

# Ajánlások



**01/2020. számú ajánlás azon intézkedésekről, amelyek  
kiegészítik az adattovábbítási eszközöket  
a személyes adatok uniós védelmi szintjének való  
megfelelés biztosítása érdekében**

**2.0. változat**

**Elfogadás időpontja: 2021. június 18.**

## A dokumentum eddigi változatai

|               |                    |  |
|---------------|--------------------|--|
| 2.0. változat | 2021. június 18.   | Az ajánlás nyilvános konzultációt követő elfogadása          |
| 1.0. változat | 2020. november 10. | Az ajánlás nyilvános konzultáció céljából történő elfogadása |

## 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 adatexportőrként eljáró adatkezelők vagy adatfeldolgozók feladata, hogy esetről esetre és adott esetben a harmadik országbeli adatimportőrrel 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 adatexportőrök olyan kiegészítő 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 adatexportőröknek 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 a megfelelés igazolására.

Annak érdekében, hogy segítséget nyújtson az adatexportőröknek (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 kiegészítő intézkedések azonosításának összetett feladatában, az Európai Adatvédelmi Testület elfogadta ezt az ajánlást. Ez az ajánlás egymásután követendő lépéseket, lehetséges információforrásokat és néhány alkalmazható kiegészítő intézkedésekre vonatkozó példát kínál az adatexportőrök számára.

**Első lépésként** az Európai Adatvédelmi Testület azt tanácsolja Önnek, mint adatexportőrnek, 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 az 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 megfeleléségi 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 megfeleléségi határozat érvényességét. Megfeleléségi határozat hiányában az általános adatvédelmi rendelet 46. cikkében felsorolt adattovábbítási eszközök valamelyikét kell igénybe vennie. Az általános adatvédelmi rendelet 49. cikkében meghatározott eltérésekre csak néhány esetben hivatkozhat, ha teljesíti a feltételeket. Az

eltérések nem válhatnak a gyakorlatban „a főszabállyá”, hanem meghatározott helyzetekre kell korlátozódnuk.

A **harmadik lépés** annak **értékelése**, hogy a harmadik országban fennálló jogi helyzet és/vagy gyakorlat bármilyen módon hatást gyakorolhat-e azon adattovábbítási eszközök megfelelő garanciáinak hatékonyságára, amelyeket az adott adattovábbítással összefüggésben igénybe vesz. Az értékelésnek mindenekelőtt 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. A harmadik ország hatóságainak gyakorlatait is megvizsgálva ellenőrizheti, hogy az adattovábbítási eszközben foglalt garanciák képesek-e biztosítani a gyakorlatban a továbbított személyes adatok hatékony védelmét. E gyakorlatok megvizsgálása különösen fontos az Ön értékelése szempontjából, amennyiben:

(i.) a harmadik ország uniós előírásoknak formálisan megfelelő jogszabályait a gyakorlatban nyilvánvalóan nem alkalmazzák/nem tartják be;

(ii.) léteznek olyan gyakorlatok, amelyek összeegyeztethetetlenek az adattovábbítási eszköz kötelezettségvállalásaival, amennyiben a harmadik országban hiányoznak a vonatkozó jogszabályok;

(iii.) az Ön által továbbított adatok és/vagy az adatimportőr problematikus jogszabályok hatálya alá tartoznak vagy tartozhatnak (azaz megkérdőjelezi az adattovábbítási eszközben foglalt szerződéses garanciát a lényegében azonos védelmi szintről, és nem felelnek meg az alapvető jogokra, a szükségességre és az arányosságra vonatkozó uniós követelményeknek).

Az első két esetben fel kell függesztenie az adattovábbítást, vagy megfelelő kiegészítő intézkedéseket kell végrehajtania, ha folytatni kívánja azt.

A harmadik esetben a problematikus jogszabályoknak az Ön által végzett adattovábbításra való esetleges alkalmazását övező bizonytalanságokra tekintettel a következőképpen dönthet: felfüggeszti az adattovábbítást; további kiegészítő intézkedéseket hajt végre az adattovábbítás folytatása érdekében; vagy dönthet úgy is, hogy kiegészítő intézkedések végrehajtása nélkül folytatja az adattovábbítást, ha úgy ítéli meg, és képes bizonyítani és dokumentálni, hogy nincs oka azt feltételezni, hogy a vonatkozó és problematikus jogszabályokat a gyakorlatban úgy értelmezik és/vagy alkalmazzák majd, hogy azok hatálya kiterjedjen az Ön által továbbított adatokra és az adatimportőrré.

Azon elemek értékelését illetően, amelyeket figyelembe kell venni egy harmadik ország hatóságainak adatokhoz való megfigyelési célú hozzáféréseire vonatkozó jogának értékelése során, kérjük, olvassa el az Európai Adatvédelmi Testület alapvető európai garanciákról szóló ajánlását.

Ezt az értékelést kellő gondossággal kell elvégeznie, és alaposan dokumentálnia kell. Az illetékes felügyeleti és/vagy igazságügyi hatóságok kérhetik ezt, és elszámoltathatják Önt az ez alapján hozott bármely döntésért.

A **negyedik lépés** azon **kiegészítő 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 és/vagy gyakorlatai 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 kiegészítő intézkedések példáinak és a hatékonyságukhoz szükséges egyes feltételeknek a nem kimerítő felsorolását tartalmazza. A 46. cikk szerinti adattovábbítási eszközökben foglalt megfelelő garanciákhoz hasonlóan egyes kiegészítő intézkedések egyes országokban hatékonyak lehetnek, másokban azonban nem feltétlenül. Az Ön feladata értékelni ezen intézkedések hatékonyságát az adattovábbítással összefüggésben, valamint a harmadik ország jogának, gyakorlatainak és az Ön által igénybe vett adattovábbítási eszköznek a fényében, mivel elszámoltatható lesz az Ön által ez alapján hozott bármely döntésért. Ehhez több kiegészítő intézkedés kombinálására is szükség lehet. Végző soron úgy találhatja, hogy egyetlen kiegészítő intézkedés sem képes lényegében azonos védelmi szintet

biztosítani az Ön által végzett konkrét adattovábbítás esetében. Azokban az esetekben, amelyekben egyetlen kiegészítő 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 kiegészítő intézkedések ezen értékelését kellő gondossággal kell elvégeznie és dokumentálnia.

Az **ötödik lépés minden olyan hivatalos eljárási lépés megtétele**, amelyre az Ön kiegészítő intézkedésének elfogadásához szükség lehet, az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköztől függően. A jelen ajánlás részletezi ezen alakiságok némelyikét. Előfordulhat, hogy ezek 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 személyes adatok védelmi szintjének **újraértékelését**, és kísérelje 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 adatexportőrök 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 adatexportőrök részére történő kidolgozását, és továbbra is összehangolják fellépésüket az Európai Adatvédelmi Testületen belül.

## TARTALOMJEGYZÉK

|     |   |    |
|-----|---|----|
| 1   | Az adattovábbítással kapcsolatos elszámoltathatóság .....   | 9  |
| 2   | Útmutató: az elszámoltathatóság elvének gyakorlati alkalmazása az adattovábbítások során ...  | 10 |
| 2.1 | 1. lépés: Ismerje az Ön által végzett adattovábbításokat .....  | 10 |
| 2.2 | 2. lépés: Azonosítsa azokat az adattovábbítási eszközöket, amelyeket igénybe kíván venni  | 12 |
| 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 | 15 |
| 2.4 | 4. lépés: Fogadjon el kiegészítő intézkedéseket .....   | 24 |
| 2.5 | 5. lépés: Eljárási lépések hatékony kiegészítő intézkedések azonosítása esetén .....  | 26 |
| 2.6 | 6. lépés: Végezzen újraértékelést megfelelő időközönként.....   | 28 |
| 3   | Következtetés .....   | 29 |
| 1.  | MELLÉKLET: FOGALOMMEGHATÁROZÁSOK .....  | 30 |
| 2.  | MELLÉKLET: PÉLDÁK KIEGÉSZÍTŐ INTÉZKEDÉSEKRE .....   | 31 |
| 2.1 | Technikai intézkedések .....  | 31 |
| 2.2 | További szerződéses intézkedések.....   | 40 |
| 2.3 | Szervezési intézkedések .....   | 49 |
| 3.  | MELLÉKLET Harmadik országok ÉRTÉKELÉSÉHEZ FELHASZNÁLHATÓ INFORMÁCIÓFORRÁSOK .....   | 53 |

## 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<sup>1</sup> 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.<sup>2</sup>

(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.<sup>3</sup>

(3) Az általános adatvédelmi rendelet (108) preambulumbekzdése 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.

---

<sup>1</sup> A jelen dokumentumban a „tagállamokra” történő bármely hivatkozást „EGT-tagállamokra” történő hivatkozásként kell érteni.

<sup>2</sup> 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.

<sup>3</sup> „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 adatfeldolgozóknak 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 adatexportőröknek az uniós jog által megkövetelt védelmi szint egy adott harmadik országban történő tiszteletben tartásának biztosítása érdekében kiegészítő intézkedésekkel kell kiegészíteniük azon garanciákat, amelyeket ezen általános adatvédelmi kikötések tartalmaznak. A Bíróság hivatkozik az általános adatvédelmi rendelet (109) preambulumbekzdésére, amely megemlíti ezt a lehetőséget, és arra ösztönzi az adatkezelőket és az adatfeldolgozókat, hogy éljenek azzal.<sup>4</sup>

(5) A Bíróság megállapította, hogy mindenekelőtt az adatexportőr feladata, hogy esetről esetre és adott esetben az adatimportőrrel 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 kiegészítő intézkedéseket előírva.<sup>5</sup>

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

(7) Az általános adatvédelmi rendelet vagy a Bíróság nem határozza meg vagy pontosítja azokat a „további garanciákat” vagy „kiegészítő intézkedéseket” az általános adatvédelmi rendelet 46. cikkének (2) bekezdésében felsorolt adattovábbítási eszközök garanciáihoz képest, 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 adatexportőrként eljáró adatkezelőknek és adatfeldolgozóknak arra vonatkozóan, hogy milyen eljárást követhetnek kiegészítő intézkedések azonosítása és elfogadása érdekében. Ezen ajánlás célja, hogy módszertan biztosítson az adatexportőrök számára annak megállapításához, hogy szükség van-e kiegészítő intézkedésekre, és ha igen, milyen kiegészítő intézkedésekre van szükség az általuk végzett adattovábbításhoz. Az adatexportőrök elsődleges felelőssége annak biztosítása, hogy a továbbított adatok az EGT-ben 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<sup>7</sup>

## **ELFOGADTA A KÖVETKEZŐ AJÁNLÁST:**

---

<sup>4</sup> „Schrems II” ítélet (C-311/18), 132. és 133. pont.

<sup>5</sup> „Schrems II” ítélet (C-311/18), 134. pont.

<sup>6</sup> „Schrems II” ítélet (C-311/18), 135. pont.

<sup>7</sup> 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.<sup>8</sup> Az adatvédelemhez való jog következképpen magas szintű védelmet élvez, és csak a törvény által, e jog lényeges tartalmának tiszteletben tartásával, arányosan 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.<sup>9</sup> 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.<sup>10</sup>
2. Annak biztosítása érdekében, hogy az általános adatvédelmi rendeletben garantált védelmi szint se az adattovábbítás során, se azt követően 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 adatexportőrök és adatimportőrök (függetlenül attól, hogy adatkezelők és/vagy adatfeldolgozók-e) egyszerűen elismerjék vagy passzívan tiszteletben tartsák ezt a jogot.<sup>11</sup> 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 és az adatvédelmi felügyeleti hatóságok felé. Ez az úgynevezett elszámoltathatóság elve.<sup>12</sup>
4. Az általános adatvédelmi rendelet által biztosított védelmi szint hatékony alkalmazásának biztosításához szükséges elszámoltathatóság elve a harmadik országokba irányuló adattovábbításokra is vonatkozik<sup>13</sup>, mivel ezek önmagukban az adatkezelés egyik formájának minősülnek.<sup>14</sup> 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.<sup>15</sup>
5. A „Schrems II” ítéletben a Bíróság hangsúlyozza az adatexportőrök és adatimportőrök 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

---

<sup>8</sup> Az Alapjogi Charta 8. cikkének (1) bekezdése és az EUMSZ 16. cikk (1) bekezdése, az általános adatvédelmi rendelet (1) preambulumbekzdése, 1. cikkének (2) bekezdése.

<sup>9</sup> Az Európai Unió Alapjogi Chartája 52. cikkének (1) bekezdése.

<sup>10</sup> Az általános adatvédelmi rendelet (4) preambulumbekzdése; Google LLC, a Google Inc. jogutódja, kontra Commission nationale de l'informatique et des libertés (CNIL) ítélet, C-507/17, 60. pont.

<sup>11</sup> Sharpston főtanácsnok 2010. június 17-i indítványa, Volker und Markus Schecke GbR kontra Land Hessen, C-92/09 és C-93/02, 71. pont.

<sup>12</sup> Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 28. cikke (3) bekezdésének h) pontja.

<sup>13</sup> Az általános adatvédelmi rendelet 44. cikke és (101) preambulumbekzdése, valamint 47. cikke (2) bekezdésének d) pontja.

<sup>14</sup> Az EUB 2015. október 6-i ítélete, *Maximillian Schrems kontra Data Protection Commissioner*, (a továbbiakban: „Schrems I” ítélet [C-362/14]), 45. pont.

<sup>15</sup> „Schrems II” ítélet (C-311/18), 92. és 93. pont.

felfüggesztéséért és/vagy a szerződéstől való elállásért, ha az adatimportőr nem, vagy már nem képes tiszteletben tartani az adatexportőr és az adatimportőr közötti vonatkozó szerződésben foglalt általános adatvédelmi kikötéseket.<sup>16</sup> Az adatexportőrként eljáró adatkezelőnek vagy adatfeldolgozónak biztosítani kell, hogy az adatimportőrök adott esetben együttműködjenek az adatexportőrrel e kötelezettségeinek teljesítése során olyan módon, hogy tájékoztatják például a kapott személyes adatok védelmének szintjét érintően, az adatimportőr országában bekövetkezett bármely fejleményről.<sup>17</sup> Ezek a kötelezettségek az általános adatvédelmi rendeletben rögzített elszámoltathatóság elvének az adattovábbításokra történő alkalmazását jelentik.<sup>18</sup>

## 2 ÚTMUTATÓ: AZ ELSZÁMOLTATHATÓSÁG ELVÉNEK GYAKORLATI ALKALMAZÁSA AZ ADATTOVÁBBÍTÁSOK SORÁN

6. Az alábbi útmutató felvázolja, hogy milyen lépéseket kell tenni annak megállapítása érdekében, hogy Önnek (mint adatexportőrnek) kiegészítő 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 – adatexportőrként eljáró adatkezelőt vagy adatfeldolgozót<sup>19</sup> jelenti.<sup>20</sup> 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.<sup>21</sup>
7. Ezt az értékelést és az Ön által választott és végrehajtott kiegészítő intézkedéseket megfelelően dokumentálnia kell, és kérésre az illetékes felügyeleti hatóság rendelkezésére kell bocsátania ezt a dokumentációt.<sup>22</sup>

### 2.1 1. lépés: Ismerje az Ön által végzett adattovábbításokat

8. Annak megállapítása érdekében, hogy mi szükséges ahhoz, hogy Ön (mint adatexportőr) folytathassa a személyes adatok továbbítását, vagy új személyesadat-továbbításokat hajthasson

---

<sup>16</sup> „Schrems II” ítélet (C-311/18), 134., 135., 139., 140., 141., 142. pont.

<sup>17</sup> „Schrems II” ítélet (C-311/18), 134. pont.

<sup>18</sup> Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 28. cikke (3) bekezdésének h) pontja.

<sup>19</sup> Ezért például Ön nem minősül adatexportőrnek, ha érintettként egy harmadik országban letelepedett adatkezelőnek online kérdőív útján adja meg személyes adatait.

<sup>20</sup> 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](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en)

<sup>21</sup> 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\\_en](https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en)

<sup>22</sup> Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 24. cikkének (1) bekezdése.

végre<sup>23</sup>, 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 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.<sup>24</sup> 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.<sup>25</sup>
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<sup>26</sup>.
11. Önnek az általános adatvédelmi rendelet „adattakarékosságra” vonatkozó elvével<sup>27</sup> összhangban ellenőriznie kell, hogy az Ön által továbbított adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak-e, és a szükségesre korlátozódnak-e.

---

<sup>23</sup> Kérjük, vegye figyelembe, hogy adattovábbításnak minősül a harmadik országbeli jogalany által az EGT-ben található adatokhoz való távoli hozzáférés is.

<sup>24</sup> Lásd az általános 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).

<sup>25</sup> 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 megfelelési 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 ítélezési gyakorlatának fényében.

<sup>26</sup> Ha az adatkezelő az általános adatvédelmi rendelet 28. cikkének (2) bekezdésével összhangban előzetesen írásban eseti vagy általános felhatalmazást tett.

<sup>27</sup> Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja.

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 adatimportőrök által kezelhetők (célállomások térképe).
13. Tartsa szem előtt, hogy a harmadik országból való távoli hozzáférés (például támogatási helyzetekben) és/vagy az EGT-n kívül található, egy szolgáltató által kínált felhőben való tárolás szintén adattovábbításnak minősül.<sup>28</sup> Konkrétabban, ha Ön nemzetközi felhőinfrastruktúrát használ, fel kell mérnie, hogy adatait harmadik országokba továbbítják-e, és ha igen, hova, kivéve, ha a felhőszolgáltató az EGT-ben telepedett le, és 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.<sup>29</sup>
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).<sup>30</sup>
18. Az Európai Bizottság a honlapján közzéteszi a megfelelőségi határozatok jegyzékét.<sup>31</sup>

---

<sup>28</sup> 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 Maximilian Schrems ügyben hozott ítéletéről, 2020. július 23.

<sup>29</sup> Az Európai Bizottság az általános adatvédelmi rendelet 45. cikke alapján megállapíthatja, hogy valamely Európai Unióon kívüli ország megfelelő adatvédelmi szintet biztosít-e. Az Európai Bizottság azt is megállapíthatja, hogy egy nemzetközi szervezet megfelelő védelmi szintet biztosít.

<sup>30</sup> Az általános adatvédelmi rendelet 45. cikkének (1) bekezdése.

<sup>31</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

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.**<sup>32</sup> Továbbra is figyelemmel kell azonban kísérnie, hogy az Ön által végzett adattovábbításokkal kapcsolatos megfelelőségi határozatokat visszavonták vagy érvénytelenítették-e.<sup>33</sup>
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.<sup>34</sup>

**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.<sup>35</sup>

<sup>32</sup> Feltéve, hogy Ön és az adatimportőr intézkedéseket hajtott végre az általános adatvédelmi rendelet szerinti egyéb kötelezettségeknek való megfelelés érdekében; ellenkező esetben végre kell hajtani ezeket az intézkedéseket.

<sup>33</sup> 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) 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]).

<sup>34</sup> „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.

<sup>35</sup> „Schrems I” ügy (C-362/14).

### 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 adatexportőrök 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<sup>36</sup>);
  - kötelező erejű vállalati szabályok (BCR<sup>36</sup>);
  - magatartási kódexek;
  - tanúsítási mechanizmusok;
  - ad hoc szerződéses rendelkezések.
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 („kiegészítő intézkedések”).<sup>36</sup>

### 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 oly módon kell értelmezni, amely nem mond ellent az eltérések természetének, vagyis annak, hogy azok kivételt képeznek azon főszabály alól, hogy a személyes adatok nem továbbíthatók harmadik országba, kivéve, ha az adott ország megfelelő adatvédelmi szintet biztosít, vagy megfelelő garanciák állnak rendelkezésre. Az eltérések nem válhatnak a gyakorlatban „a főszabállyá”, hanem meghatározott helyzetekre kell korlátozódniuk. Az Európai Adatvédelmi Testület kiadta az (EU) 2016/679 rendelet 49. cikke szerinti eltérésekről szóló 2/2018. sz. iránymutatását.<sup>37</sup>
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.

\*\*\*

---

<sup>36</sup> „Schrems II” ítélet (C-311/18), 130. és 133. pont. Lásd a lenti 2.3. alszakaszt is.

<sup>37</sup> Ezzel kapcsolatban további útmutatásért lásd: [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en).

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. Az általános adatvédelmi rendelet 46. cikke alapján választott adattovábbítási eszköznek hatékonyan biztosítania kell, hogy az adattovábbítás a gyakorlatban ne sértse az általános adatvédelmi rendeletben garantált védelem szintjét.<sup>38</sup>

29. A továbbított személyes adatoknak különösen olyan védelmet kell élvezniük a harmadik országban, amely lényegében azonos az EGT-ben az Európai Unió Alapjogi Chartájával összefüggésben értelmezett általános adatvédelmi rendelet által biztosított védelemmel.<sup>39</sup> Nem ez a helyzet akkor, ha az adatimportőr a harmadik ország adattovábbításra vonatkozó jogszabályai és gyakorlatai miatt nem tud eleget tenni – az adatoknak az adatexportőr által az adatimportőr országába történő továbbítása során sem – az általános adatvédelmi rendelet 46. cikke alapján választott adattovábbítási eszköz szerinti kötelezettségeinek<sup>40</sup>.

30. Önnek – adott esetben az adatimportőrrel együttműködve – először értékelnie kell, hogy a harmadik országban fennálló jogi helyzet és/vagy gyakorlat<sup>41</sup> 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. Ez magában foglalja annak meghatározását, hogy az Ön által végzett adattovábbítás olyan jogszabályok és/vagy gyakorlatok hatálya alá tartozik-e, amelyek hatást gyakorolhatnak az Ön általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközének hatékonyságára. Az elvégzendő értékelésnek mindenképp a nyilvánosan elérhető jogszabályokon kell alapulnia.

31. Ezen értékelésnek olyan elemeket kell tartalmaznia, melyek arra vonatkoznak, hogy az Ön adatátvevője harmadik országának hatóságai miként férhetnek hozzá az adatokhoz, mint például:

- az arra vonatkozó elemeket, hogy az Ön adatimportőrje harmadik országának hatóságai a jogszabályok, a gyakorlat és a bejelentett precedensek fényében az adatimportőr tudtával vagy anélkül hozzá kívánhatnak-e férni az adatokhoz;
- az arra vonatkozó elemeket, hogy az Ön adatimportőrje harmadik országának hatóságai a jogszabályok, a jogkörök, a rendelkezésükre álló technikai, pénzügyi és emberi erőforrások, valamint a bejelentett precedensek fényében az adatimportőrön keresztül vagy a távközlési szolgáltatókon vagy kommunikációs csatornákon keresztül képesek lehetnek-e hozzáférni az adatokhoz.

---

<sup>38</sup> Az általános adatvédelmi rendelet 44. cikke és a „Schrems II” ítélet (C-311/18) 126., 137. és 148. pontja.

<sup>39</sup> „Schrems II” ítélet (C-311/18), 105. pont és a rendelkező rész 2) pontja.

<sup>40</sup> Lásd: „Schrems II” ítélet (C-311/18), a 184. ponttal összefüggésben értelmezett 183. pont.

<sup>41</sup> Lásd a „Schrems II” ítélet (C-311/18) 126. pontját, amelyben a Bíróság kifejezetten hivatkozik „az érintett harmadik országban fennálló jogi helyzetre és gyakorlatra”, és megköveteli „az érintett harmadik országba továbbított személyes adatok hatékony védelmének a gyakorlatban történő biztosítását” (utólagos kiemelés), valamint 158. pontját.

### Az adattovábbítás összes körülményének fényében releváns jogszabályok és gyakorlatok azonosítása

32. Meg kell vizsgálnia minden egyes adattovábbítás jellemzőit, és meg kell állapítania, hogy az Ön által végzett egyes adattovábbításokra hatást gyakorol-e az adattovábbítás (vagy az újbóli adattovábbítás) célországában fennálló belső jogrend és/vagy gyakorlat. Az Ön által végzett értékelés terjedelme ezért az Ön által továbbított konkrét adatok védelme szempontjából releváns jogszabályokra és gyakorlatokra korlátozódik, ellentétben az Európai Bizottság által az általános adatvédelmi rendelet 45. cikkével összhangban végzett általános és széles körű megfelelőségi értékelésekkel.
33. Az alkalmazandó jogi háttér és/vagy gyakorlatok az Ön által végzett adattovábbítás konkrét körülményeitől, különösen a következőktől függenek:
- 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);<sup>42</sup>
  - az adatokat a harmadik országban tárolják-e, vagy csak távoli hozzáféréssel érhetőek-e el az EU-ban/EGT-ben tárolt adatok;
  - a továbbítandó adatok formátuma (például egyszerű szöveg/álnevesített vagy titkosított<sup>43</sup>);
  - lehetőség arra, hogy az adatokat a harmadik országból újból továbbítsák egy másik harmadik országba.<sup>44</sup>
34. 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 adatimportőr működik közre, annál összetettebb lesz az Ön értékelése. Ezen értékelés keretében a tervezett újbóli adattovábbítást is figyelembe kell vennie.

---

<sup>42</sup> A személyes adatok továbbítása adatkezelési művelet (az általános adatvédelmi rendelet 4. cikkének (2) bekezdése). Ha Ön az általános adatvédelmi rendelet 9. és 10. cikkének hatálya alá tartozó különleges adatokat kíván továbbítani, csak akkor végezhet adattovábbítást, ha az az általános adatvédelmi rendelet 9. és 10. cikkében, valamint az uniós tagállamok jogában meghatározott eltérések és feltételek valamelyikének hatálya alá tartozik. Az általános adatvédelmi rendelet 32. cikkével összhangban Önnek – az adatkezelőként vagy adatfeldolgozóként eljáró adatimportőrrel együtt – megfelelő technikai és szervezési intézkedéseket is végre kell hajtania annak érdekében, hogy az érintettek jogaira és szabadságaira a továbbított adatokat érintő esetleges adatvédelmi incidens által jelentett kockázatok mértékének megfelelő szintű adatbiztonságot garantálja (az általános adatvédelmi rendelet 4. cikkének 12. pontja). A továbbított adatok kategóriái és különleges jellege releváns lesz a kockázat értékelése és az intézkedések megfelelősége szempontjából.

<sup>43</sup> Egyes harmadik országok nem engedélyezik titkosított adatok átvételét.

<sup>44</sup> Ha az adatkezelő az általános adatvédelmi rendelet 28. cikkének (2) bekezdésével összhangban előzetesen írásban eseti vagy általános felhatalmazást tett.



35. Minden esetben különös figyelmet kell fordítani 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 vagy nemzetbiztonsági célokból). Ha ezek a követelmények vagy hatáskörök korlátozzák az érintettek alapvető jogait, miközben tiszteletben tartják azok lényeges tartalmát, és az uniós jogban vagy az uniós tagállamok jogában is elismert fontos célkitűzések védelméhez szükséges és arányos intézkedések egy demokratikus társadalomban,<sup>45</sup> akkor azok nem lehetnek hatással az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszközben foglalt kötelezettségvállalásokra.
36. Értékelnie kell a vonatkozó általános jellegű szabályokat és gyakorlatokat, amennyiben azok hatással vannak az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt garanciák hatékony alkalmazására.
37. Ezen értékelés elvégzése során az adott harmadik ország jogrendszerének különböző elemei – például az általános adatvédelmi rendelet 45. cikkének (2) bekezdésében felsorolt tényezők – is relevánsak. Például valamely harmadik országban a jogállamiság helyzete releváns lehet az egyének számára a személyes adatokhoz való jogellenes kormányzati hozzáféréssel szemben rendelkezésre álló (bírói) 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.
38. Az ilyen jogszabályokból és gyakorlatokból eredő kötelezettségek és hatáskörök akkor tekintendők úgy, hogy hatással vannak az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt kötelezettségvállalásokra, illetve hogy összeegyeztethetetlenek azokkal, ha<sup>46</sup>:
- ) nem tartják tiszteletben az Európai Unió Alapjogi Chartájában foglalt alapvető jogok és szabadságok lényeges tartalmát, vagy
  - ) túllépi az uniós vagy tagállami jogban is elismert – az általános adatvédelmi rendelet 23. cikkének (1) bekezdésében felsoroltakhoz hasonló – fontos célkitűzések valamelyikének védelméhez egy demokratikus társadalomban szükséges és arányos mértéket.
39. Ellenőriznie kell, hogy az adatimportőrnek az érintettek számára jogaik gyakorlását az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben előírtaknak megfelelően lehetővé tevő kötelezettségvállalásai (például a továbbított adatokhoz való hozzáférés, azok helyesbítése és törlése iránti kérelmek, valamint a [bírói] jogorvoslat) hatékonyan

---

<sup>45</sup> 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\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en).

<sup>46</sup> Lásd az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, az általános adatvédelmi rendelet 23. cikkének (1) bekezdését, a „Schrems II” ítélet (C-311/18) 174. és 187. pontját, valamint az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló, 2020. november 10-i 02/2020. sz. ajánlását.

alkalmazhatók-e a gyakorlatban, és azokat nem akadályozzák-e a célországoknak számító harmadik ország jogszabályai és/vagy gyakorlatai.

40. Az uniós előírásokat, például az Európai Unió Alapjogi Chartájának 47. és 52. cikkét, referenciaként kell használni különösen annak értékeléséhez, hogy a hatóságok hozzáférése a demokratikus társadalomban szükséges és arányos mértékre korlátozódik-e, és hogy az érintettek számára hatékony jogorvoslatot biztosítanak-e.
41. Az Európai Adatvédelmi Testület alapvető európai garanciákról szóló ajánlása<sup>47</sup> pontosítja azokat az elemeket, amelyeket értékelni kell annak megállapításához, hogy a nemzetbiztonsági ügynökségként vagy bűnüldöző hatóságként működő harmadik országbeli hatóságok személyes adatokhoz való hozzáférést szabályozó jogi keret igazolható beavatkozásnak tekinthető-e<sup>48</sup>. Ezt különösen akkor kell gondosan mérlegelni, ha a hatóságok adatokhoz való hozzáféréseire vonatkozó jogszabályok nem egyértelműek, vagy nem érhető el nyilvánosan. Az alapvető európai garanciák első követelménye, hogy nyilvánosan elérhető és kellően egyértelmű jogi keretnek kell szabályoznia az ilyen hozzáférést, amennyiben az elő van irányozva.
42. A 46. cikk szerinti adattovábbítási eszközökön alapuló adattovábbítások helyzetére alkalmazva az Európai Adatvédelmi Testület alapvető európai garanciákról szóló ajánlása útmutatással szolgálhat az adatexportőr számára annak értékeléséhez, hogy ezek a hatáskörök indokolatlanul akadályozzák-e az adatexportőrnek és az adatimportőrnek a lényegi azonosság biztosítására vonatkozó, az általános adatvédelmi rendelet vagy az adattovábbítási eszközben foglalt kötelezettségvállalások szerinti kötelezettségeit. A lényegében azonos védelmi szint hiánya különösen akkor válik nyilvánvalóvá, ha a harmadik országnak az Ön által végzett adattovábbításra vonatkozó jogi szabályozása és/vagy gyakorlatai nem felelnek meg az alapvető európai garanciák követelményeinek. Az Európai Adatvédelmi Testület ismét kiemeli, hogy az alapvető európai garanciák referenciaszintnek minősülnek a harmadik ország megfigyelési intézkedései által eredményezett beavatkozás értékelése során, a nemzetközi adattovábbításokkal összefüggésben. E követelmények az uniós jogból és az EUB, valamint az EJEB ítélezési gyakorlatából következnek, amely kötelező az uniós tagállamokra.
43. Az Ön értékelésének mindenekelőtt a nyilvánosan elérhető jogszabályokon kell alapulnia. A harmadik ország hatóságainak gyakorlatait is megvizsgálva ellenőrizheti, hogy az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt garanciák megfelelő eszközök lehetnek-e a gyakorlatban a továbbított személyes adatok hatékony védelmének biztosítására.<sup>49</sup> A harmadik országban fennálló gyakorlatok vizsgálata különösen fontos lesz az Ön által az alábbiakban ismertetett helyzetekben elvégzett értékelés szempontjából.
- 43.1 **Előfordulhat, hogy a harmadik ország vonatkozó jogszabályai formálisan megfelelnek az alapvető jogokra és szabadságokra vonatkozó uniós előírásoknak, valamint az azokra vonatkozó korlátozások szükségességének és arányosságának.** A harmadik ország hatóságainak gyakorlatai (pl. a magánszektor birtokában lévő személyes adatokhoz való hozzáférés vagy a jogszabályok felügyeleti vagy igazságügyi hatóságként történő végrehajtása – vagy ennek mellőzése – körében) azonban egyértelműen arra utalhatnak, hogy e hatóságok

---

<sup>47</sup> [EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.](#)

<sup>48</sup> És ezért úgy tekinthető-e, mint amely nincs hatással az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz keretében tett kötelezettségvállalásokra.

<sup>49</sup> „Schrems II” ítélet (C-311/18), 126. pont.

általában nem alkalmazzák/nem tartják be azokat a jogszabályokat, amelyek főszabály szerint a tevékenységeiket szabályozzák. Ebben az esetben az értékelés során figyelembe kell vennie ezeket a gyakorlatokat, és úgy kell tekintenie, hogy az általános adatvédelmi rendelet 46. cikke szerinti eszköz önmagában (azaz kiegészítő intézkedések nélkül) nem lesz képes hatékonyan biztosítani a lényegében azonos védelmi szintet. Ilyen esetben, ha folytatni kívánja az adattovábbítást, megfelelő kiegészítő intézkedéseket kell végrehajtania.

**43.2 Előfordulhat, hogy a harmadik országban hiányoznak a vonatkozó jogszabályok (pl. a magánszektor birtokában lévő személyes adatokhoz való hozzáférésre vonatkozóan).** Ebben az esetben a vonatkozó jogszabályok hiányából nem következtethet automatikusan arra, hogy az Ön általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköze hatékonyan alkalmazható. Ellenőriznie kell, hogy vannak-e az országban fennálló olyan gyakorlatokra utaló jelek, amelyek nem egyeztethetők össze az uniós joggal és az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt kötelezettségvállalásokkal. Összeegyeztethetetlen gyakorlatok fennállása esetén az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz önmagában (azaz megfelelő kiegészítő intézkedések nélkül) nem lesz képes hatékonyan biztosítani a lényegében azonos védelmi szintet. Ilyen esetben, ha folytatni kívánja az adattovábbítást, megfelelő kiegészítő intézkedéseket kell végrehajtania.

**43.3 Előfordulhat, hogy az értékelés azt tárja fel, hogy a harmadik ország vonatkozó jogszabályai problematikusak<sup>50</sup> lehetnek, és hogy a továbbított adatok és/vagy az érintett adatimportőr e problematikus jogszabályok hatálya alá tartozik vagy tartozhat<sup>51</sup>.**

A problematikus jogszabályoknak az Ön által végzett adattovábbításra való esetleges alkalmazását övező bizonytalanságokra tekintettel Ön a következőképpen dönthet:

- J felfüggeszti az adattovábbítást;
- J kiegészítő intézkedéseket hajt végre<sup>52</sup> annak érdekében, hogy megelőzze annak kockázatát, hogy esetlegesen az adatimportőr harmadik országának olyan jogszabályait és/vagy gyakorlatait alkalmazzák az Ön adatimportőrijére és/vagy az Ön által továbbított adatokra, amelyek megkérdőjelezhetik az EGT-ben biztosítottal lényegében azonos védelmi szint adattovábbítási eszközben foglalt szerződéses garanciáját; vagy

---

<sup>50</sup> A „problematikus jogszabályok” alatt olyan jogszabályok értendők, amelyek 1) olyan kötelezettségeket írnak elő az Európai Unióból származó személyes adatok továbbításának címzettjével szemben, és/vagy olyan hatást gyakorolnak a továbbított adatokra, amelyek, illetve amely megkérdőjelezheti a lényegében azonos védelmi szint adattovábbítási eszközökben foglalt szerződéses garanciáját, és 2) nem tartják tiszteletben az Európai Unió Alapjogi Chartája által elismert alapvető jogok és szabadságok lényeges tartalmát, vagy túllépi az uniós jogban vagy az uniós tagállamok jogában is elismert – az általános adatvédelmi rendelet 23. cikkének (1) bekezdésében felsoroltakhoz hasonló – fontos célkitűzések valamelyikének védelméhez egy demokratikus társadalomban szükséges és arányos mértéket.

<sup>51</sup> Nem feltétlenül egyértelmű, hogy az adatimportőr és/vagy a továbbított adatok a nemzetbiztonsági jogszabályokban az alkalmazási körük korlátozása érdekében gyakran használt olyan általános kifejezések hatálya alá tartoznak-e, mint például az „elektronikus hírközlési szolgáltató” és a „külföldi hírszerzési információ”.

<sup>52</sup> Lásd: az általános adatvédelmi rendelet (109) preambulumbekzdése és a „Schrems II” ítélet (C-311/18) 132. pontja.

J) dönthet úgy, hogy az adattovábbítást kiegészítő intézkedések végrehajtása nélkül folytatja, ha úgy ítéli meg, hogy nincs oka azt feltételezni, hogy az Ön által továbbított adatokra és/vagy az Ön adatimportőrére a gyakorlatban a vonatkozó és problematikus jogszabályokat fogják alkalmazni. Értékelése révén – adott esetben az adatimportőrrel együttműködve – igazolnia és dokumentálnia kell, hogy a jogot nem értelmezik és/vagy alkalmazzák úgy a gyakorlatban, hogy annak hatálya kiterjedjen az Ön által továbbított adatokra és az Ön adatimportőrére, figyelembe véve az ugyanazon ágazatban működő és/vagy hasonló továbbított személyes adatokhoz kötődő más szereplők tapasztalatait és az alábbiakban ismertetett további információforrásokat is<sup>53</sup>.

Ezért Önnek részletes jelentéssel<sup>54</sup> kell igazolnia és dokumentálnia, hogy a problematikus jogszabályokat a gyakorlatban nem fogják az Ön által továbbított adatokra és/vagy az Ön adatimportőrére alkalmazni, és így ez nem fogja megakadályozni az adatimportőrt abban, hogy teljesítse az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközökből eredő kötelezettségeit<sup>55</sup>.

#### *Felhasználható információforrások*

44. Adatimportőrének az Ön rendelkezésére kell bocsátania a letelepedési helye szerinti harmadik országgal kapcsolatos releváns forrásokat és információkat, valamint az adattovábbításra alkalmazandó hatályos jogszabályokat és gyakorlatokat.
45. Ön és adatimportőrije kiegészítheti értékelését a 3. mellékletben példaként felsoroltakhoz hasonló forrásokból származó információkkal.
46. A harmadik ország adattovábbításra alkalmazandó jogi kerete mellett a forrásoknak és információknak relevánsnak, objektívnek, megbízhatónak, ellenőrizhetőnek és nyilvánosan elérhetőnek vagy egyéb módon hozzáférhetőnek kell lenniük annak megállapítása érdekében, hogy az Ön 46. cikk szerinti adattovábbítási eszköze hatékonyan alkalmazható-e<sup>56</sup>, és Önnek értékelnie és dokumentálnia kell ezt.

---

<sup>53</sup> Lásd a 45–47. pontot.

<sup>54</sup> Az Ön által készített jelentéseknek átfogó információkat kell tartalmazniuk a jogszabályok és gyakorlatok jogi értékeléséről, valamint azoknak a konkrét adattovábbításokra való alkalmazásáról, az értékelés elkészítéséhez szükséges belső eljárásról (ideértve az értékelésben részt vevő szereplőkre – például ügyvédi irodákra, tanácsadókra vagy belső szervezeti egységekre – vonatkozó információkat is) és az ellenőrzések időpontjáról. A jelentéseket az adatexportőr jogi képviselőjének kell jóváhagynia.

<sup>55</sup> Annak igazolása, hogy az Ön által továbbított adatokra és az Ön adatimportőrére a gyakorlatban nem alkalmazzák a problematikus jogszabályokat, figyelembe véve az ugyanazon ágazatban működő és/vagy hasonló továbbított személyes adatokhoz kötődő más szereplők tapasztalatait is, nem mentesíti Önt az alól, hogy a személyes adatoknak a célországnak számító harmadik országba történő továbbítása és ott történő kezelése során biztosítandó védelméhez szükséges kiegészítő intézkedéseket írjon elő (pl. az adatok végponttól végpontig terjedő titkosítása – lásd a 2. mellékletben a további technikai intézkedésekre vonatkozó példákat), amennyiben a célországnak számító harmadik ország alkalmazandó jogszabályainak Ön által elvégzett elemzése azt mutatja, hogy az adatokhoz való hozzáférésre az adatimportőr beavatkozásának hiányában is sor kerülhet az adattovábbítás pillanatában. Elképzelhető, hogy az általános adatvédelmi rendelet 32. cikkével összhangban az adatkezelőként vagy adatfeldolgozóként eljáró adatimportőrrel Ön már rendelkezett ilyen intézkedésekről.

<sup>56</sup> Az Ön és az adatimportőr által felhasználható információforrások nem kimerítő felsorolását illetően lásd a 3. mellékletet.

**Releváns:** az információknak relevánsnak kell lenniük a konkrét adattovábbítás és/vagy adatimportőr, valamint az uniós jogban és az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben meghatározott követelményeknek való megfelelés szempontjából, és nem lehetnek túlzottan általánosak vagy elvontak.

**Objektív információk:** olyan információk, amelyeket a múltban szerzett ismereteken alapuló empirikus bizonyítékok támasztanak alá, nem pedig lehetséges eseményekre és kockázatokra vonatkozó feltételezések.

**Megbízható:** az adatexportőrnek és az adatimportőrnek objektíven értékelnie kell az információforrásnak és magának az információnak a megbízhatóságát, és azokat külön kell értékelnie.

**Ellenőrizhető:** az információknak és következtetéseknek az átfogó értékelés részeként ellenőrizhetőnek vagy más típusú információkkal vagy forrásokkal szembeállíthatónak kell lenniük többek között azért, hogy az illetékes felügyeleti vagy igazságügyi hatóság szükség esetén ellenőrizhesse ezen információk objektivitását és megbízhatóságát.

**Nyilvánosan elérhető vagy egyéb módon hozzáférhető információk:** az információknak lehetőleg nyilvánosnak vagy legalább hozzáférhetőnek kell lenniük a fenti kritériumok ellenőrzésének megkönnyítése és a felügyeleti hatóságokkal, az igazságügyi hatóságokkal és végső soron az érintettekkel való lehetséges megosztásuk biztosítása érdekében.

47. Ön figyelembe veheti továbbá az adatimportőrnek a harmadik ország hatóságaitól kapott hozzáférésre irányuló felhívások korábbi releváns eseteivel kapcsolatos dokumentált gyakorlati tapasztalatait is. Ön csak akkor lesz képes további információforrásként felhasználni az adatimportőr tapasztalatait, ha a harmadik ország jogi kerete nem tiltja az adatimportőr számára, hogy információkat szolgáltasson a hatóságok közlésre irányuló felhívásairól vagy azok hiányáról (és ezt az értékelést Önnek dokumentálnia is kell). Figyelembe kell azonban vennie, hogy az a körülmény, hogy az adatimportőr korábban nem kapott felhívásokat, önmagában soha nem tekinthető olyan döntő tényezőnek az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz hatékonysága szempontjából, amely lehetővé teszi a kiegészítő intézkedések nélküli adattovábbítást. Ezeket az információkat az egyéb forrásokból származó más típusú információkkal együtt figyelembe veheti a harmadik ország jogszabályainak és gyakorlatainak az Ön által végzett adattovábbítással kapcsolatos átfogó értékelésének részeként. Az adatimportőr releváns és dokumentált tapasztalatait meg kell erősíteni, és azoknak nem mondhatnak ellent a vonatkozó jogszabályok gyakorlati alkalmazására vonatkozó releváns, objektív, megbízható, ellenőrizhető és nyilvánosan elérhető vagy egyéb módon hozzáférhető információk (pl. az ugyanazon ágazatban működő és/vagy hasonló továbbított személyes adatokhoz kötődő más szereplők által kapott hozzáférésre irányuló felhívások megléte vagy hiánya<sup>57</sup> és/vagy a jog gyakorlati alkalmazása, például az ítélkezési gyakorlat és független felügyeleti szervek jelentései).

---

<sup>57</sup> A tapasztalat lehet más olyan szervezetek tapasztalata is, amelyeket Ön közvetlenül ismer az Ön által végzett korábbi, hasonló jellegű adattovábbítások miatt, vagy olyan tapasztalat is, amelyről a vonatkozó ítélkezési gyakorlat, nem kormányzati szervezetek jelentései stb. (lásd a 3. mellékletet) számolnak be.

### *Az Ön által elvégzett értékelés eredményei*

48. Önnek kellő gondossággal kell elvégeznie az adatimportőrje harmadik országának az Ön által végzett adattovábbításra alkalmazandó jogának és gyakorlatának ezt az átfogó értékelését, és azt alaposan dokumentálnia kell. Az illetékes felügyeleti és/vagy igazságügyi hatóságok kérhetik ezt, és elszámoltathatják Önt az ez alapján hozott bármely döntésért<sup>58</sup>.
49. Az Ön értékelése végső soron feltárhatja, hogy az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszköz:
- hatékonyan biztosítja, 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 adatimportőr 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); vagy
  - nem biztosítja hatékonyan a lényegében azonos védelmi szintet. Az adatimportőr a harmadik ország adattovábbításra vonatkozó jogszabályai és/vagy gyakorlatai miatt nem tud eleget tenni kötelezettségeinek, mivel azok nem felelnek meg az alapvető jogokra és szabadságokra vonatkozó uniós előírásoknak, valamint azok jogszerű közérdekű célok védelme érdekében történő korlátozása szükségességének és arányosságának. Az EUB hangsúlyozta, hogy amennyiben az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök nem megfelelőek, az adatexportőr felelőssége, hogy hatékony kiegészítő intézkedéseket hozzon, vagy hogy ne továbbítsa a személyes adatokat.<sup>59</sup>

#### **Példa:**

##### Háttér:

Az EUB megállapította, 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.

##### Értékelés:

Ha Ön a vonatkozó egyesült államokbeli jogszabályok értékelése alapján úgy ítéli meg, hogy az Ön által végzett adattovábbítás a FISA 702. szakaszának hatálya alá tartozhat, de bizonytalan abban, hogy az a gyakorlati alkalmazási körébe tartozik-e, a következőképpen dönthet:

1. leállítja az adattovábbítást;
2. olyan megfelelő kiegészítő intézkedéseket fogad el, amelyek hatékonyan biztosítják a továbbított adatok védelmének az EGT-ben biztosított védelmi szinttel lényegében azonos szintjét; vagy
3. más objektív, megbízható, releváns, ellenőrizhető és lehetőleg nyilvánosan elérhető információkat (amelyek az adatimportőrje által az Ön rendelkezésére bocsátott információkat is magukban

<sup>58</sup> Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése.

<sup>59</sup> Az EUB „Schrems II” ítélete (C-311/18), 134. és 135. pont.

foglalhatnak) vizsgál meg annak érdekében, hogy pontosítsa a FISA 702. szakaszának az Ön konkrét adattovábbításával kapcsolatos gyakorlati alkalmazási körét. Ezen információknak választ kell adniuk néhány releváns kérdésre, például a következőkre:

- Azt mutatják-e a nyilvánosan elérhető információk, hogy jogszabály tiltja a kapott adatokhoz való hozzáférésre irányuló konkrét felhívásról való tájékoztatást, és széles körű korlátozások vonatkoznak a kapott adatokhoz való hozzáférésre irányuló felhívásokkal vagy a kapott felhívások hiányával kapcsolatos általános tájékoztatásra?

- Megerősítette-e az Ön adatimportőrje, hogy korábban adatokhoz való hozzáférésre irányuló felhívásokat kapott az Egyesült Államok hatóságaitól? Vagy megerősítette-e az Ön adatimportőrje, hogy korábban nem kapott adatokhoz való hozzáférésre irányuló felhívásokat az Egyesült Államok hatóságaitól, és hogy nem tilos számára tájékoztatást nyújtani az ilyen felhívásokról vagy azok hiányáról?

- Azt mutatják-e az Egyesült Államok ítélkezési gyakorlatáról Ön által beszerzett nyilvánosan elérhető információk, valamint a felügyeleti szervek, civil társadalmi szervezetek és tudományos intézmények<sup>60</sup> jelentései, hogy az Ön adatimportőrével azonos ágazatban működő adatimportőrök korábban adatokhoz való hozzáférésre irányuló felhívásokat kaptak hasonló továbbított adatokkal kapcsolatban?

Az e kérdésekre az átfogó értékelés során kapott válaszok alapján az alábbi következtetésre jut:

- A FISA 702. szakasza alkalmazandó a gyakorlatban az Ön konkrét adattovábbítására, és ezért hatással van az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz hatékonyságára. Következésképpen, ha Ön folytatni kívánja az adattovábbítást, mérlegelnie kell – adott esetben az adatimportőrrel együttműködve –, hogy el tud-e fogadni olyan kiegészítő intézkedéseket, amelyek hatékonyan biztosítják a továbbított adatok védelmének az EGT-ben biztosított védelmi szinttel lényegében azonos szintjét. Ha nem talál hatékony kiegészítő intézkedéseket, nem továbbíthatja a személyes adatokat.

Vagy:

- A FISA 702. szakasza nem alkalmazandó a gyakorlatban az Ön konkrét adattovábbítására, és ezért nincs hatással az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz hatékonyságára. Ebben az esetben kiegészítő intézkedések nélkül is elvégezheti az adattovábbítást.

---

<sup>60</sup> Pl. a FISA 702. szakaszának rendelkezései; a Foreign Intelligence Surveillance Court (hírszerzési felügyeleti bíróság, FISC) eljárási szabályzata, a FISC feloldott minősítésű véleményei és határozatai, az Egyesült Államok bíróságainak ítélkezési gyakorlata; a Privacy and Civil Liberties Oversight Board (adatvédelmi és polgári szabadságjog felügyeleti tanács, PCLOB) jelentései és meghallgatási jegyzőkönyvei; az Office of the Inspector General – U.S. Department of Justice (főellenőri iroda – az Egyesült Államok igazságügyi minisztériuma) jelentései; az NSA Director of Civil Liberties and Privacy Office (az NSA alapvető szabadságjogok és magánélet védelméért felelős irodájának igazgatója) jelentései; a Congressional Research Service (kongresszusi kutatószolgálat) által készített jelentések; az American Civil Liberties Union Foundation (Amerikai Polgárjogi Unió alapítvány, ACLU) jelentései.

## 2.4 4. lépés: Fogadjon el kiegészítő intézkedéseket

50. 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 adatimportőrrel együttműködve – meg kell vizsgálnia, hogy léteznek-e olyan kiegészítő 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.<sup>61</sup> A „kiegészítő intézkedések” jellegüknél fogva kiegészítik az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben már előírt garanciákat és az általános adatvédelmi rendeletben meghatározott minden egyéb alkalmazandó biztonsági követelményt (pl. technikai biztonsági intézkedések).<sup>62</sup>
51. Eseti alapon meg kell állapítania, hogy az általános adatvédelmi rendelet 46. cikke szerinti konkrét adattovábbítási eszköz használata esetén milyen kiegészítő intézkedések lehetnek hatékonyak egy adott harmadik országba irányuló adattovábbítások esetében. Nem kell megismételnie az értékelést minden olyan esetben, amikor ugyanazon harmadik országba azonos módon továbbít meghatározott típusú adatokat. A továbbításra szánt adatok némelyike kiegészítő intézkedéseket tehet szükségessé, más adatok pedig nem (figyelembe véve a harmadik ország jogának formális és/vagy gyakorlati alkalmazását). A fenti 1., 2. és 3. lépésben elvégzett korábbi értékelései és következtetései alapján ellenőrizheti, hogy a kiegészítő intézkedések mennyire hatékonyak a szükséges védelmi szint biztosítása szempontjából.
52. A kiegészítő 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.
53. A szerződéses és szervezési intézkedések önmagukban általában nem akadályozzák meg a harmadik országbeli hatóságok személyes adatokhoz problematikus jogszabályok és/vagy gyakorlatok<sup>63</sup> alapján való hozzáférést. Lesznek ugyanis olyan helyzetek, amelyekben csak megfelelően végrehajtott technikai intézkedések akadályozhatják meg vagy tehetik hatástalanná a harmadik országbeli hatóságok személyes adatokhoz való – különösen megfigyelési célú – hozzáférést.<sup>64</sup> Ilyen helyzetekben a szerződéses vagy szervezési intézkedések kiegészíthetik a

---

<sup>61</sup> „Schrems II” ítélet (C-311/18), 96. pont.

<sup>62</sup> Az általános adatvédelmi rendelet (109) preambulumbekzdése és a „Schrems II” ítélet (C-311/18) 133. pontja.

<sup>63</sup> A „problematikus jogszabályok” alatt olyan jogszabályok értendők, amelyek 1) olyan kötelezettségeket írnak elő az Európai Unióból származó személyes adatok továbbításának címzettjével szemben, és/vagy olyan hatást gyakorolnak a továbbított adatokra, amelyek, illetve amely megkérdőjelezheti a lényegében azonos védelmi szint adattovábbítási eszközökben foglalt szerződéses garanciáját, és 2) nem tartják tiszteletben az Európai Unió Alapjogi Chartája által elismert alapvető jogok és szabadságok lényeges tartalmát, vagy túllépi az uniós jogban vagy az uniós tagállamok jogában is elismert – az általános adatvédelmi rendelet 23. cikkének (1) bekezdésében felsoroltakhoz hasonló – fontos célkitűzések valamelyikének védelméhez egy demokratikus társadalomban szükséges és arányos mértéket.

<sup>64</sup> 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->



technikai intézkedéseket, és növelhetik az adatvédelem általános szintjét (például azáltal, hogy ellenőrzéseket vezetnek be, és kiküszöbölik az automatizmusokat a hatóságok arra irányuló kísérletei esetében, hogy az uniós előírásokkal összeegyeztethetetlen módon férjenek hozzá az adatokhoz).

54. Adott esetben az adatimportőrrel együttműködve megvizsgálhatja az alábbi (nem kimerítő jelleggel felsorolt) tényezőket annak megállapításához, hogy milyen kiegészítő intézkedések lennének a leghatékonyabbak a továbbított adatoknak a hatóságok gyakorlatban alkalmazott problematikus jogszabályokon alapuló, adatokhoz való hozzáférésre irányuló felhívásaival szembeni védelme szempontjából:

- a továbbítandó adatok formátuma (például egyszerű szöveg/álnevesített vagy titkosított);
- az adatok jellege (pl. az EGT-ben magasabb szintű védelemben részesülnek az általános adatvédelmi rendelet 9. és 10. cikkének hatálya alá tartozó adatkategóriák)<sup>65</sup>;
- 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 adatimportőréhez továbbítják [figyelembe véve a célországoknak számító harmadik ország jogszabályai szerint rájuk alkalmazandó vonatkozó rendelkezéseket]);<sup>66</sup>
- a harmadik ország joga gyakorlati alkalmazásának a 3. lépésben megállapított technikája vagy paraméterei;
- annak lehetősége, hogy az adatok ugyanazon harmadik országon belül vagy akár más harmadik országok irányába is újbóli továbbítás tárgyát képezhetik (például az adatimportőr további adatfeldolgozóinak bevonása<sup>67</sup>).

#### Példák kiegészítő intézkedésekre

55. A 2. mellékletben foglalt, nem kimerítő felsorolások bemutatnak néhány példát a figyelembe vehető technikai, szerződéses és szervezési intézkedésekre, amennyiben azokat nem foglalja eleve magában az általános adatvédelmi rendelet 46. cikke alapján alkalmazott adattovábbítási eszköz.

\*\*\*

---

tools/our-documents/recommendations/edpb-recommendations-022020-european-essential\_hu.  
[https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en).

<sup>65</sup> Lásd a 42. lábjegyzetet.

<sup>66</sup> 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.

<sup>67</sup> Lásd a 26. lábjegyzetet.

56. Ha olyan hatékony kiegészítő 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.
57. Amennyiben nem talál, vagy nem hajt végre olyan hatékony kiegészítő intézkedéseket, amelyek biztosítják, hogy a továbbított személyes adatok lényegében azonos szintű védelemben részesüljenek,<sup>68</sup> 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 szüntetnie a személyes adatok továbbítását.<sup>69</sup> Az általános adatvédelmi rendelet 46. cikke szerinti, Ön által igénybe vett adattovábbítási eszközben foglalt garanciáknak megfelelően az adatimportőrnek 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.<sup>70</sup>

**Példa:**

Példa: a harmadik ország joga tiltja az Ön által azonosított kiegészítő 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.

58. 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 kiegészítő intézkedések azonosítása esetén

59. 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 kiegészítő intézkedéseket azonosított.

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

60. Amennyiben Ön kiegészítő 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 kiegészítő intézkedések sem közvetlen, sem közvetett módon nem

---

<sup>68</sup> 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\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en).

<sup>69</sup> „Schrems II” ítélet (C-311/18), 135. pont.

<sup>70</sup> Lásd például 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.

ellentétesek az SCC-kkel, és elegendőek annak biztosításához, hogy az általános adatvédelmi rendelet által biztosított védelmi szint ne sérüljön.<sup>71</sup> Az adatexportőrnek és az adatimportőrnek biztosítania kell, hogy a további kikötéseket semmiképpen ne lehessen úgy értelmezni, hogy korlátozzák az SCC-kben foglalt jogokat és kötelezettségeket, vagy bármilyen más módon csökkentse 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).

61. Ha módosítani kívánja magukat az általános adatvédelmi kikötéseket, vagy ha a hozzáadott kiegészítő intézkedések közvetlen vagy közvetett módon „ellentétesek” az SCC-kkel, akkor már nem tekinthető úgy, hogy Ön általános szerződési feltételekre támaszkodik<sup>72</sup>, 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)

62. 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.<sup>73</sup>
63. 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.

---

<sup>71</sup> Az általános adatvédelmi rendelet (109) preambulumbekzdése 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 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.

<sup>72</sup> 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\\_art28scs\\_si\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28scs_si_en.pdf).

<sup>73</sup> Az EUB „Schrems II” ítélete (C-311/18), 132. pont.

64. Minden beillesztendő kötelezettségvállalásra hivatkozni fognak az aktualizált WP256/257 referenciadokumentumok<sup>74</sup>, amelyekkel valamennyi, adattovábbítási eszközként BCR-eket igénybe vevő csoportnak összhangba kell hoznia meglévő és jövőbeli BCR-eit.
65. A Bíróság kiemelte, hogy az adatexportőr és az adatimportőr 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 kell, hogy tud-e kiegészítő intézkedéseket hozni a védelem EGT-ben biztosított lényegében azonos szintjének biztosítása érdekében, és hogy a harmadik ország joga vagy gyakorlata nem fogja-e megsérteni ezeket a kiegészítő intézkedéseket azok hatékonyságának megakadályozása érdekében.

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

66. 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.<sup>75</sup> 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.

## 2.6 6. lépés: Végezzen újraértékelést megfelelő időközönként

67. Önnek – adott esetben az adatimportőrökkel 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).
68. Kellően megbízható mechanizmusokat kell bevezetnie annak biztosítására, hogy az adattovábbításokat haladéktalanul felfüggeszti vagy megszünteti, ha:
- az adatimportőr megszegte vagy nem tudja teljesíteni az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben vállalt kötelezettségeit;
  - a kiegészítő intézkedések már nem hatékonyak az érintett harmadik országban.

---

<sup>74</sup> 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.

<sup>75</sup> Az EUB „Schrems II” ítélete (C-311/18), 132. pont.

### 3 KÖVETKEZTETÉS

69. 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.<sup>76</sup>
70. Adatai lényegében azonos szintű védelmének biztosítása érdekében Önnek mindenképp alaposan ismernie kell az Ön által végzett adattovábbításokat. Azt is ellenőriznie kell, hogy az Ön által továbbított adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak-e, és a szükségesre korlátozódnak-e.
71. 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 célszágnak 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 kiegészítő intézkedésekkel pótolhatók.
72. Amennyiben nem talál, vagy nem hajt végre olyan hatékony kiegészítő 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.
73. 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)

---

<sup>76</sup> „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.
- „Adatexportőr”: az EGT-n belüli adatkezelő vagy adatfeldolgozó, aki személyes adatokat továbbít egy harmadik országbeli adatkezelő vagy adatfeldolgozó részére.
- „Adatimportőr”: 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 adatexportőröknek 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 KIEGÉSZÍTŐ INTÉZKEDÉSEKRE

74. Az alábbi intézkedések példák olyan kiegészítő intézkedésekre, amelyeket a 4. lépés („Fogadjon el kiegészítő intézkedéseket”) során fontolóra vehet. Ez a felsorolás nem kimerítő. Más kiegészítő intézkedéseket is megvizsgálhat. A jövőbeli technológiai, jogi vagy szervezeti fejlemények olyan új kiegészítő intézkedések megjelenéséhez vezethetnek, amelyeket mérlegelni kell. 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 kiegészítő intézkedéseket kell kiválasztania, amelyek hatékonyan képesek biztosítani az ilyen védelmi szintet az Ön által végzett adattovábbítások tekintetében.
75. Bármely további intézkedés csak akkor és annyiban tekinthető hatékonnak az EUB „Schrems II” ítélete értelmében, ha és amennyiben – önmagában vagy más intézkedésekkel együtt – orvosolja a harmadik országban fennálló helyzet értékelése során a harmadik országnak az Ön által végzett adattovábbításra alkalmazandó jogszabályait és gyakorlatait illetően feltárt konkrét hiányosságokat. Ha Ön végső soron nem tud lényegében azonos védelmi szintet biztosítani, nem továbbíthatja a személyes adatokat.
76. Előfordulhat, hogy adatkezelőként vagy adatfeldolgozóként Ön már köteles a jelen mellékletben ismertetett intézkedések némelyikének végrehajtására az általános adatvédelmi rendeletnek való megfelelés érdekében. Ez azt jelenti, hogy adott esetben hasonló intézkedéseket kell bevezetni az EGT-ben kezelt, a megfelelési határozat hatálya alá tartozó adatimportőrnek vagy más harmadik országokba továbbított személyes adatok tekintetében.<sup>77</sup>

### 2.1 Technikai intézkedések

77. 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 adatimportőrrel 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 hozzáféréssel szembeni lényegében azonos szintű védelem szerződéses garanciáját<sup>78</sup>.
78. A fokozott egyértelműség érdekében ez a szakasz először néhány olyan foratókönyvet ismertet, amelyek esetében egyes technikai intézkedések potenciálisan hatékonyak lehetnek a lényegében azonos védelmi szint biztosításában. A szakasz néhány olyan foratókönyvvel folytatódik, amelyek esetében nem került sor azon technikai intézkedések azonosítására, amelyek biztosítanák ezt a védelmi szintet.

---

<sup>77</sup> Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése és 32. cikke.

<sup>78</sup> „Schrems II” ítélet (C-311/18), 135. pont.

---

Példák olyan esetekre vonatkozó forgatókönyvekre, amelyekben *hatékony* intézkedések azonosítására került sor

---

79. 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 szükségesek az EGT-ben biztosítottal lényegében azonos védelmi szint biztosításához, ha a hatóságok hozzáférése megfelel az adatimportőr országa jogának, amennyiben a hozzáférés a gyakorlatban meghaladja a demokratikus társadalomban szükséges és arányos mértéket<sup>79</sup>. 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.
80. A harmadik országok hatóságai megpróbálhatnak hozzáférni a továbbított adatokhoz
- 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.
  - 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 nyerve ki az érdeklődésre számot tartó adatokat, majd adja át azokat a hatóságoknak.
81. Ez a szakasz azokat a forgatókönyveket vizsgálja, amelyekben mindkét esetben hatékony intézkedések alkalmazására kerül sor. A konkrét adattovábbítás adott körülményei között különböző kiegészítő intézkedések lehetnek alkalmazhatók és megfelelőek, ha a fogadó ország joga csak egyfajta hozzáférést ír elő. Ezért az adatexportőrnek – az adatimportőr támogatásával – gondosan elemeznie kell az adatimportőrre vonatkozó kötelezettségeket.

Például az USC 50. címe 1881a. §-ának (a FISA 702. szakaszának) hatálya alá tartozó egyesült államokbeli adatimportőröket 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.

---

<sup>79</sup> 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.



82. A forgatókönyvek ismertetik a konkrét körülményeket és a meghozott intézkedéseket, hogy példaként szolgáljanak. A forgatókönyvek bármilyen változása eltérő eredményekhez vezethet. A forgatókönyvek olyan helyzetekre vonatkoznak, amelyekben arra a következtetésre jutottak, hogy elsősorban kiegészítő intézkedésekre van szükség, azaz amelyekben a gyakorlatban a harmadik ország problematikus jogszabályait alkalmazzák a szóban forgó adattovábbításra.
83. Előfordulhat, hogy az adatkezelőknek az adatimportőrre 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 adatexportőrök kötelesek a jelen dokumentumban ismertetett intézkedések végrehajtására, még akkor is, ha az adatimportőrök 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.

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

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

Ha

1. a személyes adatokat továbbítás előtt erős titkosítás alkalmazásával kezelik, és ellenőrizték az adatimportőr személyazonosságát,
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)<sup>80</sup>,
3. a titkosítás erőssége és a kulcs hossza figyelembe veszi azt a konkrét időtartamot, amely alatt a titkosított személyes adatok titkosságát meg kell őrizni<sup>81</sup>,

---

<sup>80</sup> A titkosítási algoritmusok erősségének, lehető legkorszerűbb jellegüknek, valamint a rejtjelelemzéssel szembeni időbeli megbízhatóságuknak az értékelése során az adatexportőrök támaszkodhatnak az Unió és tagállamai hivatalos kiberbiztonsági hatóságai által közzétett technikai iránymutatásokra. Lásd például: az ENISA „What is »state of the art« in IT security?” („Mi minősül a »lehető legkorszerűbbnek« az informatikai biztonság területén?”) című jelentése, 2019, <https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security>; a német szövetségi információbiztonsági hivatal iránymutatása a TR-02102 sorozat technikai iránymutatásaiban, valamint „Algorithms, Key Size and Protocols Report (2018) (Algoritmusok, kulcsméret és protokollok jelentés [2018]), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018” az alábbi internetes oldalon: <https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>.

<sup>81</sup> A kriptográfiai algoritmusok védelmi kapacitása idővel csökken új rejtjelfejtési technikák felfedezése, új számítástechnikai paradigmák – mint például a kvantum-számítástechnika – megjelenése, valamint a rendelkezésre álló számítási teljesítmény általános növekedése miatt, kivéve, ha az alkalmazott algoritmusok információelméletileg biztonságosnak bizonyulnak. Ez az aggály különösen a jelen dokumentum elkészítésének időpontjában általánosan használt nyilvános kulcsú algoritmusokra vonatkozik. Következésképpen az adatexportőrnek figyelembe kell vennie, hogy a hatóságok a 80. pontban ismertetett körülmények között hozzáférhetnek a titkosított adatokhoz, és azokat addig tárolhatják, amíg erőforrásaik elegendőek nem lesznek

4. a titkosítási algoritmust hibátlanul hajtja végre egy megfelelően karbantartott és ismert sebezhetőségek nélküli 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)<sup>82</sup>, valamint
6. a kulcsokat kizárólag az adatexportőr ellenőrzése mellett őrzik meg, vagy azokat az adatexportőr által megbízott, az EGT-ben letelepedett vagy az EGT-ben biztosítottal lényegében azonos védelmi szintet nyújtó joghatóság szerinti szervezet őrzi meg,

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

## 2. alkalmazási eset: Álnevesített adatok továbbítása

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

Ha

1. az adatexportőr 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<sup>83</sup>,
2. az említett további információkat kizárólag az adatexportőr birtokolja, és azokat külön tárolja egy tagállamban vagy egy harmadik országban az adatexportőr által megbízott, az EGT-ben letelepedett vagy az EGT-ben biztosítottal lényegében azonos védelmi szintet nyújtó joghatóság szerinti szervezet,
3. e további információk közlését vagy jogosulatlan felhasználását megfelelő technikai és szervezési garanciák révén megakadályozzák, és biztosított, hogy az adatexportőr 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 várhatóan rendelkeznek, és amelyet várhatóan használnak– megállapította, hogy az álnevesített személyes adatok akkor sem

---

a visszafejtéshez. A további intézkedés csak akkor tekinthető hatékonynak, ha az ilyen visszafejtés és az azt követő további adatkezelés ebben az időpontban már nem jelenti az érintettek jogainak megsértését, például mert az adatok már nem használhatók fel közvetlen vagy közvetett módon történő azonosításukra.

<sup>82</sup> NIST különleges kiadás 800-57, Recommendation for Key Management (A kulcskezelésre vonatkozó ajánlás) <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>

<sup>83</sup> Az általános adatvédelmi rendelet 4. cikkének 5. bekezdése 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”. A további adatok tartalmazhatnak olyan táblázatokat, amelyek az álneveket az általuk helyettesített azonosító jellegzetességekkel, kriptográfiai kulcsokkal vagy a jellegzetességek átalakítására szolgáló egyéb paraméterekkel kapcsolják össze, vagy más olyan adatokat, amelyek lehetővé teszik az álnevesített adatok azonosított vagy azonosítható természetes személyekhez való hozzárendelését.

kapcsolhatók egy azonosított vagy azonosítható természetes személyhez, ha azokat összevetik az említett információkkal,

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

86. 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<sup>84</sup> lehetővé teheti az adott személy azonosítását még akkor is, ha nevét, címét vagy más egyszerű azonosítóját nem tüntetik fel.
87. 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.
88. 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.
89. Ha az álnevesítés során a személyes adatokban szereplő jellegzetességeket kriptográfiai algoritmus segítségével alakítják át, akkor a 80. és 81. lábjegyzetben szereplő útmutatást kell alkalmazni. A jövőben ajánlatos lemondani a kriptográfia kizárólagos használatáról és táblázatos megfeleltetési mechanizmusokon alapuló átalakításokat alkalmazni.

### 3. alkalmazási eset: Az adatok titkosítása annak érdekében, hogy az adatimportőr harmadik országának hatóságai ne férjenek hozzájuk az adatexportőr és az adatimportőr közötti továbbításuk során

90. Az adatexportőr olyan célállomásra kíván adatokat továbbítani, ahol a jogszabályok és/vagy gyakorlatok lehetővé teszik, hogy a hatóságok hozzáférjenek az adatokhoz azoknak az adatexportőr országa és a célország közötti továbbítása során.

Ha

1. az adatexportőr olyan joghatóság alá tartozó adatimportőrnek továbbít személyes adatokat, ahol a jog és/vagy a gyakorlat lehetővé teszi, hogy a hatóságok hozzáférjenek az adatokhoz azoknak az interneten keresztül e harmadik országba történő továbbítása során az e hozzáférésre vonatkozó alapvető európai garanciák nélkül, olyan adattovábbítási titkosítást alkalmaznak, amelynek tekintetében biztosított, hogy az alkalmazott titkosítási protokollok a

---

<sup>84</sup> Az általános adatvédelmi rendelet 4. cikkének 1. bekezdése 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”.

lehető legkorszerűbbek, és hatékony védelmet nyújtsanak az e harmadik ország hatóságai számára ismertén rendelkezésre álló erőforrásokkal végrehajtott aktív és passzív támadásokkal szemben,

2. a kommunikációban részt vevő felek megbízható, nyilvános kulcsú tanúsító hatóságról vagy infrastruktúráról állapotnak meg,
3. az adattovábbítási titkosítást biztosító küldő és fogadó rendszerek elleni aktív és passzív támadásokkal szemben konkrét védelmi és a technika állásának megfelelő intézkedéseket alkalmaznak, ideértve a szoftverek sebezhetőségének és az esetleges hátsó ajtóknak a tesztelését is.
4. 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,
5. a titkosítási algoritmus és annak paraméterezése (például a kulcs hossza, adott esetben működési módja) a lehető legkorszerűbb, és a hatóságok által az adatok e harmadik országba történő továbbítása során végzett rejtjelelemzéssel szemben megbízhatónak tekinthető, figyelembe véve a rendelkezésükre álló erőforrásokat és műszaki lehetőségeket (például a próbálgatásos támadásokhoz szükséges számítástechnikai teljesítmény) (lásd a fenti 80. lábjegyzetet),<sup>85</sup>
6. a titkosítás erőssége figyelembe veszi azt a konkrét időtartamot, amely alatt a titkosított személyes adatok titkosságát meg kell őrizni,
7. a titkosítási algoritmust hibátlanul hajtja végre egy megfelelően karbantartott és ismert sebezhetőségek nélküli szoftver, amelynek a választott algoritmus specifikációjának való megfelelését ellenőrizték, például tanúsítással,
8. a kulcsokat megbízhatóan kezeli (hozza létre, adminisztrálja, – adott esetben – tárolja, kapcsolja össze a szándékolt címzett személyazonosságával, és vonja vissza) az adatexportőr vagy egy, az adatexportőr 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

91. Az adatexportőr személyes adatokat továbbít az ezen ország joga által kifejezetten védett harmadik országbeli adatimportőr 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 adatimportőrt az e címzett birtokában lévő adatokhoz az adott célból való potenciálisan jogsértő hozzáférés alól, például az adatimportőrre vonatkozó szakmai titoktartási kötelezettség alapján,

---

<sup>85</sup> Lásd a 80. lábjegyzetet az Unió és tagállamai hivatalos kiberbiztonsági hatóságai által közzétett technikai iránymutatásokra vonatkozó néhány példáért.

2. ez a mentesség az adatimportőr birtokában lévő minden olyan információra kiterjed, amely felhasználható bizalmas információk védelmének megkerüléséhez (kriptográfiai kulcsok, jelszavak, egyéb hitelesítő adatok stb.),
3. az adatimportőr nem veszi igénybe adatfeldolgozó szolgáltatásait olyan módon, amely lehetővé teszi, hogy a hatóságok hozzáférjenek az adatfeldolgozó birtokában lévő adatokhoz, és az adatimportőr nem továbbítja az adatokat egy másik, az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközök alapján nem védett jogalanyra 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 adatimportőrnek és – esetlegesen – magának az adatexportőrnek vagy az adatexportőr által megbízott, az EGT-ben található vagy az EGT-ben biztosítottal lényegében azonos védelmi szintet nyújtó joghatóság szerinti másik szervezetnek a kizárólagos megőrzésében van, és azt a legkorszerűbb technikai és szervezési intézkedésekkel megfelelően védik a jogosulatlan felhasználással vagy közléssel szemben, és
6. az adatexportőr 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

92. Az adatexportőr 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 adatexportőr 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 adatexportőr 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. az adatkezelő a szóban forgó adatok alapos elemzésével, figyelembe véve azokat a hiányzó információdarabokat, amelyekkel a fogadó országok hatóságai várhatóan rendelkeznek, és amelyeket várhatóan használnak, megállapította, hogy az adatfeldolgozók részére általa továbbított személyesadat-darabok akkor sem kapcsolhatók egy azonosított vagy azonosítható természetes személyhez, ha azokat összevetik az említett információkkal,

6. 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.

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

---

### Példák olyan esetekre vonatkozó forgatókönyvekre, amelyekben *hatékony* intézkedések azonosítására nem került sor

---

93. Az alábbiakban ismertetett intézkedések bizonyos forgatókönyvek esetében nem biztosítanak hatékonyan a harmadik országba továbbított adatok lényegében azonos szintű védelmét. Ezért azok nem minősülnének megfelelő kiegészítő intézkedéseknek.

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

94. Az adatexportőr személyes adatokat továbbít – akár elektronikus továbbítás, akár felhőszolgáltató vagy más adatfeldolgozó rendelkezésére bocsátásuk útján –, hogy a személyes adatokat utasításainak megfelelően egy harmadik országban kezeljék (pl. technikai segítségnyújtás vagy bármilyen típusú felhőalapú feldolgozás céljából), és ezeket az adatokat nem álnevesítették – illetve nem lehet álnevesíteni – a 2. alkalmazási esetben leírtak szerint, vagy nem titkosították – illetve nem lehet titkosítani – az 1. alkalmazási esetben leírtak szerint, mert az adatkezeléshez kódolatlan adatokhoz való hozzáférésre van szükség,

Ha

1. az adatkezelő személyes 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 szóban forgó továbbított adatokhoz való hozzáférés tekintetében biztosított hatáskör meghaladja a demokratikus társadalomban szükséges és arányos mértéket, ha a gyakorlatban a harmadik ország problematikus jogszabályait kell alkalmazni a szóban forgó adattovábbításokra (lásd a 3. lépést).<sup>86</sup>

akkor az Európai Adatvédelmi Testület a technika állását figyelembe véve nem tud elképzelni olyan hatékony technikai intézkedést, amely megakadályozná, hogy a hozzáférés sértse az érintett alapvető

---

<sup>86</sup> 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.

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.

95. 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 adatimportőr rendelkezik a kriptográfiai kulcsokkal.

#### 7. alkalmazási eset: Személyes adatok üzleti célokból – többek között távoli hozzáférés útján – történő továbbítása

96. Az adatexportőr személyes adatokat továbbít harmadik országbeli jogalanyoknak közös üzleti célokra történő felhasználás céljából – akár elektronikus továbbítás, akár az adatimportőr általi távoli hozzáférésre történő rendelkezésre bocsátásuk útján –, és ezeket az adatokat nem álnevesítették – illetve nem lehet álnevesíteni – a 2. alkalmazási esetben leírtak szerint, vagy nem titkosították – illetve nem lehet titkosítani – az 1. alkalmazási esetben leírtak szerint, mert az adatkezeléshez kódolatlan adatokhoz való hozzáférésre van szükség. 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 adatimportőr felhasználhatja a kapott adatokat például arra, hogy az adatexportőr számára olyan személyzeti szolgáltatásokat nyújtson, amelyekhez humánerőforrás-adatokra van szüksége, vagy arra, hogy telefonon vagy e-mailben kommunikáljon az adatexportőr Európai Unióban élő ügyfeleivel.

Ha

1. az adatexportőr személyes adatokat továbbít egy harmadik országbeli adatimportőr részére ezen adatoknak egy információs rendszerben olyan módon történő hozzáférhetővé tétele révén, amely lehetővé teszi az adatimportőr számára a saját választása szerinti adatokhoz való közvetlen hozzáférést, vagy ezen adatok hírközlési szolgáltatás igénybevételével közvetlenül, egyedileg vagy ömlesztve történő továbbítása révén,
2. az adatimportőr<sup>87</sup> a kódolatlan adatokat a harmadik országban kezeli (ideértve a saját céljaira történő adatkezelést is, ha az adatimportőr adatkezelőnek minősül),
3. a fogadó ország hatóságai számára a továbbított adatokhoz való hozzáférés tekintetében biztosított hatáskör meghaladja a demokratikus társadalomban szükséges és arányos mértéket, ha a gyakorlatban a harmadik ország problematikus jogszabályait kell alkalmazni a szóban forgó adattovábbításokra (lásd a 3. lépést),

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

---

<sup>87</sup> Az EGT-ből továbbított személyes adatokat fogadó vagy azokhoz hozzáférést kapó harmadik országbeli adatkezelő vagy adatfeldolgozó.

97. 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 adatimportőr rendelkezik a kriptográfiai kulcsokkal.

## 2.2 További szerződéses intézkedések

98. Ezek az intézkedések általában egyoldalú, kétoldalú vagy többoldalú<sup>88</sup> szerződéses kötelezettségvállalásokból állnak.<sup>89</sup> Az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszköz alkalmazása esetén az a legtöbb esetben már tartalmazza az adatexportőr és az adatimportőr számos (többnyire szerződéses) kötelezettségvállalását, amelyek célja, hogy garanciaként szolgáljanak a személyes adatok tekintetében.<sup>90</sup>
99. Bizonyos helyzetekben ezek az intézkedések kiegészíthetők és megerősíthetők 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 EGT-ben 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<sup>91</sup>, ezeket az intézkedéseket gyakran egyéb technikai és szervezési intézkedésekkel kell kombinálni a szükséges adatvédelmi szint biztosítása érdekében. 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.
100. 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 adatexportőrök tudomást szerezzenek a harmadik országokba továbbított adatok védelmét érintő új fejleményekről.
101. 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 adatimportőröket, hogy tegyenek eleget a hatóságoktól kapott, adatközlést elrendelő határozatoknak.<sup>92</sup>

---

<sup>88</sup> Például a BCR-eken belül, amelyeknek mindenképpen szabályozniuk kell az alább felsorolt intézkedések némelyikét.

<sup>89</sup> 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.

<sup>90</sup> 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 tartásuk, és hogy a személyes adatok ilyen kikötéseken alapuló továbbítását az e kikötések megsértése, illetve tiszteletben tartásuk lehetetlensége esetén felfüggeszék vagy megtiltsák”; lásd még a 148. pontot.

<sup>91</sup> „Schrems II” ítélet (C-311/18), 125. pont.

<sup>92</sup> Az EUB „Schrems II” ítélete (C-311/18), 132. pont.



102. 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

103. Az adattovábbítások konkrét körülményeitől (ideértve a harmadik ország jogszabályainak gyakorlati alkalmazását is) függően a szerződésnek adott esetben elő kell írnia, hogy az adattovábbítások megvalósulásához meghatározott technikai intézkedéseket kell végrehajtani (lásd fent a javasolt technikai intézkedéseket).

104. A hatékonyság feltételei:

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

#### Átláthatósági kötelezettségek:

105. Az adatexportőr mellékleteket csatolhat a szerződéshez olyan információkkal, amelyeket az adatimportőr minden tőle telhetőt megtéve szolgáltatott a szerződés megkötését megelőzően 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 adatexportőrt abban, hogy eleget tegyen azon kötelezettségének, hogy dokumentálja a harmadik ország védelmi szintjére vonatkozó értékelését. Hangsúlyozhatja továbbá az adatimportőr azon kötelezettségét is, hogy segítse az adatexportőrt értékelése elvégzésében, és vállaljon felelősséget azért, hogy objektív, megbízható, releváns, ellenőrizhető és nyilvánosan elérhető vagy egyéb módon hozzáférhető információkat szolgáltasson számára.

106. Az adatimportőrt kötelezni lehet például arra, hogy:

(1) felsorolja a célországban az adatimportőrre 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;

(2) a hatóságok adatokhoz való hozzáférést szabályozó jogszabályok hiányában szolgáltatson az adatimportőr 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 adatimportőr 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 adatimportőr egy meghatározott időszak alatt<sup>93</sup> kapott, különösen a fenti (1) pontban említett területeken, beleértve a beérkezett felhívásokra, a kért adatokra, a megkereső szerve és a közlés jogalapjára, valamint az arra vonatkozó tájékoztatást is, hogy az adatimportőr milyen mértékben közölte a kért adatokat;<sup>94</sup>

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

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

108. A hatékonyság feltételei:

- Az adatimportőrnek képesnek kell lennie arra, hogy legjobb tudomása szerint az adatexportőr rendelkezésére bocsássa ezeket az információkat, miután minden tőle telhetőt megtett azok megszerzése érdekében.
- Ez az adatimportőrre rótt kötelezettség annak biztosítására szolgál, hogy az adatexportőr tudomást szerezzen a harmadik országba történő adattovábbítással járó kockázatokról, és folyamatosan tudatában legyen azoknak. Így lehetővé teszi az adatexportőr 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 EGT-ben biztosított védelmi szinttel lényegében azonos védelmi szintet biztosítani. Ez a kötelezettség azonban nem igazolhatja a személyes adatok adatimportőr általi közlését, és nem keltheti azt az elvárást sem, hogy nem lesznek további hozzáférésre irányuló felhívások.

\*\*\*

109. Az adatexportőr olyan kikötéseket is beilleszthet, amelyekkel az adatimportőr 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 adatimportőrtől, hogy hátsó ajtókat hozzon létre vagy

---

<sup>93</sup> 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 adatexportőrrel való lezárását megelőző utolsó év.

<sup>94</sup> E kötelezettség teljesítése önmagában nem jelenti a megfelelő védelmi szint biztosítását. Ugyanakkor minden olyan nem megfelelő közlés, amelyre ténylegesen sor került, kiegészítő intézkedések végrehajtását teszi szükségessé.

tartson fenn, vagy megkönnyítse a személyes adatokhoz vagy rendszerekhez való hozzáférést, vagy hogy az adatimportőr birtokában legyen a titkosítási kulcs, vagy adja át azt.<sup>95</sup>

110. A hatékonyság feltételei:

- Olyan jogszabályok vagy kormányzati politikák megléte, amelyek megakadályozzák, hogy az adatimportőrök közöljék ezeket az információkat, hatástalanná teheti ezt a kikötést. Az adatimportőr így nem kötheti meg a szerződést, vagy értesítenie kell az adatexportőrt arról, hogy nem tudja tovább teljesíteni szerződéses kötelezettségeit.
- A szerződésnek szankciókat és/vagy az adatexportőr azon lehetőségét is tartalmaznia kell, hogy rövid határidővel elálljon a szerződéstől azokban az esetekben, amikor az adatimportőr nem fed fel egy hátsó ajtó vagy hasonló programozás vagy manipulált üzleti folyamatok vagy az ezek bármelyikének végrehajtására vonatkozó követelmény meglétét, vagy nem tájékoztatja haladéktalanul az adatexportőrt, amint ezek megléte a tudomására jut.
- Abban az esetben, ha az adatimportőr a választott adattovábbítási eszközben foglalt kötelezettségvállalások megsértésével továbbított személyes adatokat közölt, a szerződés magában foglalhatja az adatimportőr által az érintettnek az elszenvedett vagyoni és nem vagyoni kár megtérítését.

\*\*\*

111. Az adatexportőr megerősítheti arra vonatkozó lehetőségét, hogy a helyszínen és/vagy távolról ellenőrizze<sup>96</sup> vagy megvizsgálja az adatimportőr 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 adatexportőr ellenőrző testületek kiválasztásával kapcsolatos autonómiájának megerősítésével.

112. A hatékonyság feltételei:

- Ahhoz, hogy teljes mértékben hatékony legyen, az ellenőrzésnek jogilag és technikailag ki kell terjednie a harmadik országba továbbított személyes adatoknak az adatimportőr adatfeldolgozói vagy további adatfeldolgozói által történő minden feldolgozására.
- A hozzáférési naplónak és más hasonló nyomoknak hamisíthatatlannak kell lenniük (pl. a lehető legkorszerűbb titkosítási technikák – például hashing – alkalmazásával azokat megváltoztathatatlaná kell tenni, és rendszeres időközönként továbbítani kell az adatexportőrnek is), hogy az ellenőrök bizonyítékot találhassanak a közlésre. A hozzáférési naplónak 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.

---

<sup>95</sup> Ez a kikötés fontos a továbbított személyes adatok megfelelő szintű védelmének biztosításához, és azt általában elő kell írni.

<sup>96</sup> 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.

113. Ha az adatimportőr harmadik országának jogát és gyakorlatát kezdetben értékelték, és úgy ítélték meg, hogy az az adatexportőr által továbbított adatok tekintetében biztosítja az Európai Unióban biztosított védelmi szinttel lényegében azonos védelmi szintet, az adatexportőr még mindig megerősítheti az adatimportőr azon kötelezettségét, hogy a helyzetben bekövetkező változás esetén haladéktalanul tájékoztassa az adatexportőrt arról, hogy nem képes megfelelni a szerződéses kötelezettségvállalásoknak és ennélfogva a „lényegében azonos adatvédelmi szint” követelményének.<sup>97.</sup>

114. Ez a megfelelésre való képtelenség a harmadik ország jogszabályaiban vagy gyakorlatában bekövetkezett változások következménye lehet.<sup>98</sup> A kikötések konkrét és szigorú határidőket és eljárásokat állapíthatnak meg az adattovábbítás gyors felfüggesztésére és/vagy a szerződéstől való elállásra, valamint a kapott adatok adatimportőr általi visszaszolgáltatására vagy törlésére. A beérkezett felhívások, azok hatálya és az ellenük hozott intézkedések hatékonysága nyomon követésének elegendő támpontot kell szolgáltatnia az adatexportőr számára ahhoz, hogy eleget tegyen az adattovábbítás felfüggesztésére vagy megszüntetésére és/vagy a szerződéstől való elállásra vonatkozó kötelezettségének.

115. A hatékonyság feltételei:

- Az értesítésnek az adatokhoz való hozzáférés engedélyezése előtt kell megtörténnie. Ellenkező esetben előfordulhat, hogy mire az adatexportőr 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 adatexportőr eleget tegyen a személyes adatok harmadik országba történő továbbításának felfüggesztésére és/vagy a szerződéstől való elállásra vonatkozó kötelezettségének.
- Az adatimportőrnek figyelemmel kell kísérnie minden olyan jogi vagy politikai fejleményt, amely azzal járhat, hogy nem képes megfelelni kötelezettségeinek, és haladéktalanul tájékoztatnia kell az adatexportőrt minden ilyen változásról és fejleményről, lehetőség szerint még azok végrehajtása előtt, hogy az adatexportőr visszaszerezhesse az adatokat az adatimportőrtől.
- A kikötéseknek rendelkezniük kell egy gyors mechanizmusról, amelynek keretében az adatexportőr engedélyezi az adatimportőr számára, hogy azonnal biztonságba helyezze vagy visszaszolgáltassa az adatokat az adatexportőrnek, vagy ha ez nem lehetséges, törölje vagy

---

<sup>97</sup> Az általános szerződési feltételekről szóló 2010/87/EU határozat 5. általános szerződési feltételének a) pontja és d) pontjának i. alpontja.

<sup>98</sup> 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”.

biztonságosan titkosítsa az adatokat anélkül, hogy feltétlenül meg kellene várnia az adatexportőr utasításait, amennyiben az adatexportőr és az adatimportőr által közösen megállapítandó konkrét küszöbérték<sup>99</sup> teljesül. Az adatimportőrnek ezt a mechanizmust az adattovábbítás kezdetétől fogva alkalmaznia kell, és rendszeresen tesztelnie kell azt annak biztosítása érdekében, hogy rövid időn belül alkalmazható legyen.

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

\*\*\*

116. Amennyiben azt a harmadik ország nemzeti joga lehetővé teszi, a szerződés megerősítheti az adatimportőr átláthatósági kötelezettségeit egy olyan „Warrant Canary” („végzéskanári” – hozzáférést elrendelő végzésre vonatkozó figyelmeztetés) módszer előírásával, amellyel az adatimportőr kötelezettséget vállal arra, hogy rendszeresen (például legalább 24 óránként) kriptográfiailag aláírt üzenetet tesz közzé, amelyben tájékoztatja az adatexportőrt 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 adatexportőr számára, hogy az adatimportőr adott esetben határozatot kapott.

117. A hatékonyság feltételei:

- A harmadik ország szabályozásának lehetővé kell tennie az adatimportőr számára, hogy kiadja ezt a fajta passzív értesítést az adatexportőr felé.
- Az adatexportőrnek automatikusan figyelemmel kell kísérnie a „Warrant Canary” értesítéseket.
- Az adatimportőrnek 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

118. Az adatimportőr 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 adatimportőrnek ideiglenes intézkedések elrendelését kell kérnie a határozat joghatóságainak felfüggesztéséhez mindaddig, amíg a bíróság érdemi döntést nem hoz. Az adatimportőr köteles lenne arra, hogy a kért személyes adatokat mindaddig ne közölje, amíg az alkalmazandó eljárási szabályok alapján nem

---

<sup>99</sup> E küszöbértéknek biztosítania kell, hogy az érintettek továbbra is az EGT-ben biztosítottal azonos szintű védelemben részesüljenek.

köteles erre. Az adatimportőr kötelezettséget vállalna arra is, hogy a határozat észszerű értelmezése alapján a határozatra válaszul rendelkezésre bocsátja a megengedett minimális mennyiségű információt.

#### 119. 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 kiegészítő 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 adatimportőrnek képesnek kell lennie arra, hogy az adatexportőr felé dokumentálja és igazolja azokat az intézkedéseket, amelyeket e kötelezettségvállalás teljesítése érdekében minden tőle telhetőt megtéve megtett.

\*\*\*

120. A fent ismertetett helyzetben az adatimportőr kötelezettséget vállalhat arra, hogy tájékoztatja az elrendelő hatóságot a határozatnak az általános adatvédelmi rendelet 46. cikke szerinti adattovábbítási eszközben foglalt garanciákkal<sup>100</sup> való összeegyeztethetlenségéről, valamint az adatimportőr kötelezettségeinek ebből eredő összeütközéséről. Az adatimportőr egyidejűleg és a lehető leghamarabb értesíti az adatexportőrt és/vagy az EGT illetékes felügyeleti hatóságát, amennyiben ezt a harmadik ország jogrendje lehetővé teszi.

#### 121. 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.

---

<sup>100</sup> Az általános szerződési feltételek például úgy rendelkeznek, hogy az adatok feldolgozása, ideértve azok továbbítását is, megfelel és továbbra is megfelel „az alkalmazandó adatvédelmi jognak”. Fogalom meghatározása szerint e jog „az egyének alapvető jogaik és szabadságjogaik, különösen – a személyes adatok feldolgozásával kapcsolatban – a magánélet tiszteletben tartásához való jogaik védelméről szóló, az adatexportőr 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 ország jogrendszere nem akadályozhatja meg az adatimportőrt abban, hogy a kapott, hozzáférést elrendelő határozatról vagy hozzáférésre irányuló felhívásról értesítse az adatexportőrt vagy legalább az EGT illetékes felügyeleti hatóságát.
- Az adatimportőrnek képesnek kell lennie arra, hogy az adatexportőr felé dokumentálja és igazolja azokat az intézkedéseket, amelyeket e kötelezettségvállalás teljesítése érdekében minden tőle telhetőt megtéve megtett.

#### Az érintettek képessé tétele jogaik gyakorlására

122. A szerződés előírhatja, hogy a rendes üzletvitel során (beleértve a támogatási eseteket is) egyszerű szöveggént továbbított személyes adatokhoz csak az adatexportőrnek és/vagy az érintettnek az adatokhoz való konkrét hozzáféréshez adott kifejezett vagy hallgatólagos hozzájárulásával lehet hozzáférni.

123. A hatékonyság feltételei:

- E kikötés azokban a helyzetekben lehet hatékony, amelyekben az adatimportőrök a hatóságoktól önkéntes alapon történő együttműködésre irányuló felhívásokat kapnak, szemben például a hatóságok adatokhoz való olyan hozzáféréssel, amelyre az adatimportőr 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)<sup>101</sup>.
- Azok a nemzeti szabályozások vagy politikák, amelyek arra kötelezik az adatimportőrt, hogy ne közölje a hozzáférést elrendelő határozatot, hatástalanná tehetik ezt a kikötést, kivéve, ha azt olyan technikai módszerekkel lehet megtámogatni, amelyek szükségessé teszik az adatexportőr vagy az érintett beavatkozását ahhoz, hogy az egyszerű szöveges adatok hozzáférhetőek 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.

\*\*\*

124. A szerződés arra kötelezheti az adatimportőrt és/vagy az adatexportőrt, hogy haladéktalanul értesítse az érintettet a harmadik ország hatóságaitól kapott felhívásról vagy határozatról, vagy arról, hogy az adatimportőr 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 bírósági előtti keresetőségi jogát), ideértve a választott adattovábbítási eszközben foglalt kötelezettségvállalások megsértésével ezen adattovábbítási eszköz alapján továbbított személyes adatok közlése miatt elszenvedett vagyoni és nem vagyoni kár adatimportőr általi megtérítését is.

---

<sup>101</sup> Az általános adatvédelmi rendelet 4. cikkének 11. bekezdése.

#### 125. 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 adatexportőröktől, és eljárást indítson az illetékes felügyeleti hatóságnál. Ez a kikötés azon nehézségek némelyikére is megoldást jelenthet, és kompenzálhatja azokat, amelyekkel az egyén akkor szembesülhet, ha igazolnia kell harmadik országok bíróságai előtti keresetösségi jogát (locus standi) az adataihoz való hatósági hozzáférés megtámadásához.
- A nemzeti szabályozások és politikák megakadályozhatják az érintett ilyen értesítését. Az adatexportőr és az adatimportőr 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 adatexportőr vagy az illetékes felügyeleti hatóság értesítheti az érintettet legalább személyes adatai továbbításának azon okból történő felfüggesztéséről vagy megszüntetéséről, hogy a hozzáférésre irányuló felhívás miatt az adatimportőr nem képes megfelelni szerződéses kötelezettségvállalásainak.

\*\*\*

126. A szerződés arra kötelezheti az adatexportőrt és az adatimportőrt, hogy ad hoc jogorvoslati mechanizmusok és jogi tanácsadás révén segítse az érintettet jogainak a harmadik ország joghatósága alatt történő gyakorlásában.

#### 127. A hatékonyság feltételei

- Előfordulhat, hogy egyes nemzeti szabályozások nem teszik lehetővé az adatimportőr számára, hogy közvetlenül nyújtson ilyen jellegű segítséget az érintettek számára, bár lehetővé tehetik az adatimportőr számára, hogy az érintettek számára ilyen segítséget szerezzen.
- 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 EGT-ben biztosított védelmi szinttel lényegében azonos védelmi szintet. E szerződéses intézkedésnek szükségszerűen kiegészítő jellegűnek kell lennie egyéb kiegészítő 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, többek között a megfigyelési intézkedésekkel szemben.



## 2.3 Szervezési intézkedések

128. 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 adatexportőrök 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 EGT-ben biztosított védelmi szinttel.
129. 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 adatexportőrök végrehajthatnak, jóllehet a felsorolás nem kimerítő, és más intézkedések szintén megfelelőek lehetnek:

### Az adattovábbítások irányítására vonatkozó belső politikák, különösen a vállalkozáscsoportokkal összefüggésben

130. Megfelelő belső politikák elfogadása az adattovábbítással kapcsolatos feladatok egyértelmű megosztásával, bejelentési csatornákkal és eljárási standardokkal a hatóságok adatokhoz való hozzáférésre irányuló, formális vagy informális felhívásainak eseteire. Különösen a vállalkozáscsoportok közötti adattovábbítások esetében ezek a politikák magukban foglalhatják többek között egy, az informatikai, adatvédelmi és a magánélet védelmére vonatkozó jogszabályok szakértőiből álló külön munkacsoport kijelölését az EGT-ből továbbított személyes adatokat érintő felhívások kezelésére; a jogi és vállalati felső vezetés, valamint az adatexportőr értesítését az ilyen felhívások kézhezvételekor; az aránytalan vagy jogellenes felhívások megtámadására irányuló eljárási lépéseket és az érintettek átlátható tájékoztatásának előírását.
131. 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 adatimportőr sajátos helyzetét, például a harmadik ország azon törvényeit és rendeleteit, amelyeknek az adatimportőr a hatálya alá tartozik, és azt lehetőség szerint az adatexportőrrel együttműködve kell kidolgozni.

#### 132. A hatékonyság feltételei:

- Ezek a politikák csak azokra az esetekre irányozhatók elő, amelyekben a harmadik ország hatóságainak felhívása összeegyeztethető az uniós joggal.<sup>102</sup> 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 kiegészítő intézkedéseket kell hozni a hozzáférés elkerülése érdekében.

#### Átláthatósági és elszámoltathatósági intézkedések

133. 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 adatexportort értesítették, az adatexportor válaszát, az ilyen felhívások kezeléséért felelős munkacsoport értékelését stb.). Ezeket a nyilvántartásokat az adatexportor rendelkezésére kell bocsátani, aki átadja azokat az érintetteknek.

#### 134. 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 adatimportőrnek tájékoztatnia kell az adatexportort arról, hogy nem képes ilyen dokumentumokat és nyilvántartásokat rendelkezésre bocsátani, ezáltal lehetőséget biztosítva az adatexportornek arra, hogy felfüggesse az adattovábbításokat, amennyiben az információszolgáltatási képesség e hiánya miatt nem lehetne biztosítani a megfelelő védelmi szintet.

\*\*\*

135. 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.

#### 136. 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 adatimportőrnek minden tőle telhetőt meg kell tennie annak érdekében, hogy statisztikai információkat vagy hasonló típusú összesített információkat tegyen közzé.

#### Szervezési módszerek és adattakarékossági intézkedések

137. 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

---

<sup>102</sup> Lásd: „Schrems I” ítélet (C-362/14), 94. pont; „Schrems II” ítélet (C-311/18), 168., 174., 175. és 176. pont.

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 kitétségét. 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).

138. 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 adatexportőrnek 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 adatimportőrrel.
- 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.

\*\*\*

139. 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.

140. 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 adatimportőr kötelezettséget vállalt.

### Szabványok és bevált módszerek elfogadása

141. 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 összhangban.

## Egyéb

142. Belső politikák elfogadása és rendszeres felülvizsgálata a végrehajtott kiegészítő 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 EGT-ben biztosított védelmi szinttel lényegében azonos szintje.

\*\*\*

143. Az adatimportőr arra vonatkozó kötelezettségvállalása, hogy nem továbbítja újból a személyes adatokat ugyanazon vagy más harmadik országban belül, vagy hogy felfüggeszti a folyamatban lévő adattovábbításokat, ha a harmadik országban nem biztosítható a személyes adatoknak az EGT-ben biztosítottal lényegében azonos szintű védelme.<sup>103</sup>

---

<sup>103</sup> „Schrems II” ítélet (C-311/18), 135. és 137. pont.

### 3. MELLÉKLET HARMADIK ORSZÁGOK ÉRTÉKELÉSÉHEZ FELHASZNÁLHATÓ INFORMÁCIÓFORRÁSOK

144. Az adatimportőrnek képesnek kell lennie arra, hogy tájékoztassa Önt a letelepedési helye szerinti harmadik országgal – az adatimportőrre és a továbbított adatokra alkalmazandó jogszabályokat és gyakorlatokat is ideértve – kapcsolatos releváns forrásokról és információkról. Ön és az adatimportőr számos információforrásra – például az alábbiakban nem kimerítő jelleggel fontossági sorrendben felsorolt forrásokra – támaszkodhat:

- az Európai Unió Bíróságának (EUB) és az Emberi Jogok Európai Bíróságának (EJEB)<sup>104</sup> az alapvető európai garanciákról szóló ajánlásban hivatkozott ítélkezési gyakorlata;<sup>105</sup>
- megfelelőségi határozatok a célországban, ha az adattovábbításra más jogalapon kerül sor;<sup>106</sup>
- kormányközi szervezetek, például az Európa Tanács,<sup>107</sup> más regionális szervek<sup>108</sup>; valamint az ENSZ szerveinek és ügynökségeinek (például az ENSZ Emberi Jogi Tanácsának,<sup>109</sup> az ENSZ Emberi Jogi Bizottságának<sup>110</sup>) határozatai és jelentései;
- az illetékes szabályozói hálózatok, például a Global Privacy Assembly (globális adatvédelmi közgyűlés, GPA) jelentései és elemzései;<sup>111</sup>
- a magánélet és az adatvédelem területén hatáskörrel rendelkező, harmadik országbeli független igazságügyi vagy közigazgatási hatóságok nemzeti ítélkezési gyakorlata vagy határozatai;
- független felügyeleti vagy parlamenti szervek jelentései;
- az adatimportőrrel azonos ágazatban működő szervezetektől származó, közzétételre irányuló hatósági felhívások vagy ilyen felhívások hiányának korábbi eseteivel kapcsolatos gyakorlati tapasztalatokon alapuló jelentések;
- az adatimportőrrel azonos területen adatokat kezelő más szervezetek „Warrant Canary”-jai;
- az adatexportőr vagy az adattovábbítás célországának számító harmadik országnak adatokat átadó más harmadik országok kereskedelmi kamarái, vállalkozói, szakmai és kereskedelmi

---

<sup>104</sup> Lásd az EJEB tömeges megfigyeléssel kapcsolatos ítélkezési gyakorlatáról szóló tájékoztatót:

[https://www.echr.coe.int/Documents/FS\\_Mass\\_surveillance\\_ENG.pdf](https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf)

<sup>105</sup> Az Európai Adatvédelmi Testületnek a megfigyelési intézkedésekkel kapcsolatos alapvető európai garanciákról szóló, 2020. november 10-i 02/2020. sz. ajánlása, [https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential\\_en](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en)

<sup>106</sup> „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](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

<sup>107</sup> <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

<sup>108</sup> Lásd például az Emberi Jogok Amerikaközi Bizottságának (IACHR) országjelentéseit, <https://www.oas.org/en/iachr/reports/country.asp>.

<sup>109</sup> Lásd: <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>

<sup>110</sup> Lásd:

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

<sup>111</sup> Lásd például: [https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1\\_2a-Day-3-3\\_2b-v1\\_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf](https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf)

szövetségei, valamint kormányzati diplomáciai, kereskedelmi és beruházási ügynökségei által készített vagy megrendelt jelentések;

- tudományos intézmények és civil társadalmi szervezetek (pl. nem kormányzati szervezetek) jelentései;
- üzleti hírszerzési magánszolgáltatóknak a vállalatokat érintő pénzügyi, szabályozási és reputációs kockázatokról szóló jelentései;
- magának az adatimportőrnek a „Warrant Canary”-jai;<sup>112</sup>
- átláthatósági jelentések, azzal a feltétellel, hogy kifejezetten megemlítik azt a tényt, hogy nem érkeztek hozzáférésre irányuló felhívások. Az átláthatósági jelentések e kérdésben való pusztán hallgatása nem minősül elegendő bizonyítéknak, mivel ezek a jelentések leggyakrabban a bűnüldöző hatóságoktól kapott hozzáférésre irányuló felhívásokra összpontosítanak, és csak e tekintetben szolgálnak számadatokkal, miközben hallgatnak a nemzetbiztonsági célból kapott hozzáférésre irányuló felhívásokról. Ez nem azt jelenti, hogy nem érkeztek hozzáférésre irányuló felhívások, hanem azt, hogy ez az információ nem osztható meg;<sup>113</sup>
- az adatimportőr belső nyilatkozatai vagy nyilvántartásai, amelyek kifejezetten megemlítik, hogy kellően hosszú ideig nem érkeztek hozzáférésre irányuló felhívások; előnyben részesítve az adatimportőr felelősségét megalapozó és/vagy a bizonyos autonómiával rendelkező alkalmazottak, például belső ellenőrök, adatvédelmi tisztviselők stb. által kiállított nyilatkozatokat és nyilvántartásokat.<sup>114</sup>

---

<sup>112</sup> Az adatimportőrnek a harmadik ország hatóságaitól kapott hozzáférésre irányuló felhívások korábbi releváns eseteivel kapcsolatos dokumentált gyakorlati tapasztalatainak figyelembevételére vonatkozó feltételeket lásd a 47. pontban.

<sup>113</sup> *Uo.*

<sup>114</sup> *Uo.*