatkezelő vagy adatfeldolgozó az általános adatvédelmi rendelet 46. cikkének (2) bekezdésében felsorolt adattovábbítási eszközök – például általános adatvédelmi kikötések – használata révén nyújthat megfelelő garanciákat a felügyeleti hatóság külön engedélye nélkül.

[1] A jelen dokumentumban a „tagállamokra” történő bármely hivatkozást „EGT-tagállamokra” történő hivatkozásként kell érteni.
[2] Az EUB 2020. július 16-i ítélete, Data Protection Commissioner kontra Facebook Ireland Ltd, Maximillian Schrems (a továbbiakban: „Schrems II” ítélet [C-311/18]), a rendelkező rész 2) pontja.
[3] „Schrems II” ítélet (C-311/18), 92. és 93. pont.

(4) A Bíróság egyértelművé teszi, hogy a Bizottság által elfogadott általános adatvédelmi kikötések kizárólag arra irányulnak, hogy az Unióban letelepedett adatkezelőknek vagy az ott letelepedett adatfeldolgozóiknak minden harmadik országban egységesen alkalmazandó szerződéses garanciákat biztosítsanak. Szerződéses jellegük miatt az általános adatvédelmi kikötések nem köthetik harmadik országok hatóságait, mivel ez utóbbiak nem szerződő felek. Következésképpen előfordulhat, hogy az adatátadóknak az uniós jog által megkövetelt védelmi szint egy adott harmadik országban történő tiszteletben tartásának biztosítása érdekében további intézkedésekkel kell kiegészíteniük azon garanciákat, amelyeket ezen általános adatvédelmi kikötések tartalmaznak. A Bíróság hivatkozik az általános adatvédelmi rendelet (109) preambulumbekezdésére, amely megemlíti ezt a lehetőséget, és arra ösztönzi az adatkezelőket és az adatfeldolgozókat, hogy éljenek azzal.[4]

(5) A Bíróság megállapította, hogy mindenekelőtt az adatátadó feladata, hogy esetről esetre és adott esetben az adatátvevővel együttműködve ellenőrizze, hogy a célországnak számító harmadik ország joga az általános adatvédelmi kikötések alapján továbbított személyes adatok védelmének lényegében azonos szintjét biztosítja-e az uniós jog tekintetében, szükség esetén az e kikötések által előírt intézkedéseken felül további intézkedéseket előírva.[5]

(6) Ha az Unióban letelepedett adatkezelő vagy adatfeldolgozója nem hozhat az uniós jog tekintetében lényegében azonos védelmi szint biztosításához szükséges további intézkedéseket, az adatkezelő, vagy másodlagosan az illetékes felügyeleti hatóság köteles felfüggeszteni vagy megszüntetni a személyes adatoknak az érintett harmadik országba irányuló továbbítását.[6]

(7) Az általános adatvédelmi rendelet vagy a Bíróság nem határozza meg vagy pontosítja azokat az általános adatvédelmi rendelet 46. cikkének (2) bekezdésében felsorolt adattovábbítási eszközök garanciáihoz képest „további garanciákat" vagy „további intézkedéseket", amelyeket az adatkezelők és adatfeldolgozók elfogadhatnak az uniós jog által megkövetelt védelmi szint egy adott harmadik országban történő tiszteletben tartásának biztosítása érdekében.

(8) Az Európai Adatvédelmi Testület a saját kezdeményezésére úgy határozott, hogy megvizsgálja ezt a kérdést, és ajánlást ad az adatátadóként eljáró adatkezelőknek és adatfeldolgozóknak arra vonatkozóan, hogy milyen eljárást követhetnek további intézkedések azonosítása és elfogadása érdekében. Ezen ajánlás célja, hogy módszertant biztosítson az adatátadók számára annak megállapításához, hogy szükség van-e további intézkedésekre, és ha igen, milyen további intézkedésekre van szükség az általuk végzett adattovábbításhoz. Az adatátadók elsődleges felelőssége annak biztosítása, hogy a továbbított adatok az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet élvezzenek a harmadik országban. Ezen ajánlással az Európai Adatvédelmi Testület a megbízatásának megfelelően az általános adatvédelmi rendelet és a Bíróság ítéletének egységes alkalmazását kívánja elősegíteni[7]

ELFOGADTA A KÖVETKEZŐ AJÁNLÁST:

[4] „Schrems II" ítélet (C-311/18), 132. és 133. pont.
[5] „Schrems II" ítélet (C-311/18), 134. pont.
[6] „Schrems II" ítélet (C-311/18), 135. pont.
[7] Az általános adatvédelmi rendelet 70. cikke (1) bekezdésének e) pontja.

1 AZ ADATTOVÁBBÍTÁSSAL KAPCSOLATOS ELSZÁMOLTATHATÓSÁG

1. Az elsődleges uniós jog alapvető jognak tekinti az adatvédelemhez való jogot.[8] Az adatvédelemhez való jog következésképpen magas szintű védelmet élvez, és csak a törvény által, e jog lényeges tartalmának tiszteletben tartásával, arányoson korlátozható, csak akkor és annyiban, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.[9] A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal.[10]

2. Annak biztosítása érdekében, hogy az általános adatvédelmi rendeletben garantált védelmi szint ne sérüljön, az adatoknak az EGT-n kívüli harmadik országokba történő továbbításuk során az Európai Unióban biztosítottal lényegében azonos szintű védelmet kell élvezniük.

3. Az adatvédelemhez való jog aktív jellegű. E jog többet követel meg annál, mint hogy az adatátadók és adatátvevők (függetlenül attól, hogy adatkezelők és/vagy adatfeldolgozók-e) egyszerűen elismerjék vagy passzívan tiszteletben tartsák ezt a jogot.[11] Az adatkezelőknek és adatfeldolgozóknak törekedniük kell arra, hogy az adatvédelemhez való jog hatékonyságát biztosító jogi, technikai és szervezési intézkedések végrehajtásával aktívan és folyamatosan tiszteletben tartsák ezt a jogot. Az adatkezelőknek és adatfeldolgozóknak arra is képesnek kell lenniük, hogy ezeket az erőfeszítéseket igazolják az érintettek, a nyilvánosság és az adatvédelmi felügyeleti hatóságok felé. Ez az úgynevezett elszámoltathatóság elve.[12]

4. Az általános adatvédelmi rendelet által biztosított védelmi szint hatékony alkalmazásának biztosításához szükséges elszámoltathatóság elve a harmadik országokba irányuló adattovábbításokra is vonatkozik[13], mivel ezek önmagukban az adatkezelés egyik formájának minősülnek.[14] Amint azt a Bíróság hangsúlyozta ítéletében, a Charta fényében értelmezett, az általános adatvédelmi rendelet által az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet az V. fejezet azon rendelkezésétől függetlenül kell biztosítani, amely alapján a személyes adatokat harmadik országba továbbítják.[15]

5. A „Schrems II” ítéletben a Bíróság hangsúlyozza az adatátadók és adatátvevők felelősségét egyrészt annak biztosításáért, hogy a személyes adatok kezelése megfelelt és továbbra is megfelel az uniós adatvédelmi jog által meghatározott védelmi szintnek, másrészt pedig az adattovábbítás felfüggesztéséért és/vagy a szerződéstől való elállásért, ha az adatátvevő nem, vagy már nem képes tiszteletben tartani az adatátadó és az adatátvevő közötti vonatkozó szerződésben foglalt általános

[8] Az Alapjogi Charta 8. cikkének (1) bekezdése és az EUMSZ 16. cikk (1) bekezdése, az általános adatvédelmi rendelet (1) preambulumbekezdése, 1. cikkének (2) bekezdése.
[9] Az Európai Unió Alapjogi Chartája 52. cikkének (1) bekezdése.
[10] Az általános adatvédelmi rendelet (4) preambulumbekezdése; Google LLC, a Google Inc. jogutódja, kontra Commission nationale de l’informatique et des libertés (CNIL) ítélet, C-507/17, 60. pont.
[11] Sharpston főtanácsnok 2010. június 17-i indítványa, Volker und Markus Schecke GbR kontra Land Hessen, C-92/09 és C-93/09, 71. pont.
[12] Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 28. cikke (3) bekezdésének h) pontja.
[13] Az általános adatvédelmi rendelet 44. cikke és (101) preambulumbekezdése, valamint 47. cikke (2) bekezdésének d) pontja.
[14] Az EUB 2015. október 6-i ítélete, Maximillian Schrems kontra Data Protection Commissioner, (a továbbiakban: „Schrems I” ítélet [C-362/14]), 45. pont.
[15] „Schrems II” ítélet (C-311/18), 92. és 93. pont.

adatvédelmi kikötéseket.[16] Az adatátadóként eljáró adatkezelőnek vagy adatfeldolgozónak biztosítania kell, hogy az adatátvevők adott esetben együttműködjenek az adatátadóval e kötelezettségeinek teljesítése során olyan módon, hogy tájékoztatják például a kapott személyes adatok védelmének szintjét érintően az adatátvevő országában bekövetkezett bármely fejleményről.[17] Ezek a kötelezettségek az általános adatvédelmi rendeletben rögzített elszámoltathatóság elvének az adattovábbításokra történő alkalmazását jelentik.[18]

2 ÜTEMTERV: AZ ELSZÁMOLTATHATÓSÁG ELVÉNEK AZ ADATTOVÁBBÍTÁSOKRA VALÓ GYAKORLATI ALKALMAZÁSA

6. Az alábbi ütemterv felvázolja, hogy milyen lépéseket kell tenni annak megállapítása érdekében, hogy Önnek (mint adatátadónak) további intézkedéseket kell-e hoznia ahhoz, hogy jogszerűen továbbíthasson adatokat az EGT-n kívülre. Ebben a dokumentumban az „Ön" kifejezés az általános adatvédelmi rendelet hatálya alá tartozó személyes adatokat kezelő – ideértve a magánszervezetek és közjogi szervek által végzett adatkezelést is, amikor az adatokat magánszervezetek részére továbbítják – adatátadóként eljáró adatkezelőt vagy adatfeldolgozót jelenti.[19] A személyes adatok közjogi szervek közötti továbbítását illetően *az (EU) 2016/679 rendeletnek a személyes adatoknak az EGT-n belüli és EGT-n kívüli közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti továbbításáról szóló 46. cikke (2) bekezdésének a) pontjáról és 46. cikke (3) bekezdésének b) pontjáról szóló 2/2020. sz. iránymutatás* nyújt külön útmutatást.[20]

7. Ezt az értékelést és az Ön által választott és végrehajtott további intézkedéseket megfelelően dokumentálnia kell, és kérésre az illetékes felügyeleti hatóság rendelkezésére kell bocsátania ezt a dokumentációt.[21]

2.1 1. lépés: Ismerje az Ön által végzett adattovábbításokat

8. Annak megállapítása érdekében, hogy mi szükséges ahhoz, hogy Ön (mint adatátadó) folytathassa a személyes adatok továbbítását, vagy új személyesadat-továbbításokat hajthasson végre[22], az első lépés annak biztosítása, hogy teljes mértékben tisztában legyen az Ön által végzett adattovábbításokkal (ismerje az Ön által végzett adattovábbításokat). Az összes adattovábbítás nyilvántartásba vétele és feltérképezése összetett feladatot jelenthet azon jogalanyok számára, amelyek több, sokrétű és rendszeres adattovábbítást végeznek harmadik országok irányába, és több adatfeldolgozót és további

[16] „Schrems II" ítélet (C-311/18), 134., 135., 139., 140., 141., 142. pont.
[17] „Schrems II" ítélet (C-311/18), 134. pont.
[18] Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 28. cikke (3) bekezdésének h) pontja.
[19] Lásd: az Európai Adatvédelmi Testület 3/2018. sz. iránymutatása az általános adatvédelmi rendelet területi hatályáról (3. cikk) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[20] Az Európai Adatvédelmi Testület 2/2020. sz. iránymutatása az (EU) 2016/679 rendeletnek a személyes adatoknak az EGT-n belüli és EGT-n kívüli közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti továbbításáról szóló 46. cikke (2) bekezdésének a) pontjáról és 46. cikke (3) bekezdésének b) pontjáról; lásd: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_hu
[21] Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 24. cikkének (1) bekezdése.
[22] Kérjük, vegye figyelembe, hogy adattovábbításnak minősül a harmadik országbeli jogalany által az EGT-ben található adatokhoz való távoli hozzáférés is.

adatfeldolgozót vesznek igénybe. Az Ön által végzett adattovábbítások ismerete az első alapvető lépés az elszámoltathatóság elve alapján fennálló kötelezettségeinek teljesítéséhez.

9. Az Ön által végzett adattovábbítások teljes körű megismerése érdekében támaszkodhat azokra az adatkezelési tevékenységekre vonatkozó nyilvántartásokra, amelyeket az általános adatvédelmi rendelet 30. cikke alapján adatkezelőként vagy adatfeldolgozóként kell vezetnie.[23] Az általános adatvédelmi rendelet 13. cikke (1) bekezdésének f) pontja és 14. cikke (1) bekezdésének f) pontja szerinti, az érintetteknek a személyes adataik Ön által harmadik országokba történő továbbításáról való tájékoztatására vonatkozó kötelezettségek teljesítésére irányuló korábbi intézkedések szintén segítséget nyújthatnak Önnek.[24]

10. Az adattovábbítások feltérképezésekor ne felejtse el figyelembe venni az újbóli adattovábbításokat is, például azt, hogy az Ön EGT-n kívüli adatfeldolgozói továbbítják-e az Ön által rájuk bízott személyes adatokat egy másik harmadik országbeli vagy ugyanazon harmadik országbeli további adatfeldolgozónak[25].

11. Önnek az általános adatvédelmi rendelet „adattakarékosságra” vonatkozó elvével[26] összhangban ellenőriznie kell, hogy az Ön által továbbított adatok a harmadik országba történő adattovábbítás és a harmadik országbeli adatkezelés céljai szempontjából megfelelőek és relevánsak-e, és a szükségesre korlátozódnak-e.

12. E tevékenységeket minden adattovábbítás előtt el kell végezni, és azokat az adattovábbításoknak az adattovábbítási műveletek felfüggesztését követő folytatása előtt naprakésszé kell tenni: tudnia kell, hogy az Ön által átadott személyes adatok hol lehetnek megtalálhatók vagy az adatátvevők által kezelhetők (célállomások térképe).

[23] Lásd az adatvédelmi rendelet 30. cikkét és különösen az (1) bekezdés e) pontját és a (2) bekezdés c) pontját. Adatkezelési nyilvántartásának tartalmaznia kell ezenfelül adatkezelési tevékenységeinek ismertetését (ideértve többek között az érintettek kategóriáit, a személyes adatok kategóriáit és az adatkezelés céljait, valamint az adattovábbításra vonatkozó konkrét információkat). Egyes adatkezelők és adatfeldolgozók mentesülnek az adatkezelési nyilvántartás vezetésének kötelezettsége alól (az általános adatvédelmi rendelet 30. cikkének (5) bekezdése). Az e mentességgel kapcsolatos útmutatásért lásd a 29. cikk szerinti munkacsoportnak az általános adatvédelmi rendelet 30. cikkének (5) bekezdése szerinti, az adatkezelési tevékenységekre vonatkozó nyilvántartás vezetésének kötelezettségétől való eltérésekről szóló állásfoglalását (amelyet az Európai Adatvédelmi Testület 2018. május 25-én hagyott jóvá).

[24] Az általános adatvédelmi rendelet átláthatósági szabályai értelmében tájékoztatnia kell az érintetteket a személyes adatok harmadik országokba történő továbbításáról (az általános adatvédelmi rendelet 13. cikke (1) bekezdésének f) pontja és 14. cikke (1) bekezdésének f) pontja). Az érintetteket tájékoztatnia kell különösen az Európai Bizottság megfelelőségi határozatának létéről vagy annak hiányáról, vagy az általános adatvédelmi rendelet 46. cikkében, 47. cikkében vagy 49. cikke (1) bekezdésének második albekezdésében említett adattovábbítás esetén meg kell jelölnie a megfelelő és alkalmas garanciákat, valamint hivatkoznia kell az azok másolatának megszerzésére szolgáló módokra vagy azok elérhetőségére. Az érintett rendelkezésére bocsátott információknak pontosnak és naprakésznek kell lenniük, különösen a Bíróság adattovábbítással kapcsolatos ítélkezési gyakorlatának fényében.

[25] Ha az adatkezelő az általános adatvédelmi rendelet 28. cikkének (2) bekezdésével összhangban előzetesen írásban eseti vagy általános felhatalmazást tett.

[26] Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja.

13. Tartsa szem előtt, hogy a harmadik országból való távoli hozzáférés (például támogatási helyzetekben) és/vagy az EGT-n kívül található felhőben való tárolás szintén adattovábbításnak minősül.[27] Konkrétabban, ha Ön nemzetközi felhőinfrastruktúrát használ, fel kell mérnie, hogy adatait harmadik országokba továbbítják-e, és ha igen, hova, kivéve, ha a felhőszolgáltató egyértelműen kijelenti a szerződésben, hogy az adatokat egyáltalán nem kezelik harmadik országokban.

2.2 2. lépés: Azonosítsa azokat az adattovábbítási eszközöket, amelyeket igénybe kíván venni

14. Második lépésként azonosítania kell az általános adatvédelmi rendelet V. fejezetében felsorolt és előírt adattovábbítási eszközök közül azokat, amelyeket igénybe kíván venni.

Megfelelőségi határozatok

15. Az Európai Bizottság azon harmadik országok némelyikére vagy mindegyikére vonatkozó **megfelelőségi határozatai** révén, amelyekbe Ön személyes adatokat továbbít, elismerheti, hogy ezen országok megfelelő védelmi szintet biztosítanak a személyes adatok tekintetében.[28]

16. Az ilyen megfelelőségi határozat azzal a hatással jár, hogy az EGT-ből személyes adatok áramolhatnak az adott harmadik országba anélkül, hogy az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközre lenne szükség.

17. A megfelelőségi határozatok vonatkozhatnak egy ország egészére, vagy korlátozódhatnak annak egy részére. A megfelelőségi határozatok kiterjedhetnek az országba irányuló valamennyi adattovábbításra, vagy korlátozódhatnak bizonyos típusú adattovábbításokra (például egy ágazatban).[29]

18. Az Európai Bizottság a honlapján közzéteszi a megfelelőségi határozatok jegyzékét.[30]

19. Ha Ön személyes adatokat továbbít (az alkalmazandó mértékben) a Bizottság megfelelőségi határozatának hatálya alá tartozó harmadik országokba, régiókba vagy ágazatokba, **nem kell megtennie az ezen ajánlásban ismertetett további lépéseket**.[31] Továbbra is figyelemmel kell azonban kísérnie, hogy az Ön által végzett adattovábbításokkal kapcsolatos megfelelőségi határozatokat visszavonták vagy érvénytelenítették-e.[32]

---

[27] Lásd a gyakran feltett kérdések 11) pontját: „figyelembe kell venni, hogy még a harmadik országból származó adatokhoz való, például igazgatási célú hozzáférés biztosítása is adattovábbításnak minősül"; Európai Adatvédelmi Testület, Gyakran feltett kérdések az Európai Unió Bíróságának a C-311/18. sz., adatvédelmi biztos kontra Facebook Ireland Ltd és Maximillian Schrems ügyben hozott ítéletéről, 2020. július 23.

[28] Az Európai Bizottság az általános adatvédelmi rendelet 45. cikke alapján megállapíthatja, hogy valamely Európai Unión kívüli ország megfelelő adatvédelmi szintet biztosít-e. Az Európai Bizottság azt is megállapíthatja, hogy egy nemzetközi szervezet megfelelő védelmi szintet biztosít.

[29] Az általános adatvédelmi rendelet 45. cikkének (1) bekezdése.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[31] Feltéve, hogy Ön és az adatátvevő intézkedéseket hajtott végre az általános adatvédelmi rendelet szerinti egyéb kötelezettségeknek való megfelelés érdekében; ellenkező esetben végre kell hajtani ezeket az intézkedéseket.

[32] Az Európai Bizottságnak rendszeres időközönként felül kell vizsgálnia valamennyi megfelelőségi határozatot, és figyelemmel kell kísérnie, hogy a megfelelőségi határozatokkal rendelkező harmadik országok továbbra is megfelelő védelmi szintet biztosítanak-e (lásd az általános adatvédelmi rendelet 45. cikkének (3) és (4)

20. A megfelelőségi határozatok mindazonáltal nem akadályozzák meg az érintetteket abban, hogy panaszt nyújtsanak be. A felügyeleti hatóságokat sem akadályozzák meg abban, hogy keresetet indítsanak a nemzeti bíróság előtt, amennyiben kétségeik vannak a határozat érvényessége tekintetében, hogy így a nemzeti bíróság előzetes döntéshozatali eljárást kezdeményezhessen az EUB előtt ezen érvényesség vizsgálata céljából.[33]

Példa: 2013 júniusában egy uniós polgár, M. Schrems panaszt nyújtott be az ír adatvédelmi bizottsághoz, és azt kérte e felügyeleti hatóságtól, hogy tiltsa meg vagy függessze fel személyes adatainak a Facebook Ireland által az Egyesült Államokba való továbbítását, mivel úgy vélte, hogy az Egyesült Államok joga és gyakorlata nem biztosít a területén tárolt személyes adatok számára elégséges védelmet a hatóságok által folytatott megfigyelési tevékenységekkel szemben. Az adatvédelmi bizottság többek között azzal az indokkal utasította el a panaszt, hogy az Európai Bizottság a 2000/520 határozatban úgy ítélte meg, hogy az Egyesült Államok a továbbított személyes adatok megfelelő szintű védelmét biztosítja a „biztonságos kikötő" rendszer keretében (a továbbiakban: „biztonságos kikötő" határozat). M. Schrems megtámadta az adatvédelmi bizottság határozatát, és az ír High Court a 2000/520 határozat érvényességére vonatkozó kérdést terjesztett az Európai Unió Bírósága (EUB) elé. Az EUB ezt követően úgy határozott, hogy érvénytelennek nyilvánítja a „biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről szóló 2000/520 bizottsági határozatot.[34]

Az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök

21. Az általános adatvédelmi rendelet 46. cikke egy sor olyan, *„megfelelő garanciákat"* tartalmazó adattovábbítási eszközt sorol fel, amelyeket az adatátadók a személyes adatok harmadik országokba történő továbbításához használhatnak megfelelőségi határozatok hiányában. Az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök fő típusai a következők:

- általános adatvédelmi kikötések (SCC□k);
- kötelező erejű vállalati szabályok (BCR□ek);
- magatartási kódexek;
- tanúsítási mechanizmusok;
- ad hoc szerződéses rendelkezések.

bekezdését). Emellett az EUB érvénytelennek nyilváníthatja a megfelelőségi határozatokat (lásd az EUB „Schrems I" ítéletét [C-362/14] és „Schrems II" ítéletét [C-311/18]).

[33] „Schrems II" ítélet (C-311/18), 118–120. pont. A felügyeleti hatóságok nem hagyhatják figyelmen kívül a megfelelőségi határozatot, és nem függeszthetik fel vagy tilthatják meg a személyes adatok ilyen országokba történő továbbítását kizárólag a védelmi szint nem megfelelő voltára hivatkozva. A felügyeleti hatóságok csak egyéb indokok (például az általános adatvédelmi rendelet 32. cikkét sértő elégtelen biztonsági intézkedések, az általános adatvédelmi rendelet 6. cikkét sértő módon egyetlen jogalap sem támasztja alá érvényesen az adatkezelést) alapján gyakorolhatják a személyes adatok ilyen harmadik országba történő továbbításának felfüggesztésére vagy megtiltására vonatkozó hatáskörüket. A felügyeleti hatóságok teljes függetlenséggel megvizsgálhatják, hogy ezen adattovábbítás tiszteletben tartja□e az általános adatvédelmi rendeletben támasztott követelményeket, és adott esetben a nemzeti bíróságok előtt keresetet indíthatnak annak érdekében, hogy amennyiben az utóbbiaknak kétségei vannak a megfelelőségi határozat érvényessége tekintetében, előzetes döntéshozatali eljárást kezdeményezhessenek az Európai Unió Bírósága előtt ezen érvényesség vizsgálata céljából.

[34] „Schrems I" ügy (C-362/14).

22. Függetlenül attól, hogy az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök közül melyiket választja, biztosítania kell, hogy a továbbított személyes adatok összességében lényegében azonos szintű védelemben részesüljenek.

23. Az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök elsősorban olyan szerződéses jellegű megfelelő garanciákat tartalmaznak, amelyek valamennyi harmadik országba irányuló adattovábbítás esetében alkalmazhatók. Az azon harmadik országban fennálló helyzet, amelybe Ön adatokat továbbít, továbbra is szükségessé teheti, hogy a lényegében azonos védelmi szint biztosítása érdekében kiegészítse ezeket az adattovábbítási eszközöket és az azokban foglalt garanciákat („további intézkedések”).[35]

Eltérések

24. A megfelelőségi határozatok és az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök mellett az általános adatvédelmi rendelet egy harmadik lehetőséget is tartalmaz, amely bizonyos helyzetekben lehetővé teszi a személyes adatok továbbítását. Különleges feltételek mellett továbbra is továbbíthat személyes adatokat az általános adatvédelmi rendelet 49. cikkében felsorolt eltérések alapján.

25. Az általános adatvédelmi rendelet 49. cikke kivételes jelleggel bír. Az abban foglalt eltéréseket szűken kell értelmezni, és főként alkalmi és nem ismétlődő adatkezelési tevékenységekre alkalmazhatók. Az Európai Adatvédelmi Testület kiadta az (EU) 2016/679 rendelet 49. cikke szerinti eltérésekről szóló 2/2018. sz. iránymutatását.[36]

26. Mielőtt az általános adatvédelmi rendelet 49. cikke szerinti eltérésre hagyatkozna, ellenőriznie kell, hogy az Ön által végzett adattovábbítás megfelel-e az e rendelkezés által minden egyes adattovábbítás tekintetében előírt szigorú feltételeknek.

***

27. Ha az Ön által végzett adattovábbítás jogilag sem megfelelőségi határozatra, sem a 49. cikk szerinti eltérésre nem alapozható, akkor a 3. lépéssel kell folytatnia.

2.3 3. lépés: Értékelje, hogy az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköz hatékony-e az adattovábbítás valamennyi körülményének fényében

28. Előfordulhat, hogy az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz kiválasztása nem elegendő. Az adattovábbítási eszköznek biztosítania kell, hogy az adattovábbítás ne sértse az általános adatvédelmi rendeletben garantált védelem szintjét.[37] Más szóval, az Ön adattovábbítási eszközének a gyakorlatban hatékonynak kell lennie.

29. A hatékonyság azt jelenti, hogy a továbbított személyes adatok olyan védelmi szinttel rendelkeznek a harmadik országban, amely lényegében azonos az EGT-ben biztosított védelmi szinttel.[38] Nem ez a helyzet akkor, ha az adatátvevő a harmadik ország adattovábbításra vonatkozó jogszabályai és

[35] „Schrems II” ítélet (C-311/18), 130. és 133. pont. Lásd a lenti 2.3. pontot is.
[36] Ezzel kapcsolatban további útmutatásért lásd: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_hu.
[37] Az általános adatvédelmi rendelet 44. cikke.
[38] „Schrems II” ítélet (C-311/18), 105. pont és a rendelkező rész 2) pontja.

gyakorlatai miatt nem tud eleget tenni az általános adatvédelmi rendelet 46. cikke alapján választott adattovábbítási eszköz szerinti kötelezettségeinek.

30. Ezért Önnek – adott esetben az adatátvevővel együttműködve – értékelnie kell, hogy a harmadik ország joga vagy gyakorlata bármilyen módon hatást gyakorolhat-e az általános adatvédelmi rendelet 46. cikke szerinti azon adattovábbítási eszköz megfelelő garanciáinak hatékonyságára, amelyet az adott adattovábbítással összefüggésben igénybe vesz. Adott esetben adatátvevőjének az Ön rendelkezésére kell bocsátania a letelepedési helye szerinti harmadik országgal kapcsolatos releváns forrásokat és információkat, valamint az adattovábbításra alkalmazandó jogszabályokat. Más – például a 3. mellékletben nem kimerítő jelleggel felsorolt – információforrásokra is támaszkodhat.[39]

31. Az értékelés során figyelembe kell vennie az adattovábbításban részt vevő – az adattovábbítások feltérképezése során azonosított – valamennyi szereplőt (például a harmadik országban adatokat kezelő adatkezelőket, adatfeldolgozókat és további adatfeldolgozókat). Minél több adatkezelő, adatfeldolgozó vagy adatátvevő működik közre, annál összetettebb lesz az Ön értékelése. Ezen értékelés keretében az esetleges újbóli adattovábbítást is figyelembe kell vennie.

32. E célból meg kell vizsgálnia minden egyes adattovábbítás jellemzőit, és meg kell állapítania, hogy az egyes adattovábbításokra hogyan alkalmazandó az adattovábbítás (vagy az újbóli adattovábbítás) célországának belső jogrendje.

33. Az alkalmazandó jogi háttér az adattovábbítás körülményeitől, különösen a következőktől függ:

- az adattovábbítás és -kezelés céljai (például marketing, humán erőforrás, tárolás, informatikai támogatás, klinikai vizsgálatok);
- az adatkezelésben részt vevő szervezetek típusai (állami/magán; adatkezelő/adatfeldolgozó);
- az ágazat, amelyben az adattovábbításra sor kerül (például hirdetéstechnológiai, távközlési, pénzügyi stb.);
- a továbbított személyes adatok kategóriái (például a gyermekekre vonatkozó személyes adatok a harmadik ország külön jogszabályainak hatálya alá tartozhatnak);
- az adatokat a harmadik országban tárolják-e, vagy csak távoli hozzáféréssel érhetők-e el az EU-ban/EGT-ben tárolt adatok;
- a továbbítandó adatok formátuma (például egyszerű szöveg/álnevesített vagy titkosított[40]);
- lehetőség arra, hogy az adatokat a harmadik országból újból továbbítsák egy másik harmadik országba.[41]

34. Meg kell vizsgálnia, hogy az alkalmazandó jogszabályok közül hatással van-e bármelyik az általános adatvédelmi rendelet 46. cikke szerinti, Ön által választott adattovábbítási eszközben foglalt kötelezettségvállalásokra. Ellenőriznie kell, hogy az érintettek számára a nemzetközi adattovábbításokkal kapcsolatos jogaik gyakorlását lehetővé tevő kötelezettségvállalások (például a továbbított adatokhoz való hozzáférés, azok helyesbítése és törlése iránti kérelmek) hatékonyan alkalmazhatók-e a gyakorlatban, és azokat nem akadályozza-e a célországnak számító harmadik ország joga.

[39] Lásd a jelen ajánlás lenti 43. pontját is.

[40] Egyes harmadik országok nem engedélyezik titkosított adatok átvételét.

[41] Ha az adatkezelő az általános adatvédelmi rendelet 28. cikkének (2) bekezdésével összhangban előzetesen írásban eseti vagy általános felhatalmazást tett.

35. Értékelnie kell a vonatkozó általános jellegű szabályokat, amennyiben azok hatással vannak az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt garanciák hatékony alkalmazására és az egyének alapvető jogaira (különösen az érintett számára a harmadik országbeli hatóságok továbbított adatokhoz való hozzáférése esetén biztosított jogorvoslathoz való jogra).

36. Minden esetben különös figyelmet kell fordítania a vonatkozó jogszabályokra, különösen azokra, amelyek meghatározzák a személyes adatok hatóságokkal való közlésére vonatkozó követelményeket, vagy e hatóságok számára hatáskört biztosítanak a személyes adatokhoz való hozzáférésre (például bűnüldözési, szabályozói felügyeleti és nemzetbiztonsági célokból). Ha ezek a követelmények vagy hatáskörök arra korlátozódnak, ami egy demokratikus társadalomban szükséges és arányos,[42] akkor azok nem lehetnek hatással az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszközben foglalt kötelezettségvállalásokra.

37. Az uniós előírásokat, például az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, referenciaként kell használni annak értékeléséhez, hogy a hatóságok ilyen hozzáférése a demokratikus társadalomban szükséges és arányos mértékre korlátozódik-e, és hogy az érintettek számára hatékony jogorvoslatot biztosítanak-e.

38. Ezen értékelés elvégzése során az adott harmadik ország jogrendszerének különböző elemei – például az általános adatvédelmi rendelet 45. cikkének (2) bekezdésében felsorolt tényezők – is relevánsak.[43] Például a jogállamiság valamely harmadik országbeli helyzete releváns lehet az egyének számára a személyes adatokhoz való jogellenes kormányzati hozzáféréssel szemben rendelkezésre álló (bírósági) jogorvoslati mechanizmusok hatékonyságának értékelése szempontjából. Egy átfogó adatvédelmi törvény vagy egy független adatvédelmi hatóság megléte, valamint az adatvédelmi garanciákat előíró nemzetközi jogi eszközök betartása hozzájárulhat a kormányzati beavatkozás arányosságának biztosításához.[44]

***

39. Az Európai Adatvédelmi Testület alapvető európai garanciákról szóló ajánlása meghatározza azokat az elemeket, amelyeket értékelni kell annak megállapításához, hogy a nemzetbiztonsági ügynökségként vagy bűnüldöző hatóságként működő harmadik országbeli hatóságok személyes adatokhoz való hozzáférését szabályozó jogi keret igazolható beavatkozásnak (és ezért úgy) tekinthető-e(, mint amely nincs hatással az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz keretében tett kötelezettségvállalásokra). Ezt különösen akkor kell gondosan mérlegelni, ha a hatóságok adatokhoz való hozzáférésére vonatkozó jogszabályok nem egyértelműek, vagy nem érhetők el nyilvánosan.

[42] Lásd az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, az általános adatvédelmi rendelet 23. cikkének (1) bekezdését, valamint az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló, 2020. november 10-i 02/2020. sz. ajánlását, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_hu.

[43] „Schrems II" ítélet (C-311/18), 104. pont.

[44] Például: a 108. egyezmény (Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során, 108. sz. ETS) vagy a 108+ egyezmény (Modernizált egyezmény az egyének védelméről a személyes adatok feldolgozása során, 223. sz. CETS) érvényesíthető nemzetközi jogorvoslatot biztosít az adatvédelmi jogsértések esetére, és hozzájárul a személyes adatok védelme és a magánélet tiszteletben tartása minimális szintjének biztosításához.

40. A 46. cikk szerinti adattovábbítási eszközökön alapuló adattovábbítások helyzetére alkalmazva az Európai Adatvédelmi Testület alapvető európai garanciákról szóló ajánlása útmutatással szolgálhat az adatátadó és az adatátvevő számára annak értékeléséhez, hogy ezek a hatáskörök indokolatlanul akadályozzák-e az adatátvevőnek a lényegi azonosság biztosítására vonatkozó kötelezettségeit.

41. A lényegében azonos védelmi szint hiánya különösen akkor válik nyilvánvalóvá, ha a harmadik országnak az Ön által végzett adattovábbításra vonatkozó jogi szabályozása vagy gyakorlata nem felel meg az alapvető európai garanciák követelményeinek.

42. Az Ön értékelésének mindenekelőtt a nyilvánosan elérhető jogszabályokon kell alapulnia. Egyes helyzetekben azonban ez nem lesz elegendő, mert előfordulhat, hogy a harmadik országokban hiányoznak a jogszabályok. Ebben az esetben, ha továbbra is végre kívánja hajtani az adattovábbítást, meg kell vizsgálnia más releváns és objektív tényezőket[45], és nem támaszkodhat olyan szubjektív tényezőkre, mint például annak valószínűsége, hogy a hatóságok az uniós előírásoknak nem megfelelő módon férnek hozzá az Ön adataihoz. Ezt az értékelést kellő gondossággal kell elvégeznie, és alaposan dokumentálnia kell, mivel elszámoltatható lesz az annak alapján hozott döntésért.[46]

43. Az értékelést kiegészítheti más forrásokból származó információkkal[47], például az alábbiakkal:

- azt igazoló elemek, hogy a harmadik országbeli hatóság a jelentett precedensek, jogszabályok és gyakorlat fényében az adatátvevő tudtával vagy anélkül hozzá kíván majd férni az adatokhoz;
- azt igazoló elemek, hogy a harmadik országbeli hatóság a bejelentett precedensek, jogkörök, valamint a rendelkezésére álló technikai, pénzügyi és emberi erőforrások fényében az adatátvevőn keresztül vagy a kommunikációs csatorna közvetlen lehallgatása útján képes lesz hozzáférni az adatokhoz.

44. Az Ön értékelése végső soron feltárhatja, hogy az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköz és az abban foglalt megfelelő garanciák:

- hatékonyan biztosítják, hogy a továbbított személyes adatok olyan védelmi szinttel rendelkeznek a harmadik országban, amely lényegében azonos az EGT-ben biztosított védelmi szinttel. A harmadik ország adattovábbításra vonatkozó jogszabályai és gyakorlatai lehetővé teszik az adatátvevő számára, hogy eleget tegyen a választott adattovábbítási eszköz szerinti kötelezettségeinek. Megfelelő időközönként, vagy ha jelentős változások merülnek fel, újraértékelést kell végeznie (lásd a 6. lépést).
- Nem biztosítják hatékonyan a lényegében azonos védelmi szintet. Az adatátvevő a harmadik ország adattovábbításra vonatkozó jogszabályai és/vagy gyakorlatai miatt nem tud eleget tenni kötelezettségeinek. Az EUB hangsúlyozta, hogy amennyiben az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök nem megfelelőek, az adatátadó felelőssége, hogy hatékony további intézkedéseket hozzon, vagy hogy ne továbbítsa a személyes adatokat.[48]

[45] Lásd a jelen ajánlás lenti 43. pontját, valamint a 3. mellékletet.
[46] Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése.
[47] Lásd a 3. mellékletet is.
[48] Az EUB „Schrems II” ítélete (C-311/18), 134. és 135. pont.

Az EUB megállapította például, hogy az egyesült államokbeli FISA 702. szakasza nem felel meg az arányosság uniós jogi elvéből eredő minimális követelményeknek, és nem lehet úgy tekinteni, hogy a feltétlenül szükséges mértékre korlátozódik. Ez azt jelenti, hogy a FISA 702. szakasza által engedélyezett programok védelmi szintje nem minősül lényegében azonosnak az uniós jog által előírt garanciákkal. Következésképpen, ha az adatátvevő vagy bármely olyan további címzett, akivel az adatátvevő közölheti az adatokat, a FISA 702. szakaszának[49] hatálya alá tartozik, az ilyen adattovábbítás csak akkor alapozható SCC-kre vagy az általános adatvédelmi rendelet 46. cikke szerinti más adattovábbítási eszközökre, ha további technikai intézkedések lehetetlenné vagy hatástalanná teszik a továbbított adatokhoz való hozzáférést.

2.4 4. lépés: Fogadjon el további intézkedéseket

45. Ha a 3. lépésben elvégzett értékelése azt tárta fel, hogy az Ön általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköze nem hatékony, akkor – adott esetben az adatátvevővel együttműködve – meg kell vizsgálnia, hogy léteznek-e olyan további intézkedések, amelyek az adattovábbítási eszközökben foglalt garanciákkal együtt biztosíthatják, hogy a továbbított adatokat az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szint illesse meg.[50] A „további intézkedések" jellegüknél fogva kiegészítik az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben már előírt garanciákat.[51]

46. Eseti alapon meg kell állapítania, hogy az általános adatvédelmi rendelet 46. cikke szerinti konkrét adattovábbítási eszköz használata esetén milyen további intézkedések lehetnek hatékonyak egy adott harmadik országba irányuló adattovábbítások esetében. A fenti 1., 2. és 3. lépésben elvégzett korábbi értékelései alapján ellenőrizheti, hogy a további intézkedések mennyire hatékonyak a szükséges védelmi szint biztosítása szempontjából.

47. A további intézkedések főszabály szerint szerződéses, technikai vagy szervezési jellegűek lehetnek. A különböző intézkedések olyan módon történő ötvözése, hogy azok támogassák egymást, és építsenek egymásra, növelheti a védelmi szintet, és ezáltal hozzájárulhat az uniós követelmények teljesítéséhez.

48. A szerződéses és szervezési intézkedések önmagukban általában nem akadályozzák meg a harmadik országbeli hatóságok személyes adatokhoz való hozzáférését (amennyiben ez indokolatlanul akadályozza az adatátvevőnek a lényegi azonosság biztosítására vonatkozó kötelezettségeit). Lesznek ugyanis olyan helyzetek, amelyekben csak technikai intézkedések akadályozhatják meg vagy tehetik hatástalanná a harmadik országbeli hatóságok személyes adatokhoz való – különösen megfigyelési célú – hozzáférését.[52] Ilyen helyzetekben a szerződéses vagy szervezési intézkedések kiegészíthetik a

[49] A FISA 702. szakasza akkor alkalmazandó, ha az adatokat „elektronikus hírközlési szolgáltatótól vagy annak segítségével szerezték be" (a FISA 702. szakasza = az USC 50. címe 1881a. §-ának (h)(2)(A)(vi) pontja); az USC 50. címe 1881. §-ának (b)(4) pontja a következőképpen határozza meg az „elektronikus hírközlési szolgáltató" fogalmát:
„(A) a 47. cím 153. szakaszában meghatározott távközlési szolgáltató;
(B) a 18. cím 2510. szakaszában meghatározott elektronikus hírközlési szolgáltatás nyújtója;
(C) a 18. cím 2711. szakaszában meghatározott távoli számítástechnikai szolgáltatás nyújtója;
(D) bármely más hírközlési szolgáltató, amely a vezetékes vagy elektronikus kommunikáció továbbítása vagy tárolása során hozzáféréssel rendelkezik az ilyen kommunikációhoz;
(E) az (A), (B), (C) vagy (D) alpontban meghatározott szervezet tisztviselője, alkalmazottja vagy képviselője."
[50] „Schrems II" ítélet (C-311/18), 96. pont.
[51] Az általános adatvédelmi rendelet (109) preambulumbekezdése és a „Schrems II" ítélet (C-311/18) 133. pontja.
[52] Amennyiben az ilyen hozzáférés meghaladja a demokratikus társadalomban szükséges és arányos mértéket; lásd az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, az általános adatvédelmi rendelet 23. cikkének (1)

technikai intézkedéseket, és növelhetik az adatvédelem általános szintjét, például azáltal, hogy akadályokat gördítenek a hatóságok arra irányuló kísérletei elé, hogy az uniós előírásokkal összeegyeztethetetlen módon férjenek hozzá az adatokhoz.

49. Adott esetben az adatátvevővel együttműködve megvizsgálhatja az alábbi (nem kimerítő jelleggel felsorolt) tényezőket annak megállapításához, hogy milyen további intézkedések lennének a leghatékonyabbak a továbbított adatok védelme szempontjából:

- a továbbítandó adatok formátuma (például egyszerű szöveg/álnevesített vagy titkosított);
- az adatok jellege;
- az adatkezelési folyamat hossza és összetettsége, az adatkezelésben részt vevő szereplők száma, valamint a közöttük fennálló kapcsolat (például több adatkezelő vagy adatkezelők és adatfeldolgozók is közreműködnek-e az adattovábbításokban, vagy olyan adatfeldolgozók közreműködése, akik az adatokat Öntől az adatátvevőjéhez továbbítják [figyelembe véve a célországnak számító harmadik ország jogszabályai szerint rájuk alkalmazandó vonatkozó rendelkezéseket]);[53]
- annak lehetősége, hogy az adatok ugyanazon harmadik országon belül vagy akár más harmadik országok irányába is újbóli továbbítás tárgyát képezhetik (például az adatátvevő további adatfeldolgozóinak bevonása[54]).

Példák további intézkedésekre

50. A 2. mellékletben foglalt, nem kimerítő felsorolások bemutatnak néhány példát a figyelembe vehető technikai, szerződéses és szervezési intézkedésekre.

***

51. Ha olyan hatékony további intézkedéseket vezetett be, amelyek az általános adatvédelmi rendelet 46. cikke szerinti, Ön által választott adattovábbítási eszközzel együtt olyan védelmi szintet biztosítanak, amely lényegében azonos az EGT-ben biztosított védelmi szinttel, akkor végrehajthatók az adattovábbítások.

52. Amennyiben nem talál, vagy nem hajt végre olyan hatékony további intézkedéseket, amelyek biztosítják, hogy a továbbított személyes adatok lényegében azonos szintű védelemben részesüljenek,[55] az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköz alapján nem kezdheti meg a személyes adatok továbbítását az érintett harmadik országba. Ha már megkezdte az adattovábbítást, fel kell függesztenie vagy meg kell

bekezdését, valamint az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló, 2020. november 10-i 02/2020. sz. ajánlását, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_hu.

[53] Az általános adatvédelmi rendelet eltérő kötelezettségeket ró az adatkezelőkre és az adatfeldolgozókra. Az adattovábbításra sor kerülhet két adatkezelő, közös adatkezelők, az adatkezelő és az adatfeldolgozó, továbbá – az adatkezelő felhatalmazásától függően – az adatfeldolgozó és az adatkezelő, valamint két adatfeldolgozó között.

[54] Lásd az 25. lábjegyzetet.

[55] Amennyiben az ilyen hozzáférés meghaladja a demokratikus társadalomban szükséges és arányos mértéket; lásd az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, az általános adatvédelmi rendelet 23. cikkének (1) bekezdését, valamint az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló, 2020. november 10-i 02/2020. sz. ajánlását, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_hu.

szüntetnie a személyes adatok továbbítását.[56] Az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszközben foglalt garanciáknak megfelelően az adatátvevőnek vissza kell szolgáltatnia az Ön részére az adott harmadik országba Ön által már továbbított adatokat és azok másolatait, vagy teljes egészében meg kell semmisítenie azokat.[57]

Példa: a harmadik ország joga tiltja az Ön által azonosított további intézkedéseket (például a titkosítást), vagy más módon akadályozza azok hatékonyságát. Ön nem kezdheti meg a személyes adatok továbbítását ebbe az országba, vagy meg kell szüntetnie az ebbe az országba irányuló, folyamatban lévő adattovábbításokat.

53. Amennyiben úgy dönt, hogy annak ellenére folytatja az adattovábbítást, hogy az adatátvevő nem tud eleget tenni az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben vállalt kötelezettségeknek, értesítenie kell az illetékes felügyeleti hatóságot az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközbe beillesztett konkrét rendelkezéseknek megfelelően.[58] Az illetékes felügyeleti hatóság felfüggeszti vagy megtiltja az adattovábbítást azokban az esetekben, amelyekben úgy ítéli meg, hogy nem biztosítható lényegében azonos védelmi szint.[59]

54. Az illetékes felügyeleti hatóság bármilyen más korrekciós intézkedést is elrendelhet (például bírságot is kiszabhat), ha Ön annak ellenére, hogy nem tudja igazolni, hogy a harmadik országban lényegében azonos védelmi szint áll fenn, megkezdi vagy folytatja az adattovábbítást.

2.5 5. lépés: Eljárási lépések hatékony további intézkedések azonosítása esetén

55. Az Ön által használt vagy használni tervezett, az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköztől függően eltérőek lehetnek azok az eljárási lépések, amelyeket abban az esetben kell megtennie, ha meghozandó hatékony további intézkedéseket azonosított.

2.5.1 Általános adatvédelmi kikötések (a továbbiakban: SCC-k) (az általános adatvédelmi rendelet 46. cikke (2) bekezdésének c) és d) pontja)

56. Amennyiben Ön további intézkedéseket kíván hozni az SCC-k mellett, nem kell engedélyt kérnie az illetékes felügyeleti hatóságtól ilyen jellegű kikötések vagy további garanciák hozzáadásához, amennyiben az azonosított további intézkedések sem közvetlen, sem közvetett módon nem ellentétesek az SCC-kkel, és elegendőek annak biztosításához, hogy az általános adatvédelmi rendelet által biztosított védelmi szint ne sérüljön.[60] Az adatátadónak és az adatátvevőnek biztosítania kell, hogy

[56] „Schrems II” ítélet (C-311/18), 135. pont.
[57] Lásd az általános szerződési feltételekről szóló 2010/87/EU határozat mellékletében szereplő 12. általános szerződési feltételt; lásd az általános szerződési feltételekről szóló 2004/915/EK határozat B. mellékletében szereplő (választható) rendkívüli megszüntetési záradékot.
[58] Lásd: Európai Adatvédelmi Testület, Gyakran feltett kérdések az Európai Unió Bíróságának a C-311/18. sz., adatvédelmi biztos kontra Facebook Ireland Ltd és Maximillian Schrems ügyben hozott ítéletéről, elfogadás időpontja: 2020. július 23., különösen az 5), 6) és 9) gyakran feltett kérdés. Lásd a 2010/87/EU bizottsági határozat 4. általános szerződési feltételének g) pontját, a 2001/497/EK bizottsági határozatban foglalt általános szerződési feltételek 5. pontjának a) alpontját, valamint a 2004/915/EK bizottsági határozat mellékletében foglalt „II. csomag” II. általános szerződési feltételének c) pontját is.
[59] „Schrems II” ítélet (C-311/18), 113. és 121. pont.
[60] Az általános adatvédelmi rendelet (109) preambulumbekezdése értelmében: „Az a lehetőség, mely szerint az adatkezelő vagy az adatfeldolgozó alkalmazhatja a Bizottság vagy a felügyeleti hatóság által elfogadott általános adatvédelmi kikötéseket, egyik sem zárja ki, hogy az adatkezelő vagy az adatfeldolgozó szélesebb körű szerződésben – ideértve az adatfeldolgozó és valamely egyéb adatfeldolgozó közötti szerződéseket is – alkalmazza ezen általános adatvédelmi kikötéseket, sem azt, hogy további rendelkezéseket vagy garanciákat

a további kikötéseket semmiképpen ne lehessen úgy értelmezni, hogy korlátozzák az SCC-kben foglalt jogokat és kötelezettségeket, vagy bármilyen más módon csökkentsék az adatvédelem szintjét. Képesnek kell lennie arra, hogy ezt – beleértve az összes kikötés egyértelműségét is – az elszámoltathatóság elvének és a megfelelő szintű adatvédelem biztosítására vonatkozó kötelezettségének megfelelően igazolja. Az illetékes felügyeleti hatóságok szükség esetén felülvizsgálhatják ezeket a további kikötéseket (például panasz esetén vagy hivatalból indított vizsgálat útján).

57. Ha módosítani kívánja magukat az általános adatvédelmi kikötéseket, vagy ha a hozzáadott további intézkedések közvetlen vagy közvetett módon „ellentétesek" az SCC-kkel, akkor már nem tekinthető úgy, hogy Ön általános szerződési feltételekre támaszkodik[61], és az általános adatvédelmi rendelet 46. cikke (3) bekezdésének a) pontjával összhangban engedélyt kell kérnie az illetékes felügyeleti hatóságtól.

2.5.2 BCR-ek (az általános adatvédelmi rendelet 46. cikke (2) bekezdésének b) pontja)

58. A „Schrems II" ítéletben szereplő érvelés az általános adatvédelmi rendelet 46. cikkének (2) bekezdése szerinti egyéb adattovábbítási eszközökre is vonatkozik, mivel alapvetően ezen eszközök mindegyike szerződéses jellegű, így az azokban foglalt garanciák és a felek által azokban vállalt kötelezettségek nem köthetik harmadik országok hatóságait.[62]

59. A „Schrems II" ítélet releváns a személyes adatok BCR-ek alapján történő továbbítása szempontjából, mivel a harmadik országok jogszabályai hatással lehetnek az ilyen eszközök által biztosított védelemre. A „Schrems II" ítélet BCR-ekre gyakorolt pontos hatása még mindig vita tárgyát képezi. Az Európai Adatvédelmi Testület a lehető leghamarabb részletesebb tájékoztatást fog nyújtani arról, hogy szükség lehet-e további kötelezettségvállalások beillesztésére a WP256/257 referenciadokumentumokban[63] szereplő BCR-ekbe.

60. A Bíróság kiemelte, hogy az adatátadó és az adatátvevő feladata annak értékelése, hogy az érintett harmadik országban tiszteletben tartják-e az uniós jog által megkövetelt védelmi szintet annak megállapítása érdekében, hogy az általános szerződési feltételek vagy a kötelező erejű vállalati szabályok által nyújtott garanciák a gyakorlatban betarthatók-e. Ellenkező esetben Önnek értékelnie

---

adjon hozzá, feltéve hogy azok sem közvetlen, sem közvetett módon nem ellentétesek a Bizottság vagy a felügyeleti hatóság által elfogadott általános szerződési feltételekkel, és nem sértik az érintettek alapvető jogait és szabadságait." Hasonló rendelkezéseket tartalmaznak a 95/46/EK irányelv alapján az Európai Bizottság által elfogadott SCC-csomagok is.

[61] Lásd analógia útján: az Európai Adatvédelmi Testületnek a 28. cikk szerinti általános szerződési feltételekre vonatkozó, már elfogadott, a szlovén felügyeleti hatóság által benyújtott általános szerződési feltételek tervezetéről (az általános adatvédelmi rendelet 28. cikkének (8) bekezdése) szóló 17/2020. sz. véleményét, amely hasonló rendelkezést tartalmaz („A Testület emellett emlékeztet arra, hogy a valamely felügyeleti hatóság által elfogadott általános szerződési feltételek használatának lehetősége nem akadályozza meg a feleket abban, hogy azokat egyéb feltételekkel vagy kiegészítő biztosítékokkal egészítsék ki, feltéve, hogy azok sem közvetlenül, sem közvetve nem mondanak ellent az elfogadott általános szerződési feltételeknek, illetve nem sértik az érintettek alapvető jogait vagy szabadságait. Ezenkívül az általános adatvédelmi feltételek módosítása esetén már nem lesz úgy tekinthető, hogy a felek elfogadott általános szerződési feltételeket alkalmaztak."), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_hu.pdf.

[62] Az EUB „Schrems II" ítélete (C-311/18), 132. pont.

[63] A 29. cikk szerinti munkacsoportnak a kötelező erejű vállalati szabályokban megtalálható elemek és elvek táblázatáról szóló, legutóbb 2018. február 6-án felülvizsgált és elfogadott WP 256 rev.01 munkadokumentuma; a 29. cikk szerinti munkacsoportnak a kötelező erejű vállalati szabályokban megtalálható elemek és elvek táblázatáról szóló, legutóbb 2018. február 6-án felülvizsgált és elfogadott WP 257 rev.01 munkadokumentuma.

kell, hogy tud-e további intézkedéseket hozni a védelem EGT-ben biztosítottal lényegében azonos szintjének biztosítása érdekében, és hogy a harmadik ország joga vagy gyakorlata nem fogja-e megsérteni ezeket a további intézkedéseket azok hatékonyságának megakadályozása érdekében.

2.5.3 Ad hoc szerződéses rendelkezések (az általános adatvédelmi rendelet 46. cikke (3) bekezdésének a) pontja)

61. A „Schrems II” ítéletben szereplő érvelés az általános adatvédelmi rendelet 46. cikkének (2) bekezdése szerinti egyéb adattovábbítási eszközökre is vonatkozik, mivel alapvetően ezen eszközök mindegyike szerződéses jellegű, így az azokban foglalt garanciák és a felek által azokban vállalt kötelezettségek nem köthetik harmadik országok hatóságait.[64] A „Schrems II” ítélet ezért releváns a személyes adatok ad hoc szerződéses rendelkezések alapján történő továbbítása szempontjából, mivel a harmadik országok jogszabályai hatással lehetnek az ilyen eszközök által biztosított védelemre. A „Schrems II” ítélet ad hoc rendelkezésekre gyakorolt pontos hatása még mindig vita tárgyát képezi. Az Európai Adatvédelmi Testület a lehető leghamarabb részletesebb tájékoztatást fog nyújtani.

2.6 6. lépés: Végezzen újraértékelést megfelelő időközönként

62. Önnek – adott esetben az adatátvevőkkel együttműködve – folyamatosan figyelemmel kell kísérnie azokat az Ön által végzett személyesadat-továbbítás célországának számító harmadik országban bekövetkező fejleményeket, amelyek hatással lehetnek a védelmi szint Ön által elvégzett kezdeti értékelésére és az adattovábbítással kapcsolatban Ön által hozott esetleges döntésekre. Az elszámoltathatóság folyamatos kötelezettség (az általános adatvédelmi rendelet 5. cikkének (2) bekezdése).

63. Kellően megbízható mechanizmusokat kell bevezetnie annak biztosítására, hogy az adattovábbításokat haladéktalanul felfüggeszti vagy megszünteti, ha:

- az adatátvevő megszegte vagy nem tudja teljesíteni az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben vállalt kötelezettségeit;
- a további intézkedések már nem hatékonyak az érintett harmadik országban.

[64] Az EUB „Schrems II” ítélete (C-311/18), 132. pont.

3 KÖVETKEZTETÉS

64. Az általános adatvédelmi rendelet szabályokat állapít meg a személyes adatok EGT-n belüli kezelésére vonatkozóan, és ezáltal lehetővé teszi a személyes adatok EGT-n belüli szabad áramlását. Az általános adatvédelmi rendelet V. fejezete a személyes adatok harmadik országokba történő továbbítását szabályozva magasra teszi a mércét: az adattovábbítás nem sértheti a természetes személyek számára az általános adatvédelmi rendeletben garantált védelem szintjét (az általános adatvédelmi rendelet 44. cikke). Az EUB „Schrems II" ítélete (C-311/18) hangsúlyozza, hogy folyamatosan fenn kell tartani a harmadik országba továbbított személyes adatok védelmének az általános adatvédelmi rendeletben biztosított szintjét.[65]

65. Adatai lényegében azonos szintű védelmének biztosítása érdekében Önnek mindenekelőtt alaposan ismernie kell az Ön által végzett adattovábbításokat. Azt is ellenőriznie kell, hogy az Ön által továbbított adatok a harmadik országba történő adattovábbítás és a harmadik országbeli adatkezelés céljai szempontjából megfelelőek és relevánsak-e, és a szükségesre korlátozódnak-e.

66. Azonosítania kell azt az adattovábbítási eszközt is, amelyet az adattovábbításhoz igénybe kíván venni. Ha az adattovábbítási eszköz nem megfelelőségi határozat, eseti alapon ellenőriznie kell, hogy a célországnak számító harmadik ország joga vagy gyakorlata sérti-e (vagy sem) az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt garanciákat az Ön által végzett adattovábbításokkal összefüggésben. Ha az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz önmagában nem biztosítja az Ön által továbbított személyes adatok védelmének lényegében azonos szintjét, a hiányosságok adott esetben további intézkedésekkel pótolhatók.

67. Amennyiben nem talál, vagy nem hajt végre olyan hatékony további intézkedéseket, amelyek biztosítják, hogy a továbbított személyes adatok lényegében azonos szintű védelemben részesüljenek, az Ön által választott adattovábbítási eszköz alapján nem kezdheti meg a személyes adatok továbbítását az érintett harmadik országba. Ha már megkezdte az adattovábbítást, haladéktalanul fel kell függesztenie vagy meg kell szüntetnie a személyes adatok továbbítását.

68. Az illetékes felügyeleti hatóság felfüggesztheti vagy megszüntetheti a személyes adatok harmadik országba történő továbbítását, ha nem biztosított a továbbított adatoknak az uniós jog – különösen az általános adatvédelmi rendelet 45. és 46. cikke, valamint az Alapjogi Charta – által előírt védelme.

Az Európai Adatvédelmi Testület nevében

az elnök

(Andrea Jelinek)

[65] „Schrems II" ítélet (C-311/18), 93. pont.

1. MELLÉKLET: FOGALOMMEGHATÁROZÁSOK

- „Harmadik ország”: minden olyan ország, amely nem tagállama az EGT-nek.
- „EGT”: az Európai Gazdasági Térség, amely magában foglalja az Európai Unió tagállamait, valamint Izlandot, Norvégiát és Liechtensteint. Ez utóbbira az EGT-megállapodás és különösen annak XI. melléklete és 37. jegyzőkönyve értelmében alkalmazandó az általános adatvédelmi rendelet.
- „Általános adatvédelmi rendelet”: a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet).
- „Charta”: az Európai Unió Alapjogi Chartája, HL C 326., 2012.10.26., 391–407. o.
- „EUB” vagy „Bíróság”: az Európai Unió Bírósága. Ez az Európai Unió igazságügyi hatósága, amely a tagállami bíróságokkal együttműködve biztosítja az uniós jog egységes alkalmazását és értelmezését.
- „Adatátadó”: az EGT-n belüli adatkezelő vagy adatfeldolgozó, aki személyes adatokat továbbít egy harmadik országbeli adatkezelő vagy adatfeldolgozó részére.
- „Adatátvevő”: a harmadik országbeli adatkezelő vagy adatfeldolgozó, aki fogadja az EGT-ből továbbított személyes adatokat, vagy hozzáférést kap azokhoz.
- „Az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz”: az általános adatvédelmi rendelet 46. cikke szerinti megfelelő garanciák, amelyeket az adatátadóknak be kell vezetniük a személyes adatok harmadik országba történő továbbításakor az általános adatvédelmi rendelet 45. cikkének (3) bekezdése szerinti megfelelőségi határozat hiányában. Az általános adatvédelmi rendelet 46. cikkének (2) és (3) bekezdése tartalmazza az általános adatvédelmi rendelet 46. cikke szerinti azon adattovábbítási eszközök felsorolását, amelyeket az adatkezelők és az adatfeldolgozók alkalmazhatnak.
- „SCC-k”: az Európai Bizottság által az EGT-n belüli adatkezelők vagy adatfeldolgozók és az EGT-n kívüli adatkezelők vagy adatfeldolgozók közötti személyesadat-továbbításra vonatkozóan elfogadott általános adatvédelmi kikötések (vagy „általános szerződési feltételek”). Az Európai Bizottság által elfogadott általános szerződési feltételek az általános adatvédelmi rendelet 46. cikke (2) bekezdésének c) pontja és (5) bekezdése értelmében az általános adatvédelmi rendelet szerinti adattovábbítási eszköznek minősülnek.

2. MELLÉKLET: PÉLDÁK TOVÁBBI INTÉZKEDÉSEKRE

69. Az alábbi intézkedések példák olyan további intézkedésekre, amelyeket a 4. lépés („Fogadjon el további intézkedéseket") során fontolóra vehet. Ez a felsorolás nem kimerítő. Ezen intézkedések közül egynek vagy többnek a kiválasztása és végrehajtása nem biztosítja feltétlenül és szisztematikusan, hogy az Ön által végzett adattovábbítás megfelel a lényegi azonosság uniós jogi követelményének. Azokat a további intézkedéseket kell kiválasztania, amelyek hatékonyan képesek biztosítani az ilyen védelmi szintet az Ön által végzett adattovábbítások tekintetében.

70. Bármely további intézkedés csak akkor és annyiban tekinthető hatékonynak az EUB „Schrems II" ítélete értelmében, ha és amennyiben orvosolja a harmadik országban fennálló jogi helyzet értékelése során feltárt konkrét hiányosságokat. Ha Ön végső soron nem tud lényegében azonos védelmi szintet biztosítani, nem továbbíthatja a személyes adatokat.

71. Előfordulhat, hogy adatkezelőként vagy adatfeldolgozóként Ön már köteles a jelen mellékletben ismertetett intézkedések némelyikének végrehajtására, még akkor is, ha az adatátvevő megfelelőségi határozat hatálya alá tartozik, csakúgy, mint ahogy köteles lehet ezen intézkedések végrehajtására az adatok EGT-n belüli kezelése során is.[66]

Technikai intézkedések

72. Ez a szakasz nem kimerítő jelleggel példákat mutat be olyan technikai intézkedésekre, amelyek kiegészíthetik az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközökben foglalt garanciákat a személyes adatok harmadik országba történő továbbításával összefüggésben az uniós jog által előírt védelmi szintnek való megfelelés biztosítása érdekében. Ezen intézkedésekre különösen akkor lesz szükség, ha az adott ország joga az adatátvevővel szemben olyan kötelezettségeket ír elő, amelyek ellentétesek az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök garanciáival, és amelyek megkérdőjelezhetik különösen az említett harmadik ország hatóságainak ezen adatokhoz való hozzáférésével szembeni lényegében azonos szintű védelem szerződéses garanciáját[67].

73. A fokozott egyértelműség érdekében ez a szakasz először azokat a technikai intézkedéseket határozza meg, amelyek bizonyos forgatókönyvekben/alkalmazási esetekben potenciálisan hatékonyak lehetnek a lényegében azonos védelmi szint biztosításában. A szakasz néhány olyan forgatókönyvvel/alkalmazási esettel folytatódik, amelyekben nem lehetett olyan technikai intézkedéseket találni, amelyek biztosítanák ezt a védelmi szintet.

Forgatókönyvek, amelyek tekintetében *hatékony* intézkedéseket lehetett találni

74. Az alábbiakban felsorolt intézkedések célja annak biztosítása, hogy a harmadik országbeli hatóságok továbbított adatokhoz való hozzáférése ne legyen hatással az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközökben foglalt megfelelő garanciák hatékonyságára. Ezek az intézkedések akkor is alkalmazandók, ha a hatóságok hozzáférése megfelel az adatátvevő országa jogának,

[66] Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 32. cikke.
[67] „Schrems II" ítélet (C-311/18), 135. pont.

amennyiben a hozzáférés meghaladja a demokratikus társadalomban szükséges és arányos mértéket[68]. Ezen intézkedések célja a potenciálisan jogsértő hozzáférés kizárása azáltal, hogy megakadályozzák a hatóságokat az érintettek azonosításában, a rájuk vonatkozó információk leszűrésében, más kontextusban való elkülönítésükben vagy a továbbított adatoknak az esetlegesen birtokukban lévő más olyan adatkészletekkel való összekapcsolásában, amelyek – egyéb adatok mellett – az érintettek által más kontextusban használt készülékek, alkalmazások, eszközök és protokollok által szolgáltatott online azonosítókat is tartalmazhatnak.

75. A harmadik országok hatóságai megpróbálhatnak hozzáférni a továbbított adatokhoz

a) a továbbítás során az adatoknak a fogadó országba történő továbbítására használt kommunikációs vonalakhoz való hozzáférés révén. Ez a hozzáférés lehet passzív, amely esetben a kommunikáció tartalmát – esetleg egy kiválasztási folyamatot követően – egyszerűen lemásolják. A hozzáférés azonban aktív is lehet abban az értelemben, hogy a hatóságok beavatkoznak a kommunikációs folyamatba azáltal, hogy nem csupán elolvassák a tartalmat, hanem manipulálják vagy törlik is annak egyes részeit.

b) Amikor az adatok a szándékolt címzettjük megőrzésében vannak, azáltal, hogy vagy magukhoz az adatkezelő berendezésekhez férnek hozzá, vagy megkövetelik az adatok valamelyik címzettjétől, hogy találja meg és nyerje ki az érdeklődésre számot tartó adatokat, majd adja át azokat a hatóságoknak.

76. Ez a szakasz azokat a forgatókönyveket vizsgálja, amelyekben mindkét esetben hatékony intézkedések alkalmazására kerül sor. A konkrét adattovábbítás adott körülményei között különböző további intézkedések lehetnek alkalmazhatók és megfelelőek, ha a fogadó ország joga csak egyfajta hozzáférést ír elő. Ezért az adatátadónak – az adatátvevő támogatásával – gondosan elemeznie kell az adatátvevőre vonatkozó kötelezettségeket.

Például az USC 50. címe 1881a. §-ának (a FISA 702. szakaszának) hatálya alá tartozó egyesült államokbeli adatátvevőket arra vonatkozó közvetlen kötelezettség terheli, hogy biztosítsanak hozzáférést az általuk birtokolt, megőrzött vagy ellenőrzött, átvett személyes adatokhoz, illetve adják át azokat. Ez az adatok érthetővé tételéhez szükséges kriptográfiai kulcsokra is kiterjedhet.

77. A forgatókönyvek ismertetik a konkrét körülményeket és a meghozott intézkedéseket. A forgatókönyvek bármilyen változása eltérő eredményekhez vezethet.

78. Előfordulhat, hogy az adatkezelőknek az adatátvevőre alkalmazandó jogszabályok által biztosított védelmi szinttől függetlenül alkalmazniuk kell az itt ismertetett intézkedések egy részét vagy mindegyikét, mert azok szükségesek ahhoz, hogy az adattovábbítás konkrét körülményei között megfeleljenek az általános adatvédelmi rendelet 25. és 32. cikkének. Más szóval előfordulhat, hogy az adatátadók kötelesek a jelen dokumentumban ismertetett intézkedések végrehajtására, még akkor is, ha az adatátvevők megfelelőségi határozat hatálya alá tartoznak, csakúgy, mint ahogy az adatkezelők és adatfeldolgozók kötelesek lehetnek ezen intézkedések végrehajtására az adatok EGT-n belüli kezelése során is.

[68] Lásd az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, az általános adatvédelmi rendelet 23. cikkének (1) bekezdését, valamint az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló ajánlását.

1. alkalmazási eset: Adattárolás biztonsági másolat készítése céljából és egyéb olyan célokból, amelyek nem teszik szükségessé a kódolatlan adatokhoz való hozzáférést

79. Az adatátadó harmadik országbeli tárhelyszolgáltatót vesz igénybe személyes adatok tárolására, például biztonsági másolat készítése céljából.

HA

1. a személyes adatokat továbbítás előtt erős titkosítás alkalmazásával kezelik,
2. a titkosítási algoritmus és annak paraméterezése (például a kulcs hossza, adott esetben működési módja) a lehető legkorszerűbb, és a fogadó ország hatóságai által végzett rejtjelelemzéssel szemben megbízhatónak tekinthető, figyelembe véve a rendelkezésükre álló erőforrásokat és műszaki lehetőségeket (például a próbálgatásos támadásokhoz szükséges számítástechnikai teljesítmény),
3. a titkosítás erőssége figyelembe veszi azt a konkrét időtartamot, amely alatt a titkosított személyes adatok titkosságát meg kell őrizni,
4. a titkosítási algoritmust hibátlanul hajtja végre egy megfelelően karbantartott szoftver, amelynek a választott algoritmus specifikációjának való megfelelését ellenőrizték, például tanúsítással,
5. a kulcsokat megbízhatóan kezelik (hozzák létre, adminisztrálják, – adott esetben – tárolják, kapcsolják össze egy szándékolt címzett személyazonosságával, és vonják vissza), valamint
6. a kulcsokat kizárólag az adatátadó vagy az e feladattal megbízott, az EGT-ben vagy olyan harmadik országban, illetve egy harmadik ország olyan területén letelepedett vagy egy harmadik ország olyan egy vagy több meghatározott ágazatában, illetve olyan nemzetközi szervezet keretében működő más szervezetek ellenőrzése mellett őrzik meg, amelynek tekintetében a Bizottság az általános adatvédelmi rendelet 45. cikkével összhangban megállapította, hogy biztosított a megfelelő védelmi szint,

AKKOR az Európai Adatvédelmi Testület véleménye szerint az elvégzett titkosítás hatékony további intézkedést jelent.

2. alkalmazási eset: Álnevesített adatok továbbítása

80. Az adatátadó először álnevesíti a birtokában lévő adatokat, majd elemzés, például kutatás céljából továbbítja azokat egy harmadik országba.

HA

1. az adatátadó olyan módon kezelt személyes adatokat továbbít, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, és a személyes adat nem használható fel arra, hogy az érintettet egy nagyobb csoporton belül elkülönítsék[69],
2. az említett további információkat kizárólag az adatátadó birtokolja, és azokat külön tárolják egy tagállamban vagy olyan harmadik országban, illetve egy harmadik ország olyan területén vagy egy harmadik ország olyan egy vagy több meghatározott ágazatában, illetve olyan nemzetközi

[69] Az általános adatvédelmi rendelet 4. cikkének 5. pontja értelmében: „»álnevesítés«: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni”.

szervezetnél, amelynek tekintetében a Bizottság az általános adatvédelmi rendelet 45. cikkével összhangban megállapította, hogy biztosított a megfelelő védelmi szint,

3. e további információk közlését vagy jogosulatlan felhasználását megfelelő technikai és szervezési garanciák révén megakadályozzák, és biztosított, hogy az adatátadó megtartja a kizárólagos ellenőrzést azon algoritmus vagy adattár felett, amely lehetővé teszi a további információk felhasználásával történő újbóli azonosítást, valamint
4. az adatkezelő a szóban forgó adatok alapos elemzésével, figyelembe véve minden olyan információt, amellyel a fogadó ország hatóságai rendelkezhetnek, megállapította, hogy az álnevesített személyes adatok akkor sem kapcsolhatók egy azonosított vagy azonosítható természetes személyekhez, ha azokat összevetik az említett információkkal,

AKKOR az Európai Adatvédelmi Testület véleménye szerint az elvégzett álnevesítés hatékony további intézkedést jelent.

81. Megjegyzendő, hogy számos esetben a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó tényezők, a természetes személy fizikai helye vagy egy internetalapú szolgáltatással való kapcsolata bizonyos időpontokban[70] lehetővé teheti az adott személy azonosítását még akkor is, ha nevét, címét vagy más egyszerű azonosítóját nem tüntetik fel.

82. Ez különösen igaz abban az esetben, ha az adatok információs szolgáltatások igénybevételére vonatkoznak (a hozzáférés időpontja, az igénybe vett funkciók sora, a használt eszköz jellemzői stb.). Ezek a szolgáltatások – a személyes adatok átvevőjéhez hasonlóan – adott esetben azon kötelezettség alatt állhatnak, hogy biztosítsanak hozzáférést a joghatóságuk szerinti hatóságok számára, amelyek így valószínűleg rendelkezni fognak az ezen információs szolgáltatásoknak az általuk megcélzott személy(ek) általi használatára vonatkozó adatokkal.

83. Ezenfelül, mivel egyes információs szolgáltatások használata e szolgáltatások jellegénél fogva nyilvános, vagy jelentős erőforrásokkal rendelkező felek kihasználhatják azokat, az adatkezelőknek különös gondossággal kell eljárniuk tekintettel arra, hogy a joghatóságuk szerinti hatóságok valószínűleg rendelkeznek az információs szolgáltatásoknak az általuk megcélzott személy általi használatára vonatkozó adatokkal.

3. alkalmazási eset: Harmadik országokon csupán áthaladó titkosított adatok

84. Az adatátadó az általános adatvédelmi rendelet 45. cikkével összhangban megfelelő védelmet nyújtó célállomásként elismert célállomásra kíván adatokat továbbítani. Az adatokat egy harmadik országon keresztül továbbítják.

HA

1. az adatátadó megfelelő védelmet biztosító joghatóság alá tartozó adatátvevőnek továbbít személyes adatokat, az adatokat az interneten keresztül továbbítják, és az adatok továbbítására adott esetben földrajzilag olyan harmadik országon keresztül is sor kerülhet, amely nem biztosít lényegében azonos védelmi szintet,

[70] Az általános adatvédelmi rendelet 4. cikkének 1. pontja értelmében: „»személyes adat«: azonosított vagy azonosítható természetes személyre (»érintett«) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható”.

2. olyan adattovábbítási titkosítást alkalmaznak, amelynek tekintetében biztosított, hogy az alkalmazott titkosítási protokollok a lehető legkorszerűbbek, és hatékony védelmet nyújtsanak a harmadik ország hatóságai számára ismerten rendelkezésre álló erőforrásokkal végrehajtott aktív és passzív támadásokkal szemben,
3. visszafejtésre csak a szóban forgó harmadik országon kívül van lehetőség,
4. a kommunikációban részt vevő felek megbízható, nyilvános kulcsú tanúsító hatóságról vagy infrastruktúráról állapodnak meg,
5. a titkosított adattovábbítás elleni aktív és passzív támadásokkal szemben konkrét védelmi és a technika állásának megfelelő intézkedéseket alkalmaznak,
6. amennyiben az adattovábbítás titkosítása önmagában nem nyújt megfelelő biztonságot a használt infrastruktúra vagy szoftver sebezhetőségével kapcsolatos tapasztalatok miatt, a személyes adatokat az alkalmazási rétegen végponttól végpontig terjedően is titkosítják a legkorszerűbb titkosítási módszerek alkalmazásával,
7. a titkosítási algoritmus és annak paraméterezése (például a kulcs hossza, adott esetben működési módja) a lehető legkorszerűbb, és a tranzitország hatóságai által végzett rejtjelelemzéssel szemben megbízhatónak tekinthető, figyelembe véve a rendelkezésükre álló erőforrásokat és műszaki lehetőségeket (például a próbálgatásos támadásokhoz szükséges számítástechnikai teljesítmény),
8. a titkosítás erőssége figyelembe veszi azt a konkrét időtartamot, amely alatt a titkosított személyes adatok titkosságát meg kell őrizni,
9. a titkosítási algoritmust hibátlanul hajtja végre egy megfelelően karbantartott szoftver, amelynek a választott algoritmus specifikációjának való megfelelését ellenőrizték, például tanúsítással,
10. kizárták a (hardverben vagy szoftverben elhelyezett) hátsó ajtók meglétét,
11. a kulcsokat megbízhatóan kezeli (hozza létre, adminisztrálja, – adott esetben – tárolja, kapcsolja össze a szándékolt címzett személyazonosságával, és vonja vissza) az adatátadó vagy egy, az adatátadó által megbízott, lényegében azonos védelmi szintet nyújtó joghatóság szerinti szervezet,

AKKOR az Európai Adatvédelmi Testület véleménye szerint az adattovábbítás titkosítása – szükség esetén a tartalom végponttól végpontig terjedő titkosításával együtt – hatékony további intézkedést jelent.

4. alkalmazási eset: Védett címzett

85. Az adatátadó személyes adatokat továbbít az ezen ország joga által kifejezetten védett harmadik országbeli adatátvevő részére például abból a célból, hogy közösen nyújtsanak egy betegnek orvosi ellátást vagy egy ügyfélnek jogi szolgáltatásokat.

HA

1. egy harmadik ország joga mentesíti az ezen ország illetőségével rendelkező adatátvevőt az e címzett birtokában lévő adatokhoz az adott célból való potenciálisan jogsértő hozzáférés alól, például az adatátvevőre vonatkozó szakmai titoktartási kötelezettség alapján,
2. ez a mentesség az adatátvevő birtokában lévő minden olyan információra kiterjed, amely felhasználható bizalmas információk védelmének megkerüléséhez (kriptográfiai kulcsok, jelszavak, egyéb hitelesítő adatok stb.),
3. az adatátvevő nem veszi igénybe adatfeldolgozó szolgáltatásait olyan módon, amely lehetővé teszi, hogy a hatóságok hozzáférjenek az adatfeldolgozó birtokában lévő adatokhoz, és az adatátvevő nem továbbítja az adatokat egy másik, az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök alapján nem védett jogalanynak sem,

4. a személyes adatokat a legkorszerűbb módszerrel titkosították a továbbítás előtt, biztosítva, hogy a visszafejtés ne legyen lehetséges a visszafejtő kulcs ismerete nélkül (végponttól végpontig terjedő titkosítás) az adatvédelem szükségességének teljes időtartama alatt,
5. a visszafejtő kulcs a védett adatátvevő kizárólagos megőrzésében van, és azt a legkorszerűbb technikai és szervezési intézkedésekkel megfelelően védik a jogosulatlan felhasználással vagy közléssel szemben, és
6. az adatátadó megbízhatóan megállapította, hogy az általa használni kívánt titkosítási kulcs megfelel a címzett birtokában lévő visszafejtő kulcsnak,

AKKOR az Európai Adatvédelmi Testület véleménye szerint az adattovábbítás elvégzett titkosítása hatékony további intézkedést jelent.

5. alkalmazási eset: Megosztott vagy többszereplős adatfeldolgozás

86. Az adatátadó azt szeretné, hogy a személyes adatokat két vagy több, különböző joghatóságok alá tartozó független adatfeldolgozó közösen dolgozza fel anélkül, hogy az adatok tartalmát közölné velük. Az adattovábbítás előtt olyan módon bontja fel az adatokat, hogy az egyes adatfeldolgozók által megkapott adatrészek önmagukban nem elegendőek a személyes adatok részben vagy egészben történő rekonstruálásához. Az adatátadó a feldolgozás eredményét minden egyes adatfeldolgozótól külön kapja meg, és a megkapott darabokat egyesíti a végső eredmény megállapítása érdekében, amely személyes vagy összesített adatnak minősülhet.

HA

1. az adatátadó olyan módon kezeli a személyes adatokat, hogy azokat két vagy több olyan részre bontja fel, amelyek egyike sem értelmezhető többé már, vagy amelyek egyike alapján sem állapítható meg többé már, hogy mely konkrét természetes személyre vonatkoznak, további információk felhasználása nélkül,
2. minden egyes darabot különböző joghatóságok alá tartozó, külön adatfeldolgozók részére továbbítanak,
3. az adatfeldolgozók opcionálisan közösen dolgozzák fel az adatokat, például biztonságos, többszereplős számítás alkalmazásával, olyan módon, hogy egyikükkel sem közölnek olyan információkat, amelyekkel a számítást megelőzően nem rendelkeznek,
4. a megosztott számításhoz használt algoritmus biztonságos az aktív fenyegetésekkel szemben,
5. nincs bizonyíték az egyes adatfeldolgozók letelepedési helye szerinti joghatóságok területén működő hatóságok közötti együttműködésre, amely lehetővé tenné számukra az adatfeldolgozók birtokában lévő valamennyi személyesadat-készlethez való hozzáférést és a személyes adatok tartalmának egyértelmű formában történő helyreállítását és felhasználását olyan körülmények között, amikor az ilyen felhasználás nem tartja tiszteletben az érintettek alapvető jogainak és szabadságainak lényeges tartalmát. Hasonlóképpen, egyik ország hatóságai sem rendelkezhetnek hatáskörrel arra, hogy hozzáférjenek az adatfeldolgozók birtokában lévő személyes adatokhoz az összes érintett joghatóság területén.
6. az adatkezelő a szóban forgó adatok alapos elemzésével, figyelembe véve minden olyan információt, amellyel a fogadó országok hatóságai rendelkezhetnek, megállapította, hogy az adatfeldolgozók részére általa továbbított személyesadat-darabok akkor sem kapcsolhatók egy azonosított vagy azonosítható természetes személyekhez, ha azokat összevetik az említett információkkal,

AKKOR az Európai Adatvédelmi Testület véleménye szerint az elvégzett megosztott adatfeldolgozás hatékony további intézkedést jelent.

Forgatókönyvek, amelyek tekintetében *nem* lehetett *hatékony* intézkedéseket találni

87. Az alábbiakban ismertetett intézkedések bizonyos forgatókönyvek esetében nem biztosítanák hatékonyan a harmadik országba továbbított adatok lényegében azonos szintű védelmét. Ezért azok nem minősülnének további intézkedéseknek.

6. alkalmazási eset: Adattovábbítás felhőszolgáltatók vagy más olyan adatfeldolgozók részére, akik hozzáférést igényelnek a kódolatlan adatokhoz

88. Az adatátadó felhőszolgáltatót vagy más adatfeldolgozót vesz igénybe ahhoz, hogy a személyes adatokat utasításainak megfelelően egy harmadik országban kezeljék.

HA

1. az adatkezelő adatokat továbbít egy felhőszolgáltató vagy más adatfeldolgozó részére,
2. a felhőszolgáltatónak vagy más adatfeldolgozónak a rábízott feladat végrehajtásához hozzá kell férnie a kódolatlan adatokhoz, és
3. a fogadó ország hatóságai számára a továbbított adatokhoz való hozzáférés tekintetében biztosított hatáskör meghaladja a demokratikus társadalomban szükséges és arányos mértéket,[71]

AKKOR az Európai Adatvédelmi Testület a technika állását figyelembe véve nem tud elképzelni olyan hatékony technikai intézkedést, amely megakadályozná, hogy a hozzáférés sértse az érintettek jogait. Az Európai Adatvédelmi Testület nem zárja ki, hogy a további technológiai fejlődés lehetővé tesz majd olyan intézkedéseket, amelyek a kódolatlan hozzáférés szükségessége nélkül érik el a kívánt üzleti célokat.

89. Az adott helyzetekben, amelyekben a nem titkosított személyes adatok technikailag szükségesek az adatfeldolgozó általi szolgáltatásnyújtáshoz, az adattovábbítás titkosítása és az inaktív adatok titkosítása még együttesen sem jelentenek olyan további intézkedést, amely biztosítja a lényegében azonos védelmi szintet, ha az adatátvevő rendelkezik a kriptográfiai kulcsokkal.

7. alkalmazási eset: Távoli hozzáférés az adatokhoz üzleti célokból

90. Az adatátadó személyes adatokat bocsát harmadik országbeli jogalanyok rendelkezésére közös üzleti célokra történő felhasználás céljából. Tipikus helyzet lehet, hogy egy tagállam területén letelepedett adatkezelő vagy adatfeldolgozó személyes adatokat továbbít egy olyan harmadik országbeli adatkezelő vagy adatfeldolgozó részére, amely ugyanahhoz a vállalkozáscsoporthoz vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportjához tartozik. Az adatátvevő felhasználhatja a kapott adatokat például arra, hogy az adatátadó számára olyan személyzeti szolgáltatásokat

[71] Lásd az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, az általános adatvédelmi rendelet 23. cikkének (1) bekezdését, valamint az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló ajánlását.

nyújtson, amelyekhez humánerőforrás-adatokra van szüksége, vagy arra, hogy telefonon vagy e-mailben kommunikáljon az adatátadó Európai Unióban élő ügyfeleivel.

HA

1. az adatátadó személyes adatokat továbbít egy harmadik országbeli adatátvevő részére ezen adatoknak egy közösen használt információs rendszerben olyan módon történő hozzáférhetővé tétele révén, amely lehetővé teszi az adatátvevő számára a saját választása szerinti adatokhoz való közvetlen hozzáférést, vagy ezen adatok hírközlési szolgáltatás igénybevételével közvetlenül, egyedileg vagy ömlesztve történő továbbítása révén,
2. az adatátvevő a kódolatlan adatokat saját céljaira használja fel,
3. a fogadó ország hatóságai számára a továbbított adatokhoz való hozzáférés tekintetében biztosított hatáskör meghaladja a demokratikus társadalomban szükséges és arányos mértéket,

AKKOR az Európai Adatvédelmi Testület nem tud elképzelni olyan hatékony technikai intézkedést, amely megakadályozná, hogy a hozzáférés sértse az érintettek jogait.

91. Az adott helyzetekben, amelyekben a nem titkosított személyes adatok technikailag szükségesek az adatfeldolgozó általi szolgáltatásnyújtáshoz, az adattovábbítás titkosítása és az inaktív adatok titkosítása még együttesen sem jelentenek olyan további intézkedést, amely biztosítja a lényegében azonos védelmi szintet, ha az adatátvevő rendelkezik a kriptográfiai kulcsokkal.

További szerződéses intézkedések

92. Ezek az intézkedések általában egyoldalú, kétoldalú vagy többoldalú[72] szerződéses kötelezettségvállalásokból állnak.[73] Az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz alkalmazása esetén az a legtöbb esetben már tartalmazza az adatátadó és az adatátvevő számos (többnyire szerződéses) kötelezettségvállalását, amelyek célja, hogy garanciaként szolgáljanak a személyes adatok tekintetében.[74]

93. Bizonyos helyzetekben ezek az intézkedések kiegészíthetik és megerősíthetik azokat a garanciákat, amelyeket az adattovábbítási eszköz és a harmadik ország vonatkozó jogszabályai nyújthatnak, amennyiben – figyelembe véve az adattovábbítás körülményeit – az említett garanciák nem felelnek meg az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szint biztosításához szükséges valamennyi feltételnek. Amennyiben a szerződéses intézkedések olyan jellegűek, hogy rendszerint nem kötelezhetik az adott harmadik ország hatóságait, ha ez utóbbiak nem szerződő felek[75], ezeket az intézkedéseket egyéb technikai és szervezési intézkedésekkel kell kombinálni a szükséges adatvédelmi szint biztosítása érdekében. Ezen intézkedések közül egynek vagy többnek a

[72] Például a BCR-eken belül, amelyeknek mindenképpen szabályozniuk kell az alább felsorolt intézkedések némelyikét.

[73] Ezek magánjellegűek, és a nemzetközi közjog értelmében nem tekinthetők nemzetközi megállapodásoknak. Ennek megfelelően rendszerint nem kötelezik a harmadik ország hatóságát mint a szerződésen kívüli felet, ha a szerződést harmadik országok magánfél szervezeteivel kötik meg, amint azt a Bíróság „Schrems II" ítéletének (C-311/18) 125. pontjában hangsúlyozta.

[74] Lásd a „Schrems II" ítélet (C-311/18) 137. pontját, amelyben a Bíróság végeredményben megállapította, hogy az általános szerződési feltételekről szóló határozatok *„olyan hatékony mechanizmusokat [tartalmaznak], amelyek a gyakorlatban lehetővé teszik annak biztosítását, hogy az uniós jog által megkövetelt védelmi szintet tiszteletben tartsák, és hogy a személyes adatok ilyen kikötéseken alapuló továbbítását az e kikötések megsértése, illetve tiszteletben tartásuk lehetetlensége esetén felfüggesszék vagy megtiltsák"*.

[75] „Schrems II" ítélet (C-311/18), 125. pont.

kiválasztása és végrehajtása nem biztosítja feltétlenül és szisztematikusan, hogy az Ön által végzett adattovábbítás megfelel a lényegi azonosság uniós jogi követelményének.

94. Attól függően, hogy milyen szerződéses intézkedések szerepelnek már az általános adatvédelmi rendelet 46. cikke szerinti, igénybe vett adattovábbítási eszközben, további szerződéses intézkedések is hasznosak lehetnek annak lehetővé tételében, hogy az EGT-beli adatátadók tudomást szerezzenek a harmadik országokba továbbított adatok védelmét érintő új fejleményekről.

95. A korábbiakban említetteknek megfelelően a szerződéses intézkedések nem képesek kizárni egy olyan harmadik ország jogszabályainak alkalmazását, amely nem felel meg az Európai Adatvédelmi Testület „alapvető európai garanciák" követelményének azokban az esetekben, amelyekben a jogszabályok arra kötelezik az adatátvevőket, hogy tegyenek eleget a hatóságoktól kapott, adatközlést elrendelő határozatoknak.[76]

96. A következőkben néhány példát sorolunk fel ezekre a lehetséges szerződéses intézkedésekre, és a jellegük szerint osztályozzuk azokat:

Meghatározott technikai intézkedések alkalmazására vonatkozó szerződéses kötelezettség előírása

97. ***Az adattovábbítások konkrét körülményeitől függően a szerződésnek adott esetben elő kell írnia, hogy az adattovábbítások megvalósulásához meghatározott technikai intézkedéseket kell hozni (lásd fent a javasolt technikai intézkedéseket).***

98. ***A hatékonyság feltételei:***

- E kikötés azokban a helyzetekben lehet hatékony, amelyekben az adatátadó megállapította a technikai intézkedések szükségességét. E kikötést jogi formában kell előírni annak biztosítása érdekében, hogy az adatátvevő is kötelezettséget vállal a szükséges technikai intézkedések szükség esetén történő bevezetésére.

Átláthatósági kötelezettségek:

99. ***Az adatátadó mellékleteket csatolhat a szerződéshez olyan információkkal, amelyeket az adatátvevő minden tőle telhetőt megtéve szolgáltat a hatóságok adatokhoz való hozzáféréséről, többek között a hírszerzés területén, feltéve, hogy a célország jogszabályai megfelelnek az Európai Adatvédelmi Testület alapvető európai garanciáinak. Ez segítheti az adatátadót abban, hogy eleget tegyen azon kötelezettségének, hogy dokumentálja a harmadik ország védelmi szintjére vonatkozó értékelését.***

100. Az adatátvevőt kötelezni lehet például arra, hogy:

(1) felsorolja a célországban az adatátvevőre vagy annak további adatfeldolgozóira alkalmazandó azon törvényeket és rendeleteket, amelyek lehetővé teszik a hatóságok számára az adattovábbítás tárgyát képező személyes adatokhoz való hozzáférést, különösen a hírszerzés, a bűnüldözés, valamint a továbbított adatokra vonatkozó közigazgatási és szabályozói felügyelet területén;

[76] Az EUB „Schrems II" ítélete (C-311/18), 132. pont.

(2) a hatóságok adatokhoz való hozzáférését szabályozó jogszabályok hiányában szolgáltasson az adatátvevő tapasztalatain vagy különböző forrásokból (például partnerek, nyílt források, nemzeti ítélkezési gyakorlat és felügyeleti szervek határozatai) származó jelentéseken alapuló információkat és statisztikákat a hatóságok személyes adatokhoz való hozzáféréséről a szóban forgó adattovábbításhoz hasonló helyzetekben (azaz az adott szabályozási területen; azon szervezetek típusa tekintetében, amelyekhez az adatátvevő tartozik;…)

(3) jelezze, hogy milyen intézkedéseket hoz a továbbított adatokhoz való hozzáférés megakadályozására (ha vannak ilyenek);

(4) nyújtson kellően részletes tájékoztatást a hatóságok személyes adatokhoz való hozzáférésre irányuló valamennyi olyan felhívásáról, amelyet az adatátvevő egy meghatározott időszak alatt[77] kapott, különösen a fenti (1) pontban említett területeken, beleértve a beérkezett felhívásokra, a kért adatokra, a megkereső szervre és a közlés jogalapjára, valamint az arra vonatkozó tájékoztatást is, hogy az adatátvevő milyen mértékben közölte a kért adatokat;[78]

(5) adja meg, hogy az adatátvevő számára tiltja-e a jog, és ha igen, milyen mértékben, a fenti (1)–(5) pontban említett információk szolgáltatását.

101. Ezt a tájékoztatást strukturált kérdőívek formájában lehetne megadni, amelyeket az adatátvevő kitöltene és aláírna, és amelyeket kiegészítene az adatátvevő azon szerződéses kötelezettsége, hogy meghatározott időn belül jelentse be az ezen információkban bekövetkező esetleges változásokat, ahogyan ez az átvilágítási folyamatok esetében jelenleg is történik.

102. ***A hatékonyság feltételei:***

- Az adatátvevőnek képesnek kell lennie arra, hogy legjobb tudomása szerint az adatátadó rendelkezésére bocsássa ezeket az információkat, miután minden tőle telhetőt megtett azok megszerzése érdekében.[79]

- Ez az adatátvevőre rótt kötelezettség annak biztosítására szolgál, hogy az adatátadó tudomást szerezzen a harmadik országba történő adattovábbítással járó kockázatokról, és folyamatosan tudatában legyen azoknak. Így lehetővé teszi az adatátadó számára, hogy tartózkodjon a szerződés megkötésétől, vagy ha az információ a szerződés megkötését követően megváltozik, teljesítse az adattovábbítás felfüggesztésére és/vagy a szerződéstől való elállásra vonatkozó kötelezettségét, amennyiben a harmadik ország joga, az általános adatvédelmi rendelet 46. cikke szerinti, igénybe vett adattovábbítási eszközben foglalt garanciák és az általa esetlegesen elfogadott további garanciák már nem képesek az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítani. Ez a kötelezettség azonban nem igazolhatja a személyes adatok adatátvevő általi közlését, és nem keltheti azt az elvárást sem, hogy nem lesznek további hozzáférésre irányuló felhívások.

***

[77] Az időszak hosszának az azon érintettek jogait és szabadságait érintő kockázattól kell függenie, akiknek adatai a szóban forgó adattovábbítás tárgyát képezik – például az adatátadási eszköz adatátadóval való lezárását megelőző utolsó év.

[78] E kötelezettség teljesítése önmagában nem jelenti a megfelelő védelmi szint biztosítását. Ugyanakkor minden olyan nem megfelelő közlés, amelyre ténylegesen sor került, további intézkedések végrehajtását teszi szükségessé.

[79] Lásd a fenti 32. pont (5) alpontját.

103. ***Az adatátadó olyan kikötéseket is beilleszthet, amelyekkel az adatátvevő tanúsítja, hogy (1) nem hozott létre szándékosan olyan hátsó ajtókat vagy hasonló programozást, amely felhasználható lenne a rendszerhez és/vagy a személyes adatokhoz való hozzáféréshez, (2) nem hozta létre vagy változtatta meg szándékosan üzleti folyamatait olyan módon, amely megkönnyíti a személyes adatokhoz vagy rendszerekhez való hozzáférést, valamint (3) hogy a nemzeti jog vagy a kormányzati politika nem követeli meg az adatátvevőtől, hogy hátsó ajtókat hozzon létre vagy tartson fenn, vagy megkönnyítse a személyes adatokhoz vagy rendszerekhez való hozzáférést, vagy hogy az adatátvevő birtokában legyen a titkosítási kulcs, vagy adja át azt.***[80]

104. ***A hatékonyság feltételei:***

- Olyan jogszabályok vagy kormányzati politikák megléte, amelyek megakadályozzák, hogy az adatátvevők közöljék ezeket az információkat, hatástalanná teheti ezt a kikötést. Az adatátvevő így nem kötheti meg a szerződést, vagy értesítenie kell az adatátadót arról, hogy nem tudja tovább teljesíteni szerződéses kötelezettségeit.[81]
- A szerződésnek szankciókat és/vagy az adatátadó azon lehetőségét is tartalmaznia kell, hogy rövid határidővel elálljon a szerződéstől azokban az esetekben, amikor az adatátvevő nem fedi fel egy hátsó ajtó vagy hasonló programozás vagy manipulált üzleti folyamatok vagy az ezek bármelyikének végrehajtására vonatkozó követelmény meglétét, vagy nem tájékoztatja haladéktalanul az adatátadót, amint ezek megléte a tudomására jut.

***

105. ***Az adatátadó megerősítheti arra vonatkozó lehetőségét, hogy a helyszínen és/vagy távolról ellenőrizze[82] vagy megvizsgálja az adatátvevő adatfeldolgozó berendezéseit annak megállapítása érdekében, hogy az adatokat közölték-e a hatóságokkal, és ha igen, milyen feltételek mellett (a hozzáférés nem haladhatja meg a demokratikus társadalomban szükséges és arányos mértéket), például az ellenőrző testületek gyors beavatkozását biztosító rövid határidő és mechanizmusok előírásával, valamint az adatátadó ellenőrző testületek kiválasztásával kapcsolatos autonómiájának megerősítésével.***

106. ***A hatékonyság feltételei:***

- Ahhoz, hogy teljes mértékben hatékony legyen, az ellenőrzésnek jogilag és technikailag ki kell terjednie a harmadik országba továbbított személyes adatoknak az adatátvevő adatfeldolgozói vagy további adatfeldolgozói által történő minden feldolgozására.
- A hozzáférési naplóknak és más hasonló nyomoknak hamisíthatatlannak kell lenniük, hogy az ellenőrök bizonyítékot találhassanak a közlésre. A hozzáférési naplóknak és más hasonló nyomoknak különbséget kell tenniük a szokásos üzleti tevékenységeken alapuló hozzáférések és a hozzáférést elrendelő határozatokon vagy hozzáférésre irányuló felhívásokon alapuló hozzáférések között is.

[80] Ez a kikötés fontos a továbbított személyes adatok megfelelő szintű védelmének biztosításához, és azt általában elő kell írni.

[81] Lásd a fenti 32. pont (5) alpontját.

[82] Lásd például az adatkezelők és adatfeldolgozók közötti általános szerződési feltételekről szóló 2010/87/EU határozat 5. általános szerződési feltételének f) pontját, az ellenőrzések magatartási kódex keretében vagy tanúsítás útján is előírhatók.

***

107. ***Ha az adatátvevő harmadik országának jogát és gyakorlatát kezdetben értékelték, és úgy ítélték meg, hogy az az adatátadó által továbbított adatok tekintetében biztosítja az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet, és az adatátadó még mindig megerősítheti az adatátvevő azon kötelezettségét, hogy haladéktalanul tájékoztassa az adatátadót arról, hogy nem képes megfelelni a szerződéses kötelezettségvállalásoknak és ennélfogva a „lényegében azonos adatvédelmi szint" követelményének.[83]..***

108. Ez a megfelelésre való képtelenség a harmadik ország jogszabályaiban vagy gyakorlatában bekövetkezett változások következménye lehet.[84] A kikötések konkrét és szigorú határidőket és eljárásokat állapíthatnak meg az adattovábbítás gyors felfüggesztésére és/vagy a szerződéstől való elállásra, valamint a kapott adatok adatátvevő általi visszaszolgáltatására vagy törlésére. A beérkezett felhívások, azok hatálya és az ellenük hozott intézkedések hatékonysága nyomon követésének elegendő támpontot kell szolgáltatnia az adatátadó számára ahhoz, hogy eleget tegyen az adattovábbítás felfüggesztésére vagy megszüntetésére és/vagy a szerződéstől való elállásra vonatkozó kötelezettségének.

109. ***A hatékonyság feltételei:***

- Az értesítésnek az adatokhoz való hozzáférés engedélyezése előtt kell megtörténnie. Ellenkező esetben előfordulhat, hogy mire az adatátadó megkapja az értesítést, már megsértették az egyén jogait, ha a felhívás az adott harmadik ország olyan jogszabályain alapul, amelyek túllépnek az uniós jog által biztosított adatvédelmi szint által nyújtott lehetőségeken. Az értesítés továbbra is szolgálhatja a jövőbeli jogsértések megelőzését és annak lehetővé tételét, hogy az adatátadó eleget tegyen a személyes adatok harmadik országba történő továbbításának felfüggesztésére és/vagy a szerződéstől való elállásra vonatkozó kötelezettségének.
- Az adatátvevőnek figyelemmel kell kísérnie minden olyan jogi vagy politikai fejleményt, amely azzal járhat, hogy nem képes megfelelni kötelezettségeinek, és haladéktalanul tájékoztatnia kell az adatátadót minden ilyen változásról és fejleményről, lehetőség szerint még azok végrehajtása előtt, hogy az adatátadó visszaszerezhesse az adatokat az adatátvevőtől.
- A kikötéseknek rendelkezniük kell egy gyors mechanizmusról, amelynek keretében az adatátadó engedélyezi az adatátvevő számára, hogy azonnal biztonságba helyezze vagy visszaszolgáltassa az adatokat az adatátadónak, vagy ha ez nem lehetséges, törölje vagy biztonságosan titkosítsa az adatokat anélkül, hogy feltétlenül meg kellene várnia az adatátadó utasításait, amennyiben az adatátadó és az adatátvevő által közösen megállapítandó konkrét küszöbérték teljesül. Az adatátvevőnek ezt a mechanizmust az adattovábbítás kezdetétől fogva

[83] Az általános szerződési feltételekről szóló 2010/87/EU határozat 5. általános szerződési feltételének a) pontja és d) pontjának i. alpontja.

[84] Lásd a „Schrems II" ítélet (C-311/18) 139. pontját, amelyben a Bíróság megállapítja, hogy *„bár [az] 5. általános szerződési feltétel d) pontjának i. alpontja lehetővé teszi a személyes adatok továbbításának címzettje számára, hogy az őt védő olyan jogszabály esetén, mint például egy bűnügyi nyomozás titkosságának megőrzése érdekében fennálló büntetőjogi tilalom, ne közölje az Unióban letelepedett adatkezelővel a személyes adatok közlésére irányuló, a bűnüldöző szervek jogilag kötelező erejű felhívását, az [általános szerződési feltételekről szóló határozat] melléklete 5. általános szerződési feltétele a) pontjának megfelelően azonban köteles tájékoztatni az adatkezelőt arról, hogy nem képes eleget tenni az általános szerződési feltételeknek"*.

alkalmaznia kell, és rendszeresen tesztelnie kell azt annak biztosítása érdekében, hogy rövid időn belül alkalmazható legyen.

- Egyéb kikötések lehetővé tehetik az adatátadó számára, hogy ellenőrzések, vizsgálatok és egyéb ellenőrző intézkedések útján figyelemmel kísérje, hogy az adatátvevő eleget tesz-e ezeknek a kötelezettségeknek, és az adatátvevővel szemben kiszabott szankciók és/vagy az adatátadó azon lehetősége útján érvényesítse azokat, hogy felfüggeszthetti az adattovábbítást és/vagy azonnali hatállyal elállhat a szerződéstől.

***

110. ***Amennyiben azt a harmadik ország nemzeti joga lehetővé teszi, a szerződés megerősítheti az adatátvevő átláthatósági kötelezettségeit egy olyan „Warrant Canary" („kanári engedély" – hozzáférést elrendelő végzésre vonatkozó figyelmeztetés) módszer előírásával, amellyel az adatátvevő kötelezettséget vállal arra, hogy rendszeresen (például legalább 24 óránként) kriptográfiailag aláírt üzenetet tesz közzé, amelyben tájékoztatja az adatátadót arról, hogy egy bizonyos naptól és időponttól kezdve nem kapott személyes adatok közlését elrendelő vagy ehhez hasonló határozatot. Az értesítés frissítésének elmaradása azt jelzi az adatátadó számára, hogy az adatátvevő adott esetben határozatot kapott.***

111. ***A hatékonyság feltételei:***

- A harmadik ország szabályozásának lehetővé kell tennie az adatátvevő számára, hogy kiadja ezt a fajta passzív értesítést az adatátadó felé.
- Az adatátadónak automatikusan figyelemmel kell kísérnie a „Warrant Canary" értesítéseket.
- Az adatátvevőnek biztosítania kell, hogy a „Warrant Canary" aláírásához szükséges titkos kulcsa biztonságban legyen, és hogy a harmadik ország szabályozása alapján ne legyen hamis „Warrant Canary"-k kiadására kényszeríthető. E célból hasznos lehet, ha különböző személyek részéről több aláírásra van szükség, és/vagy ha a „Warrant Canary"-t a harmadik ország joghatóságán kívül eső személy adja ki.

Konkrét intézkedések meghozatalára vonatkozó kötelezettségek

112. ***Az adatátvevő kötelezettséget vállalhat arra, hogy a célország joga szerint felülvizsgálja az adatok közlését elrendelő bármely határozat jogszerűségét, különösen azt, hogy annak elrendelésére az azt elrendelő hatóság hatáskörének keretei között került-e sor, és hogy megtámadja a határozatot, ha alapos vizsgálatot követően arra a következtetésre jut, hogy a célország joga alapján ez indokolt. A határozat megtámadásakor az adatátvevőnek ideiglenes intézkedések elrendelését kell kérnie a határozat joghatásainak felfüggesztéséhez mindaddig, amíg a bíróság érdemi döntést nem hoz. Az adatátvevő köteles lenne arra, hogy a kért személyes adatokat mindaddig ne közölje, amíg az alkalmazandó eljárási szabályok alapján nem köteles erre. Az adatátvevő kötelezettséget vállalna arra is, hogy a határozat észszerű értelmezése alapján a határozatra válaszul rendelkezésre bocsátja a megengedett minimális mennyiségű információt.***

113. ***A hatékonyság feltételei:***

- A harmadik ország jogrendjének hatékony jogi lehetőségeket kell biztosítania az adatközlést elrendelő határozatok megtámadására.

- Ez a kikötés minden esetben rendkívül korlátozott kiegészítő védelmet nyújt, mivel az adatközlést elrendelő határozat jogszerű lehet a harmadik ország jogrendje szerint, de ez a jogrend nem feltétlenül felel meg az uniós követelményeknek. E szerződéses intézkedésnek szükségszerűen kiegészítő jellegűnek kell lennie egyéb további intézkedésekhez képest.
- A határozatok megtámadásának halasztó hatályúnak kell lennie a harmadik ország joga szerint. Ellenkező esetben a hatóságok továbbra is hozzáférhetnének az egyének adataihoz, és az ezt követően az egyén javára indított bármely kereset azzal a korlátozott hatással járna, hogy lehetővé tenné az egyén számára, hogy kártérítést követeljen az adatközlésből eredő negatív következményekért.
- Az adatátvevőnek képesnek kell lennie arra, hogy az adatátadó felé dokumentálja és igazolja azokat az intézkedéseket, amelyeket e kötelezettségvállalás teljesítése érdekében minden tőle telhetőt megtéve megtett.

***

114. ***A fent ismertetett helyzetben az adatátvevő kötelezettséget vállalhat arra, hogy tájékoztatja az elrendelő hatóságot a határozatnak az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt garanciákkal[85] való összeegyeztethetetlenségéről, valamint az adatátvevő kötelezettségeinek ebből eredő összeütközéséről. Az adatátvevő egyidejűleg és a lehető leghamarabb értesíti az adatátadót és/vagy az EGT illetékes felügyeleti hatóságát, amennyiben ezt a harmadik ország jogrendje lehetővé teszi.***

115. ***A hatékonyság feltételei:***

- Az uniós jog által biztosított védelemre és a kötelezettségek összeütközésére vonatkozó ilyen tájékoztatásnak bizonyos joghatással kell járnia a harmadik ország jogrendjében, például a hozzáférést elrendelő határozat vagy a hozzáférésre irányuló felhívás bírósági vagy közigazgatási felülvizsgálatával, a bírói engedély követelményével és/vagy a határozat végrehajtásának ideiglenes felfüggesztésével az adatok bizonyos fokú védelemmel való ellátása érdekében.
- Az ország jogrendszere nem akadályozhatja meg az adatátvevőt abban, hogy a kapott, hozzáférést elrendelő határozatról vagy hozzáférésre irányuló felhívásról értesítse az adatátadót vagy legalább az EGT illetékes felügyeleti hatóságát.
- Az adatátvevőnek képesnek kell lennie arra, hogy az adatátadó felé dokumentálja és igazolja azokat az intézkedéseket, amelyeket e kötelezettségvállalás teljesítése érdekében minden tőle telhetőt megtéve megtett.

[85] Az általános szerződési feltételek például úgy rendelkeznek, hogy az adatok feldolgozása, ideértve azok továbbítását is, megfelelt és továbbra is megfelel *„az alkalmazandó adatvédelmi jognak”*. Fogalommeghatározása szerint e jog *„az egyének alapvető jogaik és szabadságjogaik, különösen – a személyes adatok feldolgozásával kapcsolatban – a magánélet tiszteletben tartásához való jogaik védelméről szóló, az adatátadó letelepedési helye szerinti tagállamban tevékenykedő adatkezelőre vonatkozó jogszabály[t]”* jelenti. Az EUB megerősíti, hogy az általános adatvédelmi rendeletnek az Európai Unió Alapjogi Chartájával összefüggésben értelmezett rendelkezései e jogszabályok részét képezik; lásd: az EUB „Schrems II” ítélete (C-311/18), 138. pont.

Az érintettek képessé tétele jogaik gyakorlására

116. ***A szerződés előírhatja, hogy a rendes üzletvitel során (beleértve a támogatási eseteket is) egyszerű szövegként továbbított személyes adatokhoz csak az adatátadó és/vagy az érintett kifejezett vagy hallgatólagos hozzájárulásával lehet hozzáférni.***

117. ***A hatékonyság feltételei:***

- E kikötés azokban a helyzetekben lehet hatékony, amelyekben az adatátvevők a hatóságoktól önkéntes alapon történő együttműködésre irányuló felhívásokat kapnak, szemben például a hatóságok adatokhoz való olyan hozzáférésével, amelyre az adatátvevő tudtán kívül vagy akarata ellenére kerül sor.
- Bizonyos helyzetekben előfordulhat, hogy az érintett nincs abban a helyzetben, hogy ellenezze a hozzáférést, vagy olyan hozzájárulást adjon, amely megfelel az uniós jogban meghatározott valamennyi feltételnek (önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű) (például a munkavállalók esetében)[86].
- Azok a nemzeti szabályozások vagy politikák, amelyek arra kötelezik az adatátvevőt, hogy ne közölje a hozzáférést elrendelő határozatot, hatástalanná tehetik ezt a kikötést, kivéve, ha azt olyan technikai módszerekkel lehet megtámogatni, amelyek szükségessé teszik az adatátadó vagy az érintett beavatkozását ahhoz, hogy az egyszerű szöveges adatok hozzáférhetők legyenek. A hozzáférés korlátozására irányuló ilyen technikai intézkedések különösen akkor irányozhatók elő, ha a hozzáférés csak meghatározott támogatási vagy szolgáltatási esetekben engedélyezett, de magát az adatot az EGT-ben tárolják.

***

118. ***A szerződés arra kötelezheti az adatátvevőt és/vagy az adatátadót, hogy haladéktalanul értesítse az érintettet a harmadik ország hatóságaitól kapott felhívásról vagy határozatról, vagy arról, hogy az adatátvevő nem képes megfelelni a szerződéses kötelezettségvállalásoknak, hogy lehetővé tegyék az érintett számára az információszerzést és a hatékony jogorvoslatot (például azáltal, hogy eljárást indít az illetékes felügyeleti hatóságnál és/vagy igazságügyi hatóságnál, és igazolja a harmadik ország bíróságai előtti kereshetőségi jogát).***

119. ***A hatékonyság feltételei:***

- Ez az értesítés felhívhatja az érintett figyelmét arra, hogy harmadik országok hatóságai esetleg hozzáférhetnek az adataihoz. Az így lehetővé teheti az érintett számára, hogy további információkat kérjen az adatátadóktól, és eljárást indítson az illetékes felügyeleti hatóságnál. Ez a kikötés azon nehézségek némelyikére is megoldást jelenthet, amelyekkel az egyén akkor szembesülhet, ha igazolnia kell harmadik országok bíróságai előtti kereshetőségi jogát *(locus standi)* az adataihoz való hatósági hozzáférés megtámadásához.
- A nemzeti szabályozások és politikák megakadályozhatják az érintett ilyen értesítését. Az adatátadó és az adatátvevő mindazonáltal kötelezettséget vállalhat arra, hogy az adatközlésre vonatkozó korlátozások feloldását követően haladéktalanul tájékoztatja az érintettet, és minden tőle telhetőt megtesz a közlési tilalom alóli mentesség megszerzése érdekében. Az adatátadó vagy az illetékes felügyeleti hatóság értesítheti az érintettet legalább személyes

[86] Az általános adatvédelmi rendelet 4. cikkének 11. pontja.

adatai továbbításának azon okból történő felfüggesztéséről vagy megszüntetéséről, hogy a hozzáférésre irányuló felhívás miatt az adatátvevő nem képes megfelelni szerződéses kötelezettségvállalásainak.

***

120. ***A szerződés arra kötelezheti az adatátadót és az adatátvevőt, hogy ad hoc jogorvoslati mechanizmusok és jogi tanácsadás révén segítse az érintettet jogainak a harmadik ország joghatósága alatt történő gyakorlásában.***

121. ***A hatékonyság feltételei***

- A nemzeti szabályozások és politikák olyan feltételeket írhatnak elő, amelyek alááshatják az előírt ad hoc jogorvoslati mechanizmusok hatékonyságát.
- A jogi tanácsadás hasznos lehet az érintett számára, különös tekintettel arra, hogy mennyire bonyolult és költséges lehet az érintett számára, hogy megértse egy harmadik ország jogrendszerét, és hogy külföldről – adott esetben idegen nyelven – tegyen jogi lépéseket. Ez a kikötés mindazonáltal minden esetben korlátozott kiegészítő védelmet fog nyújtani, mivel az érintettek számára nyújtott segítség és jogi tanácsadás önmagában nem orvosolhatja azt, hogy egy harmadik ország jogrendje nem biztosít az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet. E szerződéses intézkedésnek szükségszerűen kiegészítő jellegűnek kell lennie egyéb további intézkedésekhez képest.

Ez a további intézkedés csak akkor lenne hatékony, ha a harmadik ország joga jogorvoslatot biztosít a nemzeti bíróságok előtt, vagy ha létezik egy ad hoc jogorvoslati mechanizmus. Jogorvoslati mechanizmus hiányában mindenesetre ez nem jelentene hatékony további intézkedést a megfigyelési intézkedésekkel szemben.

Szervezési intézkedések

122. További szervezési intézkedések lehetnek azok a belső politikák, szervezési módszerek és szabványok, amelyeket az adatkezelők és adatfeldolgozók magukra is alkalmazhatnak, és az adatok harmadik országbeli átvevőire is kötelezővé tehetnek. Ezen intézkedések az adatkezelés teljes folyamata során hozzájárulhatnak a személyes adatok védelme következetességének biztosításához. A szervezési intézkedések javíthatják az adatátadók tudatosságát is az adatokhoz való harmadik országbeli hozzáférés kockázatát és a hozzáférésre irányuló kísérleteket illetően, valamint az ezekre való reagálási képességüket. Ezen intézkedések közül egynek vagy többnek a kiválasztása és végrehajtása nem biztosítja feltétlenül és szisztematikusan, hogy az Ön által végzett adattovábbítás megfelel a lényegi azonosság uniós jogi követelményének. Az adattovábbítás konkrét körülményeitől és a harmadik ország jogszabályaira vonatkozóan elvégzett értékeléstől függően szervezési intézkedésekre van szükség a szerződéses és/vagy technikai intézkedések kiegészítése érdekében, biztosítandó, hogy a személyes adatok védelmének szintje lényegében azonos legyen az Európai Unióban biztosított védelmi szinttel.

123. A legmegfelelőbb intézkedések értékelését eseti alapon kell elvégezni, szem előtt tartva, hogy az adatkezelőknek és adatfeldolgozóknak tiszteletben kell tartaniuk az elszámoltathatóság elvét. Az alábbiakban az Európai Adatvédelmi Testület felsorol néhány példát olyan szervezési intézkedésekre, amelyeket az adatátadók végrehajthatnak, jóllehet a felsorolás nem kimerítő, és más intézkedések szintén megfelelőek lehetnek:

Az adattovábbítások irányítására vonatkozó belső politikák, különösen a vállalkozáscsoportokkal összefüggésben

124. ***Megfelelő belső politikák elfogadása az adattovábbítással kapcsolatos feladatok egyértelmű megosztásával, bejelentési csatornákkal és eljárási standardokkal a hatóságok adatokhoz való hozzáférésre irányuló, fedett vagy hivatalos felhívásainak eseteire. Különösen a vállalkozáscsoportok közötti adattovábbítások esetében ezek a politikák magukban foglalhatják többek között egy EGT-n belüli, az informatikai, adatvédelmi és a magánélet védelmére vonatkozó jogszabályok szakértőiből álló külön munkacsoport kijelölését az Európai Unióból továbbított személyes adatokat érintő felhívások kezelésére; a jogi és vállalati felső vezetés, valamint az adatátadó értesítését az ilyen felhívások kézhezvételekor; az aránytalan vagy jogellenes felhívások megtámadására irányuló eljárási lépéseket és az érintettek átlátható tájékoztatásának előírását.***

125. Speciális képzési eljárások kidolgozása a személyes adatokhoz való hozzáférésre irányuló hatósági felhívások kezelésével megbízott személyzet számára, amelyeket rendszeres időközönként naprakésszé kell tenni, hogy tükrözzék a harmadik országban és az EGT-ben bekövetkezett új jogalkotási és igazságszolgáltatási fejleményeket. A képzési eljárásoknak magukban kell foglalniuk a hatóságok személyes adatokhoz való hozzáférésére vonatkozó – különösen az Alapjogi Charta 52. cikkének (1) bekezdéséből eredő – uniós jogi követelményeket. Fokozni kell a személyzet tudatosságát különösen az adatokhoz való hozzáférésre irányuló hatósági felhívásokra vonatkozó gyakorlati példák értékelése, valamint az Alapjogi Charta 52. cikkének (1) bekezdéséből eredő követelménynek az ilyen gyakorlati példákra való alkalmazása révén. Az ilyen képzésnek figyelembe kell vennie az adatátvevő sajátos helyzetét, például a harmadik ország azon törvényeit és rendeleteit, amelyeknek az adatátvevő a hatálya alá tartozik, és azt lehetőség szerint az adatátadóval együttműködve kell kidolgozni.

126. ***A hatékonyság feltételei:***

- Ezek a politikák csak azokra az esetekre irányozhatók elő, amelyekben a harmadik ország hatóságainak felhívása összeegyeztethető az uniós joggal.[87] Ha a felhívás összeegyeztethetetlen, ezek a politikák nem elegendőek a személyes adatok azonos szintű védelmének biztosításához, és – a fent említetteknek megfelelően – az adattovábbításokat meg kell szüntetni, vagy megfelelő további intézkedéseket kell hozni a hozzáférés elkerülése érdekében.

Átláthatósági és elszámoltathatósági intézkedések

127. ***Dokumentálja és vegye nyilvántartásba a hatóságoktól kapott, hozzáférésre irányuló felhívásokat és az azokra adott választ, a jogi indoklással és az érintett szereplőkkel együtt (például ha az adatátadót értesítették, és az adatátadó válaszát, az ilyen felhívások kezeléséért felelős munkacsoport értékelését stb.). Ezeket a nyilvántartásokat az adatátadó rendelkezésére kell bocsátani, aki szükség esetén átadja azokat az érintetteknek.***

128. ***A hatékonyság feltételei:***

- A harmadik ország nemzeti jogszabályai megakadályozhatják a felhívások vagy az azokra vonatkozó lényeges információk közlését, és így hatástalanná tehetik ezt a gyakorlatot. Az adatátvevőnek tájékoztatnia kell az adatátadót arról, hogy nem képes ilyen dokumentumokat

[87] Lásd: „Schrems I” ítélet (C-362/14), 94. pont; „Schrems II” ítélet (C-311/18), 168., 174., 175. és 176. pont.

és nyilvántartásokat rendelkezésre bocsátani, ezáltal lehetőséget biztosítva az adatátadónak arra, hogy felfüggessze az adattovábbításokat, amennyiben az információszolgáltatási képesség e hiánya a védelmi szint csökkenéséhez vezetne.

***

129. ***Átláthatósági jelentések vagy összefoglalók rendszeres közzététele az adatokhoz való hozzáférésre irányuló kormányzati felhívásokról és a válasz fajtájáról, amennyiben a helyi jog lehetővé teszi a közzétételt.***

130. ***A hatékonyság feltételei:***

- A tájékoztatásnak relevánsnak, egyértelműnek és a lehető legrészletesebbnek kell lennie. A harmadik ország nemzeti jogszabályai megakadályozhatják részletes információk közlését. Ezekben az esetekben az adatátvevőnek minden tőle telhetőt meg kell tennie annak érdekében, hogy statisztikai információkat vagy hasonló típusú összesített információkat tegyen közzé.

Szervezési módszerek és adattakarékossági intézkedések

131. ***Az elszámoltathatóság elve alapján már fennálló szervezési követelmények, mint például szigorú és részletes adathozzáférési és titoktartási politikáknak, valamint bevált módszereknek a szükséges ismeret szigorú elvén alapuló elfogadása, amelyeket rendszeres ellenőrzésekkel követnek nyomon, és fegyelmi intézkedésekkel kényszerítenek ki, szintén hasznos intézkedés lehet az adattovábbítással összefüggésben. E tekintetben mérlegelni kell az adattakarékosságot annak érdekében, hogy korlátozni lehessen a személyes adatok jogosulatlan hozzáférésnek való kitettségét. Egyes esetekben például előfordulhat, hogy nem szükséges továbbítani bizonyos adatokat (például – többek között támogatási esetekben – az EGT-ben található adatokhoz való távoli hozzáférés esetében, amikor a teljes körű hozzáférés helyett korlátozott hozzáférés biztosítására kerül sor; vagy ha a szolgáltatásnyújtás csak korlátozott mennyiségű adat, nem pedig a teljes adatbázis továbbítását teszi szükségessé).***

132. ***A hatékonyság feltételei:***

- Az adattovábbítással összefüggésben is rendszeres ellenőrzéseket és szigorú fegyelmi intézkedéseket kell bevezetni az adattakarékossági intézkedéseknek való megfelelés nyomon követése és kikényszerítése érdekében.
- Az adatátadónak az adattovábbítást megelőzően el kell végeznie a birtokában lévő személyes adatok értékelését azon adatkészletek azonosítása érdekében, amelyek nem szükségesek az adattovábbításhoz, és amelyeket ezért nem oszt meg az adatátvevővel.
- Az adattakarékossági intézkedéseket olyan technikai intézkedéseknek kell kísérniük, amelyek biztosítják, hogy az adatokhoz ne lehessen jogosulatlanul hozzáférni. A biztonságos többszereplős számítási mechanizmusok végrehajtása és a titkosított adatkészletek különböző megbízható szervezetek közötti terjesztése például beépített módon megakadályozhatja, hogy bármely egyoldalú hozzáférés azonosítható adatok közléséhez vezessen.

***

133. ***Bevált módszerek kidolgozása annak érdekében, hogy megfelelő módon és időben bevonják az adatvédelmi tisztviselőt – amennyiben van ilyen –, valamint a jogi és belső ellenőrzési szolgálatokat a személyes adatok nemzetközi továbbításával kapcsolatos ügyekbe, és biztosítsák számukra az információkhoz való hozzáférést.***

134. ***A hatékonyság feltételei:***

- Az adattovábbítást megelőzően az adatvédelmi tisztviselőt – amennyiben van ilyen –, valamint a jogi és belső ellenőrzési egységet el kell látni minden vonatkozó információval, és konzultálni kell velük az adattovábbítás szükségességéről és az esetleges további garanciákról.
- A vonatkozó információknak magukban kell foglalniuk például az adott személyes adatok továbbításának szükségességére vonatkozó értékelést, a harmadik ország alkalmazandó jogszabályainak áttekintését, valamint azokat a garanciákat, amelyek biztosítására az adatátvevő kötelezettséget vállalt.

Szabványok és bevált módszerek elfogadása

135. ***Szigorú adatbiztonsági és adatvédelmi politikák elfogadása uniós tanúsítás vagy magatartási kódexek vagy nemzetközi szabványok (például ISO-szabványok) és bevált módszerek (például ENISA) alapján, a technika állásának kellő figyelembevételével, a kezelt adatok kategóriáinak kockázatával és annak valószínűségével összhangban, hogy a hatóságok megpróbálnak hozzáférni azokhoz.***

Egyéb

136. ***Belső politikák elfogadása és rendszeres felülvizsgálata a végrehajtott további intézkedések alkalmasságának értékelése, valamint szükség esetén további vagy alternatív megoldások azonosítása és végrehajtása céljából annak érdekében, hogy folyamatosan biztosítva legyen a továbbított személyes adatok védelmének az Európai Unióban biztosított védelmi szinttel azonos szintje.***

***

137. ***Az adatátvevő arra vonatkozó kötelezettségvállalása, hogy nem továbbítja újból a személyes adatokat ugyanazon vagy más harmadik országon belül, vagy hogy felfüggeszti a folyamatban lévő adattovábbításokat, ha a harmadik országban nem biztosítható a személyes adatoknak az Európai Unióban biztosítottal azonos szintű védelme.***[88]

[88] „Schrems II” ítélet (C-311/18), 135. és 137. pont.

3. MELLÉKLET HARMADIK ORSZÁGOK ÉRTÉKELÉSÉHEZ FELHASZNÁLHATÓ INFORMÁCIÓFORRÁSOK

138. Az adatátvevőnek képesnek kell lennie arra, hogy tájékoztassa Önt a letelepedési helye szerinti harmadik országgal és a rá alkalmazandó jogszabályokkal kapcsolatos releváns forrásokról és információkról. Számos információforrásra – például az alábbiakban nem kimerítő jelleggel felsorolt forrásokra – is támaszkodhat:

- az Európai Unió Bíróságának (EUB) és az Emberi Jogok Európai Bíróságának (EJEB)[89] az alapvető európai garanciákról szóló ajánlásban hivatkozott ítélkezési gyakorlata;[90]
- megfelelőségi határozatok a célországban, ha az adattovábbításra más jogalapon kerül sor;[91]
- kormányközi szervezetek, például az Európa Tanács,[92] más regionális szervek[93]; valamint az ENSZ szerveinek és ügynökségeinek (például az ENSZ Emberi Jogi Tanácsának,[94] az ENSZ Emberi Jogi Bizottságának[95]) határozatai és jelentései;
- a magánélet és az adatvédelem területén hatáskörrel rendelkező, harmadik országbeli független igazságügyi vagy közigazgatási hatóságok nemzeti ítélkezési gyakorlata vagy határozatai;
- tudományos intézmények és civil társadalmi szervezetek (például nem kormányzati szervezetek és szakmai szövetségek) jelentései.

[89] Lásd az EJEB tömeges megfigyeléssel kapcsolatos ítélkezési gyakorlatáról szóló tájékoztatót: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[91] „Schrems II” ítélet (C-311/18), 141. pont; lásd a megfelelőségi határozatokat az alábbi internetes címen: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[93] Lásd például az Emberi Jogok Amerikaközi Bizottságának (IACHR) országjelentéseit, https://www.oas.org/en/iachr/reports/country.asp.

[94] Lásd: https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[95] Lásd: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5