A BIZOTTSÁG (EU) 2023/1795 VÉGREHAJTÁSI HATÁROZATA

(2023. július 10.)

az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatoknak az EU–USA adatvédelmi keret által biztosított megfelelő szintű védelméről

(az értesítés a C(2023) 4745. számú dokumentummal történt)

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az Európai Parlament és a Tanács (EU) 2016/679 rendeletére (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az említett adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) ([1]) és különösen annak 45. cikke (3) bekezdésére,

mivel:

1. BEVEZETÉS

(1) Az (EU) 2016/679 rendelet ([2]) meghatározza a személyes adatoknak az uniós adatkezelők vagy adatfeldolgozók által a harmadik országokba és a nemzetközi szervezeteknek történő továbbítására vonatkozó szabályokat, amennyiben az említett adattovábbítás az alkalmazási körébe tartozik. A nemzetközi adattovábbításra vonatkozó szabályokat az említett rendelet V. fejezete állapítja meg. Noha a személyes adatok Európai Unión kívüli országokba és onnan az Unióba történő áramlása elengedhetetlen a határokon átnyúló kereskedelem és a nemzetközi együttműködés bővítéséhez, a személyes adatoknak az Európai Unióban biztosított védelmi szintje nem sérülhet a harmadik országokba vagy nemzetközi szervezetek részére történő továbbítás esetén ([3]).

(2) Az (EU) 2016/679 rendelet 45. cikkének (3) bekezdése értelmében a Bizottság végrehajtási jogi aktusok útján határozhat arról, hogy a harmadik ország, a harmadik ország valamely területe, illetve egy vagy több meghatározott ágazata biztosítja a megfelelő szintű védelmet. E feltétel teljesülése esetén a személyes adatok harmadik országba történő továbbítására további engedély beszerzése nélkül kerülhet sor, az (EU) 2016/679 rendelet 45. cikke (1) bekezdésében és (103) preambulumbekezdésében előírtak szerint.

(3) Az (EU) 2016/679 rendelet 45. cikkének (2) bekezdésében foglaltak szerint, a megfelelőségi határozat elfogadásának a harmadik ország jogrendjére vonatkozó átfogó elemzésen kell alapulnia, lefedve mind az adatátvevőre vonatkozó szabályokat, mind a személyes adatokhoz való, közigazgatási szervek általi hozzáférést illető korlátozásokat és biztosítékokat. Az értékelés során meg kell határozni, hogy az érintett harmadik ország olyan szintű védelmet biztosít-e, amely „lényegében megegyező” az Unión belül biztosított védelem szintjével (az (EU) 2016/679 rendelet (104) preambulumbekezdése). A „lényegi megegyezőség” értékelése az uniós jogszabályok, nevezetesen az (EU) 2016/679 rendelet, valamint az Európai Unió Bíróságának (a továbbiakban: Bíróság) ítélkezési gyakorlata alapján történik ([4]).

([1]) HL L 119., 2016.5.4., 1. o.
([2]) A hivatkozás megkönnyítése érdekében az e határozatban használt rövidítések jegyzékét a VIII. melléklet tartalmazza.
([3]) Lásd az (EU) 2016/679 rendelet (101) preambulumbekezdését.
([4]) Lásd legutóbb a C-311/18. sz., Facebook Írország és Schrems ügyet („*Schrems II*.”), ECLI:EU:C:2020:559.

(4) Amint azt a Bíróság a C-362/14. sz. Maximillian Schrems kontra adatvédelmi biztos (Schrems) ügyben 2015. október 6-án hozott ítéletében ([5]) pontosította, ehhez nem szükséges azonos szintű védelmet megállapítani. Különösen a harmadik ország által a személyes adatok védelme céljából igénybe vett eszközök különbözhetnek az Unióban alkalmazott eszközöktől, amennyiben – a gyakorlatban – ténylegesen megfelelő szintű védelmet biztosítanak ([6]). A megfelelőségre vonatkozó előírás ezért nem követeli meg az uniós szabályok pontról pontra történő leképezését. A vizsgálat ehelyett arra irányul, hogy a magánélet tiszteletben tartásához való jog tartalmát, tényleges végrehajtását, felügyeletét és érvényesítését tekintve az érintett harmadik ország rendszere összességében véve biztosítja-e az elvárt fokú védelmet ([7]). Ezen túlmenően az említett ítélet szerint ezen előírás alkalmazása során a Bizottságnak különösen azt kell értékelnie, hogy a szóban forgó harmadik ország jogi kerete tartalmaz-e olyan szabályokat, amelyek célja az azon személyek alapvető jogaiba való beavatkozás korlátozása, akiknek az adatait az Unióból továbbítják, amely beavatkozásra az adott ország állami szervezetei jogosultak lennének, ha jogszerű célokat követnek, mint például a nemzetbiztonság, és hatékony jogi védelmet nyújtanak az ilyen jellegű beavatkozásokkal szemben ([8]). Az Európai Adatvédelmi Testület által az említett előírás további pontosítása céljából kiadott „megfelelőségi referencia” szintén iránymutatást nyújt e tekintetben ([9]).

(5) A magánélethez és az adatvédelemhez való alapvető jogba való ilyen beavatkozás tekintetében alkalmazandó előírást a Bíróság a C-311/18. sz., Adatvédelmi tisztviselő kontra Facebook Ireland Limited és Maximillian Schrems (Schrems II) ügyben 2020. július 16-án hozott ítéletében tovább pontosította, amely érvénytelenítette a korábbi transzatlanti adatáramlási keretről, az EU–USA adatvédelmi pajzsról (adatvédelmi pajzs) szóló (EU) 2016/1250 bizottsági végrehajtási határozatot ([10]). A Bíróság úgy ítélte meg, hogy a személyes adatok védelmének az Egyesült Államok hatóságai által nemzetbiztonsági célokból az Unióból az Egyesült Államokba továbbított adatokhoz való hozzáférésre és azok felhasználására vonatkozó nemzeti jogából eredő korlátozásait nem olyan módon határozták meg, hogy az megfeleljen az adatvédelemhez való jogba való ilyen beavatkozás szükségessége és arányossága tekintetében az uniós jogban előírtakkal lényegében egyenértékű követelményeknek ([11]). A Bíróság azt is megállapította, hogy semmilyen jogorvoslati lehetőség nem áll rendelkezésre olyan szerv előtt, amely lényegében a Charta hatékony jogorvoslathoz való jogról szóló 47. cikkében előírtakkal egyenértékű garanciákat nyújt azon személyek számára, akiknek az adatait továbbították az Egyesült Államokba ([12]).

(6) A *Schrems II.* ítéletet követően a Bizottság tárgyalásokat kezdett az Egyesült Államok kormányával egy esetleges új megfelelőségi határozat meghozatala céljából, amely megfelelne az (EU) 2016/679 rendelet 45. cikke (2) bekezdésében foglalt, a Bíróság által értelmezett követelményeknek. E megbeszélések eredményeként az Egyesült Államok 2022. október 7-én elfogadta az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről szóló 14086. sz. elnöki rendeletet (a továbbiakban: 14086. elnöki rendelet), amelyet az Egyesült Államok főügyésze által kiadott, az adatvédelmi felülvizsgálati bíróságról szóló rendelet (a továbbiakban: főügyészi rendelet) egészít ki ([13]). Emellett sor került az e határozat alapján az Unióból továbbított adatokat kezelő kereskedelmi szervezetekre vonatkozó keret – az „EU–USA adatvédelmi keret” (a továbbiakban: EU–USA adatvédelmi keret vagy adatvédelmi keret) aktualizálására.

(7) A Bizottság gondosan elemezte az Egyesült Államok jogát és gyakorlatát, többek között a 14086. elnöki rendeletet és a főügyészi rendeletet. A (9)–(200) preambulumbekezdésben kifejtett megállapítások alapján a Bizottság arra a következtetésre jutott, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az EU–USA adatvédelmi keret alapján az Unión belüli adatkezelőtől vagy adatfeldolgozótól ([14]) az egyesült államokbeli tanúsított szervezetekhez továbbított személyes adatok védelme tekintetében.

([5]) A Bíróság ítélete, Maximillian Schrems kontra adatvédelmi biztos („*Schrems-ügy*”), C-362/14, ECLI:EU:C:2015:650, 73. pont.

([6]) Schrems-ügy, 74. pont.

([7]) Lásd: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – A személyes adatok cseréje és védelme a globalizált világban, 3.1. szakasz, 6–7. o., COM(2017) 7, 2017.1.10.

([8]) Schrems-ügy, 88–89. pont.

([9]) Európai Adatvédelmi Testület, megfelelőségi referencia, WP 254 rev. 01., a következő linken érhető el: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

([10]) A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről (HL L 207., 2016.8.1., 1. o.).

([11]) Schrems II. ügy, 185. pont.

([12]) Schrems II. ügy, 197. pont.

([13]) A 28. CFR 302. része.

([14]) Ez a határozat EGT-vonatkozású. Az Európai Gazdasági Térségről szóló megállapodás (EGT-megállapodás) kiterjeszti az Európai Unió belső piacát a három EGT-államra: Izlandra, Liechtensteinre és Norvégiára. Az EGT Vegyes Bizottság 2018. július 6-án elfogadta az (EU) 2016/679 rendeletet az EGT-megállapodás XI. mellékletébe beillesztő vegyes bizottsági határozatot, amely 2018. július 20-án lépett hatályba. E rendelet ezért az említett megállapodás hatálya alá tartozik. A határozat alkalmazásában tehát az EU-ra és az uniós tagállamokra való hivatkozásokat úgy kell értelmezni, hogy azok az EGT-államokra is vonatkoznak.

(8) E határozat azzal a joghatással jár, hogy az Unión belüli adatkezelők és adatfeldolgozók ([15]) részéről az egyesült államokbeli tanúsított szervezetek részére történő adattovábbításra további engedély nélkül kerülhet sor. Ez a határozat nem érinti az (EU) 2016/679 rendeletnek az ilyen szervezetekre történő közvetlen alkalmazását, ha teljesülnek az említett rendelet 3. cikkében meghatározott, a rendelet területi hatályára vonatkozó feltételek.

2. AZ EU–USA ADATVÉDELMI KERET

2.1. Személyi és tárgyi hatály

2.1.1. *Tanúsított szervezetek*

(9) Az EU–USA adatvédelmi keret olyan tanúsítási rendszeren nyugszik, amelynek keretében az egyesült államokbeli szervezetek kötelezettséget vállalnak egy sor adatvédelmi elv – az EU–USA adatvédelmi keret elvei, köztük a kiegészítő elvek (a továbbiakban együttesen: az elvek) – betartására. Ezeket az elveket az Egyesült Államok Kereskedelmi Minisztériuma bocsátotta ki, és megtalálhatók e határozat I. mellékletében ([16]). Az EU–USA adatvédelmi keret szerinti tanúsításra való jogosultsághoz a szervezetnek a Szövetségi Kereskedelmi Bizottság (FTC) vagy az Egyesült Államok Közlekedési Minisztériuma vizsgálati és végrehajtási hatáskörébe kell tartoznia ([17]). Az elvek a tanúsítást követően azonnal alkalmazandók. Amint azt a (48)–(52) preambulumbekezdés részletesebben kifejti, az EU–USA adatvédelmi keret szerinti szervezeteknek évente újra kell tanúsítaniuk az elvek betartását ([18]).

2.1.2. *A személyes adatok meghatározása, valamint az adatkezelő és a „megbízott” fogalma*

(10) Az EU–USA adatvédelmi keret által biztosított védelem minden olyan személyes adatra vonatkozik, amelyet az Unióból továbbítottak olyan egyesült államokbeli szervezeteknek, amelyek tanúsították a Kereskedelmi Minisztérium számára, hogy betartják az elveket, kivéve azokat az adatokat, amelyeket közzététel, sugárzás vagy más formában történő, az újságírói anyagokról szóló nyilvános kommunikáció céljából gyűjtenek, valamint a korábban közzétett, médiaarchívumokból terjesztett anyagokban szereplő információkat ([19]). Ezek az információk ezért nem továbbíthatók az EU–USA adatvédelmi keret alapján.

(11) Az elvek ugyanúgy határozzák meg a személyes adatokat/személyes információkat, mint az (EU) 2016/679 rendelet, azaz azok az „azonosított vagy azonosítható, az általános adatvédelmi rendelet hatálya alá tartozó természetes személyre vonatkozó, az Egyesült Államokban működő szervezet által az EU-ból kapott és bármilyen formában rögzített adatok” ([20]). Ennek megfelelően az álnevesített (vagy kulcskódolt) kutatási adatokra is kiterjednek (ideértve azokat az eseteket is, amikor a kulcsot nem osztják meg a fogadó egyesült államokbeli szervezettel) ([21]). A személyes adatok kezelése hasonlóképpen akként van meghatározva, hogy az „a személyes adatokkal automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés vagy terjesztés, valamint törlés vagy megsemmisítés” ([22]).

(12) Az EU–USA adatvédelmi keret azokra az egyesült államokbeli szervezetekre vonatkozik, amelyek adatkezelőnek (azaz olyan személynek vagy szervezetnek, aki vagy amely önállóan vagy másokkal együtt meghatározza a személyes adatok kezelésének céljait és módját) ([23]) vagy adatfeldolgozóknak (azaz az adatkezelő nevében eljáró megbízottaknak) ([24]) minősülnek. Az egyesült államokbeli adatfeldolgozóknak szerződéses kötelezettséget kell vállalniuk, hogy kizárólag az uniós adatkezelő utasításai alapján járhatnak el, és segítséget kell nyújtaniuk az

([15]) Ez a határozat nem érinti az (EU) 2016/679 rendelet azon követelményeit, amelyek az adatokat továbbító uniós szervezetekre (adatkezelőkre és adatfeldolgozókra) vonatkoznak, például a célhoz kötöttségre, az adatminimalizálásra, az átláthatóságra és az adatbiztonságra vonatkozóan (lásd még az (EU) 2016/679 rendelet 44. cikkét).

([16]) Lásd e tekintetben a Schrems-ügyben hozott ítélet 81. pontját, amelyben a Bíróság megerősítette, hogy az öntanúsítás rendszere megfelelő szintű védelmet biztosíthat.

([17]) I. melléklet, I. szakaszának 2. pontja. Az FTC széles körű joghatósággal rendelkezik a kereskedelmi tevékenységek felett, néhány kivétellel, például a bankok, a légitársaságok, a biztosítási üzletág és a távközlési szolgáltatók közös fuvarozói tevékenységei tekintetében (bár az Egyesült Államok Kilencedik Körzeti Fellebbviteli Bíróságának 2018. február 26-i FTC kontra AT&T ítélete megerősítette, hogy az FTC joghatósággal rendelkezik az ilyen szervezetek nem közös fuvarozói tevékenységei felett). Lásd még a IV. melléklet 2. lábjegyzetét. A Közlekedési Minisztérium hatáskörrel rendelkezik a légitársaságok és (légi közlekedés esetében) a jegyértékesítők megfelelésének kikényszerítésére, lásd az V. melléklet A. szakaszát.

([18]) I. melléklet III. szakaszának 6. pontja.

([19]) I. melléklet III. szakaszának 2. pontja.

([20]) I. melléklet I. szakasza 8. pontjának a. alpontja.

([21]) I. melléklet III. szakasza 14. pontjának g. alpontja.

([22]) I. melléklet I. szakasza 8. pontjának b. alpontja.

([23]) I. melléklet I. szakasza 8. pontjának c. alpontja.

([24]) Lásd például az I. melléklet II. szakasza 2. pontjának b. alpontját, valamint a II. szakasz 3. pontjának b. alpontját és a 7. pont d. alpontját, amelyek egyértelművé teszik, hogy a megbízottak az adatkezelő nevében járnak el, az utóbbi utasításainak megfelelően és meghatározott szerződéses kötelezettségek alapján.

utóbbinak ahhoz, hogy választ adjon az elvek alapján a jogaikat gyakorló egyéneknek ([25]). Ezenkívül a további adatfeldolgozó általi kezelés esetén az adatfeldolgozóknak az elvekben előírtakkal azonos szintű védelmet garantáló szerződést kell kötniük a további adatfeldolgozóval, és lépéseket kell tenniük annak megfelelő végrehajtása érdekében ([26]).

2.2. **Az EU–USA adatvédelmi keret elvei**

2.2.1. ***Célhoz kötöttség és választás lehetősége***

(13) A személyes adatokat jogszerűen és tisztességesen kell kezelni. A személyes adatok gyűjtésének konkrét célra kell történnie, és később csak olyan mértékben használhatók fel, amely az adatkezelés céljával nem összeegyeztethetetlen.

(14) Az EU–USA adatvédelmi keret alapján ezt különböző elvek biztosítják. Először is, az *adatintegritás és a célhoz kötöttség elve* értelmében – az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének b) pontjához hasonlóan – a szervezet nem kezelhet személyes adatokat olyan módon, amely összeegyeztethetetlen azzal a céllal, amelyre azokat eredetileg gyűjtötték, vagy amelyet az érintett később engedélyezett ([27]).

(15) Másodszor, a személyes adatok olyan új (módosított) célra történő felhasználása előtt, amely lényegesen eltérő, de még mindig összeegyeztethető az eredeti céllal, vagy harmadik félnek adják át azokat, a szervezetnek egyértelmű, jól látható és könnyen hozzáférhető mechanizmus révén lehetőséget kell biztosítania az érintettek számára, hogy a *választási elvvel* ([28]) összhangban kifogást emeljenek (önkéntes kívülmaradás). Fontos, hogy ez az elv nem helyezi hatályon kívül az összeegyeztethetetlen adatkezelés kifejezett tilalmát ([29]).

([25]) I. melléklet III. szakasza 10. pontjának a. alpontja. Lásd még a Kereskedelmi Minisztérium által az Európai Adatvédelmi Testülettel konzultálva az adatvédelmi pajzs keretében készített iránymutatást, amely tisztázta azon USA-beli adatfeldolgozók kötelezettségeit, amelyek a keret alapján személyes adatokat kapnak az Unióból. Mivel ezek a szabályok nem változtak, ez az iránymutatás/GYIK továbbra is releváns az EU–USA adatvédelmi keret szerint (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) I. melléklet II. szakasza 3. pontjának b. alpontja.

([27]) I. melléklet II. szakasza 5. pontjának a. alpontja. Az összeegyeztethető célok magukban foglalhatják a könyvvizsgálatot, a csalás megelőzését vagy más, a gyűjtés összefüggéseire tekintettel az észszerűen eljáró személy elvárásaival összhangban álló célokat (lásd az I. melléklet 6. lábjegyzetét).

([28]) I. melléklet II. szakasza 2. pontjának a. alpontja. Ez nem alkalmazandó, ha egy szervezet személyes adatokat szolgáltat a nevében és utasításai szerint eljáró adatfeldolgozónak (I. melléklet II. szakasza 2. pontjának b. alpontja). Mindemellett ebben az esetben a szervezetnek szerződést kell kötnie, és biztosítania kell az *újbóli továbbításán való elszámoltathatóság* elvének való megfelelést, amint azt a (43) preambulumbekezdés részletesebben kifejti. Emellett a *választási lehetőség* elve (valamint a *tájékoztatás* elve) korlátozható abban az esetben, ha a személyes adatokat átvilágítási eljárással (lehetséges egyesülés vagy felvásárlás részeként) vagy auditokkal összefüggésben kezelik, olyan mértékben és addig, ameddig az a jogszabályi vagy közérdekű követelmények teljesítéséhez szükséges, vagy olyan mértékben és addig, ameddig ezen elvek alkalmazása sértené a szervezet jogos érdekeit az átvilágítási eljárások vagy könyvvizsgálatok konkrét összefüggésében (I. melléklet III. szakaszának 4. pontja). A 15. kiegészítő elv (I. melléklet III. szakasza 15. pontjának a. és b. alpontja) szintén kivételt ír elő a *választási lehetőség* elve (valamint a *tájékoztatás* és az *újbóli továbbítással kapcsolatos elszámoltathatóság* elve) alól a nyilvánosan hozzáférhető forrásokból származó személyes adatok tekintetében (kivéve, ha az uniós adatátadó jelzi, hogy az információra olyan korlátozások vonatkoznak, amelyek ezen elvek alkalmazását teszik szükségessé), vagy általában véve a nyilvánosság számára betekintésre nyitva álló nyilvántartásokból gyűjtött személyes adatok tekintetében (amennyiben azokat nem kombinálják nem nyilvános nyilvántartásban lévő információkkal, és betartják a betekintési feltételeket). Hasonlóképpen, a 14. kiegészítő elv (I. melléklet III. szakasza 14. pontjának f. alpontja) kivételt biztosít a *választási lehetőség* elve (valamint a *tájékoztatás* és az *újbóli továbbítással kapcsolatos elszámoltathatóság* elve) alól a személyes adatoknak a gyógyszeripari vállalatok vagy orvostechnikai eszközökkel foglalkozó vállalatok által a termékbiztonság és a hatékonyság nyomon követése céljából végzett kezelése tekintetében, amennyiben az elvek betartása akadályozza a szabályozási követelményeknek való megfelelést.

([29]) Ez az EU–USA adatvédelmi keret alapján történő valamennyi adattovábbításra vonatkozik, így akkor is alkalmazandó, amikor ezek munkaviszony keretében gyűjtött adatokat érintenek. Bár a tanúsított amerikai szervezetek ennek értelmében főszabály szerint eltérő, nem munkaviszonnyal kapcsolatos (pl. bizonyos marketingkommunikációs) célokra felhasználhatnak humánerőforrás-adatokat, tiszteletben kell tartaniuk az összeegyeztethetetlen adatkezelés tilalmát, és ezenfelül csupán a *tájékoztatás* és a *választási lehetőség* elveivel összhangban tehetik meg ezt. Kivételes esetben a szervezet *értesítés* és *választási lehetőség* biztosítása nélkül is felhasználhatja a személyes adatokat további, összeegyeztethető célból, de csak olyan mértékben és annyi ideig, amely annak elkerüléséhez szükséges, hogy a szervezet előléptetéseket, kinevezéseket vagy más hasonló foglalkoztatási döntéseket hozzon (lásd az I. melléklet III. szakasza 9. pontja b. pontjának (iv) alpontját). Az e választási lehetőséggel élő alkalmazottal szembeni megtorló intézkedések meghozatalának – így a foglalkoztatási lehetőségek korlátozásának – az amerikai szervezetre vonatkozó tilalma biztosítani fogja, hogy az alá-fölérendeltségi viszony és az ahhoz szervesen hozzátartozó függőség ellenére az alkalmazott ne kerüljön nyomás alá és így valóban szabadon gyakorolhassa döntési jogát. Lásd: I. melléklet III. szakasza 9. pontja b. alpontjának (i) alpontja.

2.2.2. ***A személyes adatok különleges kategóriáinak kezelése***

(16) „Különleges adatok kategóriáinak” kezelése esetén külön biztosítékokat kell rendszeresíteni.

(17) A *választási lehetőség* elvével összhangban különleges biztosítékok vonatkoznak az „érzékeny információk”, azaz az orvosi vagy egészségügyi állapotot, faji vagy etnikai származást, politikai véleményt, vallási vagy világnézeti meggyőződést, szakszervezeti tagságot meghatározó személyes adatok, az egyén szexuális életére vonatkozó információk vagy bármely más, harmadik féltől kapott olyan információ kezelésére, amelyet az adott fél érzékenynek minősített és akként kezel ([30]). Ez azt jelenti, hogy az uniós adatvédelmi jog értelmében érzékenynek minősülő adatokat (beleértve a szexuális irányultságra vonatkozó adatokat, a genetikai adatokat és a biometrikus adatokat) az EU–USA adatvédelmi keret szerint a tanúsított szervezetek érzékenyként kezelik.

(18) Általános szabályként a szervezeteknek meg kell szerezniük az egyének kifejezett hozzájárulását (azaz részvételét) ahhoz, hogy érzékeny információkat az eredeti gyűjtésük vagy az egyén által később (részvételi záradékon keresztül) engedélyezett céloktól eltérő célokra használjanak fel, vagy hogy azokat harmadik felekkel közöljék ([31]).

(19) Az ilyen hozzájárulást nem kell megszerezni az uniós adatvédelmi jog által biztosított hasonló kivételekhez hasonló, korlátozott körülmények között, például ha a különleges adatok kezelése valamely személy létfontosságú érdekét szolgálja; ha jogszerű követelések kialakításához szükséges; vagy egészségügyi ellátás vagy diagnózis nyújtásához szükséges ([32]).

2.2.3. ***Adatpontosság, adattakarékosság és -biztonság***

(20) Az adatoknak pontosnak és – szükség esetén – naprakésznek kell lenniük. Továbbá megfelelőnek, relevánsnak és nem eltúlzottnak kell lenniük az adatkezelés céljaihoz képest, és elvben csak addig tárolhatók, ameddig az a személyes adatok kezelésének céljaihoz szükséges.

(21) Az *adatok sértetlensége és a célhoz kötöttség elve* ([33]) alapján a személyes adatok körét a kezelés célja szempontjából releváns mértékűre kell korlátozni. Ezenkívül a szervezeteknek az ilyen célokhoz szükséges mértékben megfelelő lépéseket kell tenniük annak biztosítására, hogy a személyes adatok a tervezett felhasználás szempontjából megbízhatók, pontosak, teljesek és naprakészek legyenek.

(22) A személyes adatok továbbá csak addig őrizhetők meg az adott egyén személyazonosságát meghatározó vagy azt lehetővé tévő formában (tehát személyes adatként) ([34]), amíg arra a célra/azokra a célokra szolgálnak, amely(ek)re eredetileg gyűjtötték őket, vagy amely(ek)et a *választási lehetőség* elve alapján később engedélyeztek. Ez a kötelezettség nem akadályozza meg a szervezeteket abban, hogy hosszabb ideig továbbra is kezeljék a személyes adatokat, azonban ezt csak addig és olyan mértékben tehetik, amennyire az ilyen adatkezelés az uniós adatvédelmi jog által biztosított kivételekhez hasonló alábbi konkrét célok valamelyikét szolgálja: közérdekű archiválás, újságírás, irodalom és művészet, tudományos és történeti kutatás, valamint statisztikai elemzés ([35]). A személyes adatok említett célokból történő hosszabb megőrzése esetén a kezelésük az elvek által nyújtott biztosítékok hatálya alá tartozik ([36]).

(23) A személyes adatokat továbbá olyan módon kell kezelni, amely biztosítja biztonságukat, többek között az illetéktelen vagy jogellenes kezelés elleni védelmüket, illetve az adatok véletlen elvesztése, megsemmisítése vagy károsodása elleni védelmüket. Az adatkezelőknek és az adatfeldolgozóknak ebből a célból megfelelő technikai vagy szervezeti intézkedéseket kell hozniuk, hogy a személyes adatokat a lehetséges veszélyektől megvédjék. Ezeket az intézkedéseket a technika állásának, a kapcsolódó költségeknek, az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint az egyének jogait érintő kockázatoknak a figyelembevételével kell értékelni.

([30]) I. melléklet II. szakasza 2. pontjának c. alpontja.
([31]) I. melléklet II. szakasza 2. pontjának c. alpontja.
([32]) I. melléklet III. szakaszának 1. pontja.
([33]) I. melléklet II. szakaszának 5. pontja.
([34]) Lásd az I. melléklet 7. lábjegyzetét, amely egyértelművé teszi, hogy az egyént „azonosíthatónak” kell tekinteni, amennyiben a szervezet vagy harmadik fél észszerűen azonosítani tudja az adott személyt, figyelembe véve az észszerű feltételezések alapján használható azonosítási eszközöket (figyelembe véve többek között az azonosításhoz szükséges költséget és időt, valamint az adatkezelés időpontjában rendelkezésre álló technológiát).
([35]) I. melléklet II. szakasza 5. pontjának b. alpontja.
([36]) *Uo.*

(24) Az EU–USA adatvédelmi keret értelmében ezt a *biztonság elve* biztosítja, amely az (EU) 2016/679 rendelet 32. cikkéhez hasonlóan előírja, hogy észszerű és megfelelő biztonsági intézkedéseket kell hozni, figyelembe véve az adatkezeléssel járó kockázatokat és az adatok jellegét ([37]).

2.2.4. *Átláthatóság*

(25) Az érintetteket tájékoztatni kell személyes adataik kezelésének főbb jellemzőiről.

(26) Ezt a *tájékoztatás elve* ([38]) biztosítja, amely – az (EU) 2016/679 rendelet szerinti átláthatósági követelményekhez hasonlóan – előírja a szervezetek számára, hogy tájékoztassák az érintetteket többek között i. a szervezet adatvédelmi keretben való részvételéről, ii. a gyűjtött adatok típusáról, iii. az adatkezelés céljáról, iv. azon harmadik felek típusáról vagy személyazonosságáról, amelyekkel vagy akikkel a személyes adatok közölhetők, valamint azok céljairól, v. egyéni jogaikról, vi. a szervezettel való kapcsolatfelvétel módjáról és vii. a rendelkezésre álló jogorvoslati lehetőségekről.

(27) Ezt a tájékoztatást világos és közérthető nyelven kell rendelkezésre bocsátani, amikor az egyéneket először kérik fel a személyes adatok közlésére, vagy azt követően a lehető leghamarabb, de mindenképpen azt megelőzően, hogy az adatokat az adatgyűjtés céljától lényegében eltérő (azonban összeegyeztethető) célra használják fel, vagy mielőtt azokat harmadik féllel megosztják ([39]).

(28) Ezen túlmenően a szervezeteknek nyilvánosságra kell hozniuk az elveket tükröző adatvédelmi szabályzataikat (vagy az emberi erőforrásokkal kapcsolatos adatok esetében azokat könnyen hozzáférhetővé kell tenniük az érintett személyek számára), és meg kell adniuk a Kereskedelmi Minisztérium honlapjára (további részletekkel a tanúsításról, az érintettek jogairól és a rendelkezésre álló jogorvoslati mechanizmusokról), az adatvédelmi keret szerinti jegyzékre és egy megfelelő alternatív vitarendezési szolgáltató weboldalára mutató linkeket ([40]).

2.2.5. *Az egyének jogai*

(29) Az érintetteknek rendelkezniük kell bizonyos jogokkal, amelyek érvényesíthetők az adatkezelővel vagy az adatfeldolgozóval szemben, különös tekintettel az adatokhoz való hozzáférés jogára, az adatkezelés elleni tiltakozásra, valamint az adatok helyesbítéséhez és töröltetéséhez való jogra.

(30) Az EU–USA adatvédelmi keret *hozzáférési elve* ([41]) ilyen jogokat biztosít az egyének számára. Az érintetteknek különösen jogukban áll – indokolás nélkül – megerősítést kérni a szervezettől arra vonatkozóan, hogy kezelik-e a rájuk vonatkozó személyes adatokat; az adatok közlését kérni; valamint információt szerezni az adatkezelés céljáról, a kezelendő személyes adatok kategóriáiról és azon címzettekről (azok kategóriáiról), akikkel az adatokat közlik ([42]). A szervezeteknek észszerű időn belül válaszolniuk kell a hozzáférési kérelmekre ([43]). A szervezet egy adott időszakon

([37]) I. melléklet II. szakasza 4. pontjának a. alpontja. Ezenkívül a humánerőforrás-adatok tekintetében az EU–USA adatvédelmi keret előírja a munkáltatók számára, hogy a személyes adatokhoz való hozzáférés korlátozásával, bizonyos adatok anonimizálásával, illetve kódok vagy álnevek kijelölésével alkalmazkodjanak a munkavállalók adatvédelmi preferenciáihoz (I. melléklet III. szakasza 9. pontja b. alpontjának (iii) alpontja).

([38]) I. melléklet II. szakaszának 1. pontja.

([39]) I. melléklet II. szakasza 1. pontjának b. alpontja. A 14. kiegészítő elv (I. melléklet III. szakasza 14. pontjának b. és c. alpontja) különös rendelkezéseket állapít meg a személyes adatoknak az egészségügyi kutatással és klinikai vizsgálatokkal összefüggésben történő kezelésére vonatkozóan. Ez az elv különösen azt teszi lehetővé a szervezetek számára, hogy a klinikai vizsgálati adatokat még azt követően is kezeljék, hogy egy személy kilépett a vizsgálatból, amennyiben ezt egyértelművé tették a tájékoztatóban, amikor az egyén beleegyezett a részvételbe. Hasonlóképpen, ha egy EU–USA adatvédelmi keretben részt vevő szervezet egészségügyi kutatási célból kap személyes adatokat, azokat csak a *tájékoztatás* és a *választási lehetőség* elveivel összhangban használhatja fel új kutatási tevékenységhez. Ebben az esetben az egyénnek szóló tájékoztatásnak elvben információt kell nyújtania az adatok bármilyen jövőbeli konkrét felhasználásáról (pl. kapcsolódó tanulmányokról). Amennyiben az adatok minden jövőbeli felhasználását nem lehet kezdettől fogva feltüntetni (mivel új kutatási felhasználás eredhet új meglátásokból vagy orvosi/kutatási fejlesztésekből), magyarázatot kell adni arra vonatkozóan, hogy az adatok felhasználhatók a jövőbeli, előre nem látható orvosi és gyógyszerészeti kutatási tevékenységek során. Ha az ilyen további felhasználás nem áll összhangban azzal az általános kutatási céllal, amelyre az adatokat gyűjtötték (azaz ha az új célok lényegesen eltérnek, de összeegyeztethetők az eredeti céllal, lásd a (14)–(15) preambulumbekezdést), új hozzájárulást kell beszerezni (azaz önkéntes részvétel). Lásd továbbá a 28. lábjegyzetben ismertetett, a *tájékoztatás* elve alóli egyedi korlátozásokat/kivételeket.

([40]) I. melléklet III. szakasza 6. pontjának d. alpontja.

([41]) Lásd még a „hozzáférésre” vonatkozó kiegészítő elvet (a II. melléklet III. szakaszának 8. pontja).

([42]) I. melléklet III. szakasza 8. pontja a. alpontjának (i)–(ii) alpontjai.

([43]) I. melléklet III. szakasza 8. pontja i. alpontja.

belül észszerű korlátozásokat állapíthat meg arra vonatkozóan, hogy egy adott személy hozzáférés iránti kérelmeinek hányszor kell eleget tennie, és nem túlzott összegű díjat számíthat fel, például ha a kérelmek nyilvánvalóan túlzóak, különösen ismétlődő jellegük miatt ([44]).

(31) A hozzáférési jog csak az uniós adatvédelmi jog által előírtakhoz hasonló kivételes körülmények között korlátozható, különösen akkor, ha mások törvényes jogai sérülnének; ha a hozzáférés biztosításának terhe vagy költsége az eset körülményei között aránytalan lenne az egyén magánéletét fenyegető kockázatokhoz képest (bár a költség és teher nem meghatározó tényező annak meghatározásakor, hogy a hozzáférés biztosítása észszerű-e); olyan mértékben, amennyiben a nyilvánosságra hozatal valószínűleg sérti az olyan fontos, egymással szemben álló közérdekek védelmét, mint a nemzetbiztonság, a közbiztonság vagy a védelem; ha az információ bizalmas kereskedelmi információt tartalmaz; vagy ha az információkat kizárólag kutatási vagy statisztikai célból kezelik ([45]). Egy jog megtagadásának vagy korlátozásának minden esetben szükségesnek kell lennie, és azt megfelelően indokolni kell, valamint az említett követelmények teljesülésének igazolása a szervezetet terheli ([46]). Ezen értékelés során a szervezetnek különösen az egyén érdekeit kell figyelembe vennie ([47]). Amennyiben lehetőség van az információk más olyan adatoktól való elkülönítésére, amelyekre korlátozás vonatkozik, a szervezetnek ki kell takarnia a védett információkat, és csak a fennmaradó információkat teheti közzé ([48]).

(32) Emellett az érintetteknek joguk van a pontatlan adatok helyesbítéséhez vagy módosításához, valamint az elvek megsértésével kezelt adatok törléséhez ([49]). Továbbá, amint azt a (15) preambulumbekezdés kifejti, az egyéneknek joguk van ahhoz, hogy tiltakozzanak adataiknak az adatgyűjtés céljától lényegesen eltérő (de összeegyeztethető) célból történő kezelése és az adataik harmadik felek részére történő közlése ellen. Ha a személyes adatokat közvetlen üzletszerzési célokra használják fel, az egyéneknek általános joguk van arra, hogy bármikor kimaradjanak az adatkezelésből ([50]).

(33) Az elvek nem foglalkoznak kifejezetten az érintettet érintő, kizárólag a személyes adatok automatizált kezelésén alapuló döntések kérdésével. Mindazonáltal az Európai Unióban gyűjtött személyes adatok vonatkozásában az automatizált kezelésen alapuló minden döntést általában az (érintettel közvetlen kapcsolatban álló) uniós adatkezelő fog meghozni, és így közvetlenül az (EU) 2016/679 rendelet hatálya alá tartozik ([51]). Idetartoznak olyan adattovábbítási forgatókönyvek, amelyek szerint az adatkezelést külföldi (például egyesült államokbeli) gazdasági szereplő végzi, aki az uniós adatkezelő megbízottjaként (adatfeldolgozóként) jár el (vagy további feldolgozóként azon uniós adatfeldolgozó nevében, amely az adatokat az azokat összegyűjtő uniós adatkezelőtől megkapta), és amely ezt követően ennek alapján hozza meg a döntést.

(34) Ezt megerősítette a Bizottság által az adatvédelmi pajzs ([52]) működésének második éves felülvizsgálata keretében 2018-ban megrendelt tanulmány, amely arra a következtetésre jutott, hogy akkoriban nem volt arra utaló bizonyíték, hogy az adatvédelmi pajzs keretében továbbított személyes adatok alapján az adatvédelmi pajzsban részt vevő szervezetek általában automatizált döntéshozatalt végeznek.

([44]) I. melléklet III. szakasza 8. pontja f. alpontjának (i)–(ii) alpontjai és a g. alpont.

([45]) I. melléklet III. szakaszának 4. pontja; 8. pontjának b., c., e. alpontjai; 14. pontjának e., f. alpontjai, és 15. pontjának d. alpontja.

([46]) I. melléklet III. szakasza 8. pontja e. alpontjának (ii) alpontja. A szervezetnek tájékoztatnia kell az egyént az elutasítás/korlátozás okairól, és kapcsolattartó pontot kell biztosítania a további vizsgálatokhoz (III. szakasz 8. pontja a. alpontjának (iii) alpontja).

([47]) I. melléklet III. szakasza 8. pontja a. alpontjának (ii)–(iii) alpontjai.

([48]) I. melléklet III. szakasza 8. pontja a. alpontjának (i) alpontja.

([49]) I. melléklet II. szakaszának 6. pontja és III. szakasza 8. pontja a. alpontjának (i) alpontja.

([50]) I. melléklet III. szakaszának 8.12. pontja.

([51]) Ezzel szemben abban a kivételes esetben, amikor az egyesült államokbeli szervezet közvetlen kapcsolatban van az uniós érintettel, ez általában annak a következménye, hogy uniós személyekre összpontosít áruk vagy szolgáltatások felkínálásával vagy viselkedésük nyomon követésével. E forgatókönyv szerint maga az egyesült államokbeli szervezet az (EU) 2016/679 rendelet hatálya alá fog tartozni (a 3. cikk (2) bekezdése), és így közvetlenül meg kell felelnie az uniós adatvédelmi jognak.

([52]) SWD(2018) 497 final, 4.1.5. szakasz. A tanulmány a következőkre összpontosított: i. az adatvédelmi pajzsban részt vevő egyesült államokbeli szervezetek milyen mértékben hoznak egyéneket érintő döntéseket az uniós vállalatoktól az adatvédelmi pajzs keretében továbbított személyes adatok automatizált kezelése alapján, és ii. az Egyesült Államok szövetségi joga által az egyénekre vonatkozóan előírt biztosítékok, valamint e biztosítékok alkalmazásának feltételei.

(35) Mindenesetre azokon a területeken, ahol a vállalatok a legvalószínűbben alkalmazzák a személyes adatok automatikus kezelését egyéneket érintő döntések meghozatalához (pl. hitelnyújtás, jelzáloghitel-ajánlatok, foglalkoztatás, lakhatás és biztosítás), az Egyesült Államok joga különleges védintézkedéseket biztosít a kedvezőtlen döntésekkel szemben ([53]). E jogszabályok általában úgy rendelkeznek, hogy az egyének jogosultak arra, hogy tájékoztatást kapjanak a döntés alapjául szolgáló konkrét okokról (pl. a hitelkérelem elutasításáról), vitassák a hiányos vagy pontatlan információkat (vagy jogellenes tényezők figyelembevételét) és jogorvoslatot igényeljenek. A fogyasztói hitelek területén a méltányos hitelminősítésről szóló törvény (FCRA) és az egyenlő hitellehetőségekről szóló törvény (ECOA) tartalmaz olyan biztosítékokat, amelyek valamilyen formában biztosítják a fogyasztók számára a magyarázathoz való jogot és a döntés megtámadásához való jogot. Ezek a törvények számos területen – többek között a hitel, a foglalkoztatás, a lakhatás és a biztosítás területén – relevánsak. Emellett egyes megkülönböztetésellenes jogszabályok – például a polgári jogokról szóló törvény VII. címe és a méltányos lakhatásról szóló törvény – védelmet biztosítanak az egyének számára az adott esetben bizonyos jellemzők alapján megkülönböztetéshez vezető automatizált döntéshozatalban használt modellek tekintetében, és biztosítják az egyének számára az ilyen döntések – köztük az automatizált döntések – megtámadásához való jogot. Az egészségügyi információk tekintetében az egészségbiztosítás hordozhatóságáról és elszámoltathatóságáról szóló törvény (HIPAA) adatvédelmi szabálya a személyes egészségügyi információkhoz való hozzáférés tekintetében az (EU) 2016/679 rendelethez hasonló jogokat hoz létre. Emellett az Egyesült Államok hatóságainak iránymutatása előírja az egészségügyi szolgáltatók számára, hogy olyan információkat kapjanak, amelyek lehetővé teszik számukra, hogy tájékoztassák az egyéneket az egészségügyi ágazatban használt automatizált döntéshozatali rendszerekről ([54]).

(36) Ezért ezek a szabályok az uniós adatvédelmi jog által biztosítotthoz hasonló védelmet nyújtanak abban a valószínűtlen helyzetben, amikor maga az EU–USA adatvédelmi keretben részt vevő szervezet hoz automatizált döntéseket.

2.2.6. ***Az újbóli adattovábbítás korlátozása***

(37) Az Európai Unióból az egyesült államokbeli szervezeteknek továbbított személyes adatok védelmi szintjét nem veszélyeztetheti az említett adatok Egyesült Államokon kívüli harmadik országokban található adatátvevők részére történő újbóli továbbítása.

(38) Az *újbóli továbbítással kapcsolatos elszámoltathatóságra vonatkozó elv* ([55]) szerint különös szabályok vonatkoznak az úgynevezett „harmadik fél részére történő adattovábbításra", vagyis arra, amikor az EU–USA adatvédelmi keretben részt vevő szervezettől harmadik fél adatkezelő vagy adatfeldolgozó részére továbbítanak személyes adatokat, függetlenül attól, hogy az utóbbi az Egyesült Államokban vagy az Egyesült Államokon (és az Unión) kívüli harmadik országban található-e. Az újbóli továbbításra csak i. korlátozott és meghatározott célokból kerülhet sor, ii. az EU–USA adatvédelmi keretben részt vevő szervezet és a harmadik fél közötti szerződés ([56]) alapján (vagy vállalatcsoporton belüli hasonló megállapodás ([57]) alapján), valamint iii. csak akkor, ha a szerződés előírja a harmadik fél számára, hogy ugyanolyan szintű védelmet nyújtson, mint az elvek által biztosított védelem.

(39) Az *adatintegritás és a célhoz kötöttség elvével* együtt értelmezett elvek által biztosítottal azonos szintű védelem biztosítására vonatkozó kötelezettség különösen azt jelenti, hogy a harmadik fél csak olyan célból kezelheti a részére továbbított személyes adatokat, amelyek nem összeegyeztethetetlenek azokkal a célokkal, amelyek érdekében az adatokat gyűjtötték, vagy amelyeket az egyén később engedélyezett (a *választási lehetőség* elvével összhangban).

([53]) Lásd pl. az egyenlő hitellehetőségről szóló törvényt (15 U.S.C. § 1691 és azt követő szakaszai), a méltányos hitelminősítésről szóló törvényt (15 U.S.C. § 1681 és azt követő szakaszai), vagy a méltányos lakhatásról szóló törvényt (42 U.S.C. § 3601 és azt követő szakaszai). Ezenkívül az Egyesült Államok csatlakozott a Gazdasági Együttműködési és Fejlesztési Szervezet mesterséges intelligenciára vonatkozó elveihez, amelyek többek között az átláthatóságra, az elmagyarázhatóságra, a biztonságra és az elszámoltathatóságra vonatkozó elveket is magukban foglalják.

([54]) Lásd a következő oldalon elérhető iránymutatást: 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Lásd az I. melléklet II. szakaszának 3. pontját és a „harmadik fél részére történő adattovábbításra vonatkozó kötelező szerződések" elnevezésű kiegészítő elvet (I. melléklet III. szakaszának 10. pontja).

([56]) Ezen általános elv alóli kivételként a szervezetek kis számú munkavállaló személyes adatait újból továbbíthatják anélkül, hogy szerződést kötnének a szolgáltatás igénybe vevőjével alkalmi, foglalkoztatással kapcsolatos operatív szükségletekre, például repülőjárat foglalására, szállodai szobafoglalásra vagy biztosítási fedezetre. A szervezetnek azonban ebben az esetben is meg kell felelnie a *tájékoztatás* és a *választási lehetőség* elveinek (lásd az I. melléklet III. szakasza 9. pontjának e) alpontját).

([57]) Lásd a „harmadik fél részére történő adattovábbításra vonatkozó kötelező szerződések" elnevezésű kiegészítő elvet (II. melléklet III. szakasza 10. pontjának b. alpontja). Bár ez az elv lehetővé teszi a nem szerződéses eszközökön (pl. vállalaton belüli megfelelőségi és ellenőrzési programokon) alapuló továbbításokat is, a szöveg egyértelművé teszi, hogy ezek az eszközök minden esetben kötelezően „biztosítják a személyes adatok védelmének a folytonosságát". Továbbá tekintettel arra, hogy a tanúsított amerikai vállalat változatlanul felelős lesz az elvek betartásáért, erős ösztönzést kap ahhoz, hogy olyan eszközöket alkalmazzon, amelyek valóban hatékonyak a gyakorlatban.

(40) Az *újbóli továbbítással kapcsolatos elszámoltathatóság elvét* a *tájékoztatás* és – harmadik fél adatkezelő részére történő adattovábbítás esetén ([58]) – a *választási lehetőség elvével* összefüggésben kell értelmezni, amelyek szerint az érintetteket tájékoztatni kell (többek között) bármely harmadik fél adatátvevő típusáról/kilétéről, a harmadik fél részére történő továbbítás céljáról, valamint a felkínált választási és kifogásolási (kívülmaradási) lehetőségről, vagy – érzékeny adatok esetén – „megerősítő kifejezett hozzájárulást" (részvétel) kell adni a harmadik fél részére történő adattovábbításokhoz.

(41) Az elvekben előírttal azonos szintű védelem biztosításának kötelezettsége az így továbbított adatok kezelésében részt vevő valamennyi harmadik félre vonatkozik, függetlenül az elhelyezkedésétől (az Egyesült Államokban vagy más, harmadik országban), valamint attól, hogy az eredeti harmadik fél adatátvevő maga továbbítja-e az említett adatokat más harmadik fél adatátvevőnek, például további kezelés céljából.

(42) A harmadik fél adatátvevővel kötött szerződésnek minden esetben elő kell írnia, hogy az utóbbi értesíti az EU–USA adatvédelmi keretben részt vevő szervezetet, ha megállapítja, hogy a továbbiakban nem tud megfelelni ennek a kötelezettségnek. Ha ilyen megállapítás történik, a harmadik fél általi adatkezelésnek meg kell szűnnie, vagy más észszerű és megfelelő lépéseket kell tenni a helyzet orvoslására ([59]).

(43) További védintézkedések alkalmazandók harmadik fél megbízott (azaz az adatfeldolgozó) részére történő adattovábbítás esetén. Ilyen esetben az egyesült államokbeli szervezetnek biztosítania kell, hogy a megbízott kizárólag az utasításai szerint járjon el, és észszerű és megfelelő lépéseket kell tennie i. annak biztosítására, hogy a megbízott ténylegesen olyan módon kezelje a továbbított személyes adatokat, amely összhangban van a szervezetet az elvek alapján terhelő kötelezettségekkel, valamint ii. azért, hogy az értesítést követően megszüntesse az engedély nélküli kezelést és helyreállítsa a korábbi helyzetet ([60]). A Kereskedelmi Minisztérium előírhatja a szervezet számára, hogy nyújtsa be a szerződés adatvédelmi rendelkezéseinek összefoglalóját vagy reprezentatív másolatát ([61]). Amennyiben egy (további) adatkezelési láncban megfelelési problémák merülnek fel, a személyes adatok kezelőjeként eljáró szervezetet terheli főszabály szerint a *jogorvoslat, végrehajtás és felelősség elvében* meghatározott felelősség, kivéve, ha bizonyítja, hogy nem felelős a kárt okozó eseményért ([62]).

2.2.7. ***Elszámoltathatóság***

(44) Az elszámoltathatóság elve értelmében az adatkezelőknek megfelelő technikai és szervezeti intézkedéseket kell hozniuk, hogy hatékonyan feleljenek meg adatvédelmi kötelezettségeiknek, és bizonyítani tudják ezt a megfelelést, különösen az illetékes felügyeleti hatóság felé.

(45) Ha egy szervezet önkéntesen az EU–USA adatvédelmi keret szerinti tanúsítás mellett dönt ([63]), az elvek tényleges betartása számára kötelező és végrehajtható. A *jogorvoslat, végrehajtás és felelősség elve* ([64]) értelmében az EU–USA adatvédelmi keretben részt vevő szervezeteknek hatékony mechanizmusokat kell biztosítaniuk az elveknek való megfelelés biztosítása érdekében. A szervezeteknek intézkedéseket kell hozniuk annak ellenőrzésére is ([65]), hogy adatvédelmi szabályzatuk összhangban áll az elvekkel és ténylegesen is megfelel azoknak. Ezt vagy önértékelési rendszer keretében tehetik meg, amelynek tartalmaznia kell az annak biztosítására irányuló eljárásokat, hogy az alkalmazottak képzésben részesüljenek a szervezet adatvédelmi szabályzatának végrehajtásáról, továbbá rendszeresen és objektíven felülvizsgálják a megfelelést, vagy pedig külső megfelelőségi felülvizsgálatok révén, amelyek módszerei közé tartozhatnak az ellenőrzések, a szúrópróbaszerű ellenőrzések vagy a technológiai eszközök használata.

([58]) Az egyének nem rendelkeznek majd kívülmaradási joggal, ha a személyes adatokat olyan harmadik félnek továbbítják, amely megbízottként jár el az egyesült államokbeli szervezet nevében és utasításai alapján. Ehhez azonban szerződésre van szükség a megbízott, valamint az egyesült államokbeli szervezet között, amely felelősséget fog viselni azért, hogy utasítási jogkörével élve garantálja az elvek szerint biztosított védintézkedéseket.

([59]) A helyzet eltérő attól függően, hogy a harmadik fél adatkezelő vagy adatfeldolgozó-e (megbízott). Az első esetben a harmadik féllel kötött szerződésben elő kell írni, hogy a harmadik fél megszünteti a kezelést vagy egyéb észszerű és megfelelő lépéseket tesz a helyzet orvoslására. A második esetben az EU–USA adatvédelmi keretben részt vevő szervezetnek – amely az általa adott utasítások alapján ellenőrzi a megbízott által végzett kezelést – feladata, hogy intézkedéseket hozzon. Lásd: I. melléklet II. szakaszának 3. pontja.

([60]) I. melléklet II. szakasza 3. pontjának b. alpontja.

([61]) *Uo.*

([62]) I. melléklet II. szakasza 7. pontjának d. alpontja.

([63]) Lásd továbbá az „öntanúsítás" kiegészítő elvet (az I. melléklet III. szakaszának 6. pontja).

([64]) Lásd továbbá a „vitarendezés és végrehajtás" kiegészítő elvet (az I. melléklet III. szakaszának 11. pontja).

([65]) Lásd továbbá az „ellenőrzés" kiegészítő elvet (az I. melléklet III. szakaszának 7. pontja).

(46) Ezen túlmenően a szervezeteknek nyilvántartást kell vezetniük az EU–USA adatvédelmi keret szerinti gyakorlataik végrehajtásáról, és azokat kérésre rendelkezésre kell bocsátaniuk egy független vitarendezési szervhez vagy illetékes végrehajtó hatósághoz benyújtott vizsgálat vagy a meg nem feleléssel kapcsolatos panasz keretében ([66]).

2.3. **Adminisztráció, felügyelet és végrehajtás**

(47) Az EU–USA adatvédelmi keretet a Kereskedelmi Minisztérium irányítja és követi nyomon. A keret felügyeleti és érvényesítési mechanizmusokat ír elő annak ellenőrzése és biztosítása céljából, hogy az EU–USA adatvédelmi keretben részt vevő vállalatok betartják az elveket és a megfelelés minden esetleges hiányosságát orvosolják. Ezeket a mechanizmusokat az elvek (I. melléklet), valamint a Kereskedelmi Minisztérium (III. melléklet), az FTC (IV. melléklet), és a Közlekedési Minisztérium (V. melléklet) által tett kötelezettségvállalások határozzák meg.

2.3.1. ***(Újra)tanúsítás***

(48) Az EU–USA adatvédelmi keret szerinti tanúsításhoz (vagy évente történő újratanúsításhoz) a szervezeteknek nyilvánosan nyilatkozniuk kell az elvek betartása iránti elkötelezettségükről, valamint elérhetővé kell tenniük és maradéktalanul végre kell hajtaniuk adatvédelmi szabályzataikat ([67]). A szervezeteknek (újra)tanúsítási kérelmük részeként információkat kell benyújtaniuk a Kereskedelmi Minisztériumhoz többek között az érintett szervezet nevéről, a személyes adatok szervezet általi kezelésének céljairól, a tanúsítás tárgyát képező személyes adatokról, valamint a választott ellenőrzési módszerről, a vonatkozó független jogorvoslati mechanizmusról és az elvek betartatására hatáskörrel rendelkező állami szervről ([68]).

(49) A szervezetek attól az időponttól kaphatnak személyes adatokat az EU–USA adatvédelmi keret alapján, amikor a Kereskedelmi Minisztérium felvette őket az adatvédelmi keretben részt vevő szervezetek listájára. A jogbiztonság biztosítása és a „hamis állítások" elkerülése érdekében az első alkalommal tanúsító szervezetek nem hivatkozhatnak nyilvánosan az elvekhez való csatlakozásukra, mielőtt a Kereskedelmi Minisztérium megállapította, hogy a szervezet tanúsításának benyújtása teljes, és a szervezetet felvette az adatvédelmi keretben részt vevő szervezetek listájára ([69]). Az ilyen szervezeteknek évente ismételten tanúsítaniuk kell az EU–USA adatvédelmi keretben való részvételüket, hogy továbbra is igénybe vehessék az adatvédelmi keretet az Unióból érkező személyes adatok fogadásához. Ha egy szervezet bármilyen okból kilép az EU–USA adatvédelmi keretből, el kell távolítania minden olyan állítást, amely arra utal, hogy a szervezet továbbra is részt vesz a keretben ([70]).

(50) Amint azt a III. mellékletben foglalt kötelezettségvállalások is tükrözik, a Kereskedelmi Minisztérium ellenőrzi, hogy a szervezetek megfelelnek-e az összes tanúsítási követelménynek, és életbe léptettek-e egy (nyilvános) adatvédelmi szabályzatot, amely tartalmazza a *tájékoztatás elvében* ([71]) előírt információkat. Az adatvédelmi pajzs szerinti (újra) tanúsítási folyamat során szerzett tapasztalatokra építve a Kereskedelmi Minisztérium számos ellenőrzést fog végezni, többek között annak ellenőrzése érdekében, hogy a szervezetek adatvédelmi szabályzata tartalmaz-e a vonatkozó vitarendezési mechanizmus honlapján található megfelelő panaszbejelentő űrlapra mutató hiperhivatkozást, és amennyiben egy szervezet több szervezetét és leányvállalatát is feltüntetik a tanúsítási beadványban, hogy e szervezetek mindegyikének adatvédelmi szabályzata megfelel-e a tanúsítási követelményeknek, és könnyen hozzáférhető-e az érintettek számára ([72]). Ezen túlmenően a Kereskedelmi Minisztérium szükség esetén keresztellenőrzéseket végez az FTC-vel és a Közlekedési Minisztériummal annak ellenőrzése érdekében, hogy a szervezetek az (újra)tanúsítási beadványaikban azonosított felügyeleti testület hatálya alá tartoznak-e, és együttműködik az alternatív vitarendezési szervekkel annak ellenőrzése érdekében, hogy a szervezeteket nyilvántartásba vették-e az (újra)tanúsítási beadványukban azonosított független jogorvoslati mechanizmus tekintetében ([73]).

([66]) I. melléklet III. szakaszának 7. pontja.
([67]) I. melléklet I. szakaszának 2. pontja.
([68]) I. melléklet III. szakasza 6. pontjának b. alpontja és III. melléklet, lásd „Az öntanúsítási követelmények ellenőrzése" szakaszt.
([69]) I. melléklet, 12. lábjegyzet.
([70]) I. melléklet III. szakasza 6. pontjának h. alpontja.
([71]) I. melléklet III. szakasza 6. pontjának a. alpontja és 12. lábjegyzet, valamint III. melléklet, lásd „Az öntanúsítási követelmények ellenőrzése" szakaszt.
([72]) III. melléklet, „Az öntanúsítási követelmények ellenőrzése" című szakasz.
([73]) Hasonlóképpen, a Kereskedelmi Minisztérium együttműködik azzal a harmadik féllel, amely az adatvédelmi hatóság testületének fizetett díj révén beszedett pénzeszközök letétkezelője lesz (lásd a (73) preambulumbekezdést), annak ellenőrzése érdekében, hogy az adatvédelmi hatóságokat független jogorvoslati mechanizmusként választó szervezetek az adott évre megfizették-e a díjat. Lásd a III. melléklet „Az öntanúsítási követelmények ellenőrzése" című szakaszát.

(51) A Kereskedelmi Minisztérium tájékoztatja a szervezeteket, hogy az (újra)tanúsítás elvégzése érdekében foglalkozniuk kell a felülvizsgálat során azonosított valamennyi kérdéssel. Abban az esetben, ha a szervezet nem válaszol a Kereskedelmi Minisztérium által meghatározott határidőn belül (például az újratanúsítás tekintetében az elvárás, hogy a folyamat 45 napon belül befejeződjön) ([74]), vagy egyéb esetben nem fejezi be a tanúsítást, a beadványt visszavontnak kell tekinteni. Ebben az esetben az EU–USA adatvédelmi keretben való részvétellel vagy az annak való megfeleléssel kapcsolatos bármilyen megtévesztés az FTC vagy a Közlekedési Minisztérium végrehajtási intézkedésének tárgyát képezheti ([75]).

(52) Az EU–USA adatvédelmi keret megfelelő alkalmazása érdekében az érdekelt feleknek, például az érintetteknek, az adatátadóknak és a nemzeti adatvédelmi hatóságoknak tudniuk kell azonosítani az elveket elfogadó szervezeteket. Az ilyen átláthatóság belépő ponton való biztosítása érdekében a Kereskedelmi Minisztérium vállalta az olyan szervezetek listájának vezetését és a nyilvánosság számára hozzáférhetővé tételét, amelyek tanúsították az elvek elfogadását, és az e határozat IV. és V. mellékletében említettek közül legalább egy végrehajtó hatóság hatáskörébe tartoznak ([76]). A Kereskedelmi Minisztérium frissíti a listát a szervezetek éves ismételt tanúsítási beadványai alapján, és valahányszor egy szervezet kilép vagy törlésre kerül az EU–USA adatvédelmi keretből. Ezenkívül az átláthatóság kilépési helyen történő biztosítása érdekében a Kereskedelmi Minisztérium vezeti továbbá a listáról eltávolított szervezetek nyilvános és hiteles listáját, amely minden esetben meghatározza az ilyen eltávolítás okát ([77]). Végül pedig az FTC EU–USA adatvédelmi keretről szóló weblapjára mutató hivatkozást biztosít, amely felsorolja az FTC által a keret alapján hozott jogérvényesítési intézkedéseket ([78]).

2.3.2. ***Megfelelés-ellenőrzés***

(53) A Kereskedelmi Minisztérium folyamatosan nyomon követi, hogy az EU–USA adatvédelmi keretben részt vevő szervezetek különböző mechanizmusokon keresztül ténylegesen megfelelnek-e az elveknek ([79]). Különösen „szúrópróbaszerű ellenőrzéseket" végez a véletlenszerűen kiválasztott szervezeteknél, valamint eseti szúrópróbaszerű ellenőrzéseket bizonyos szervezeteknél, amikor potenciális megfelelési problémákat tárnak fel (pl. harmadik felek jelentést tesznek a Kereskedelmi Minisztériumnak) annak ellenőrzése érdekében, hogy i. rendelkezésre állnak-e a panaszok és az érintettek kérelmeinek kezelésére szolgáló kapcsolattartó pontok, és reagálnak-e, ii. a szervezet adatvédelmi szabályzata könnyen elérhető-e mind a honlapján, mind a Kereskedelmi Minisztérium honlapján található hiperhivatkozáson keresztül, iii. a szervezet adatvédelmi szabályzata továbbra is megfelel-e a tanúsítási követelményeknek, és iv. a szervezetek által választott független vitarendezési mechanizmus rendelkezésre áll-e a panaszok kezelésére ([80]).

(54) Ha hitelt érdemlő bizonyíték van arra, hogy egy szervezet nem tesz eleget az EU–USA adatvédelmi keret szerinti kötelezettségvállalásainak (ideértve azt az esetet is, ha a Kereskedelmi Minisztériumhoz panasz érkezik, vagy ha a szervezet nem válaszol kielégítő módon a Kereskedelmi Minisztérium kérdéseire), a Kereskedelmi Minisztérium előírja a szervezet számára, hogy töltsön ki és nyújtson be részletes kérdőívet ([81]). Azt a szervezetet, amely nem válaszol megfelelően és időben a kérdőívre, az illetékes hatósághoz (az FTC-hez vagy Közlekedési Minisztériumhoz) utalják esetleges végrehajtási intézkedés céljából ([82]). Az adatvédelmi pajzs keretében végzett megfelelés-ellenőrzési

([74]) III. melléklet, 2. lábjegyzet.
([75]) Lásd a III. melléklet „Az öntanúsítási követelmények ellenőrzése" című szakaszát.
([76]) Az adatvédelmi keretben részt vevő szervezetek listájának kezelésére vonatkozó információk a III. mellékletben (lásd „Az adatvédelmi keretprogramnak a Kereskedelmi Minisztérium általi igazgatása és felügyelete" című bevezetőt) és az I. mellékletben (I. szakasz 3. pont, I. szakasz 4. pont, III. szakasz 6. pont d. alpont és III. szakasz 11. pont g. alpont) találhatók.
([77]) III. melléklet, lásd „Az adatvédelmi keretprogramnak a Kereskedelmi Minisztérium általi igazgatása és felügyelete" című bevezetőt.
([78]) Lásd a III. melléklet „Az adatvédelmi keret weboldalának a célközönségekhez igazítása" című szakaszát.
([79]) Lásd a III. melléklet „Az adatvédelmi keretprogram rendszeres, hivatalból végzett megfelelési felülvizsgálatai és értékelései" című szakaszát.
([80]) Nyomonkövetési tevékenységeinek részeként a Kereskedelmi Minisztérium különböző eszközöket használhat, többek között az adatvédelmi szabályzatokra mutató hibás hivatkozások ellenőrzésére, vagy a meg nem felelést hitelt érdemlően bizonyító jelentésekről szóló hírek aktív nyomon követésére.
([81]) Lásd a III. melléklet „Az adatvédelmi keretprogram rendszeres, hivatalból végzett megfelelési felülvizsgálatai és értékelései" című szakaszát.
([82]) Lásd a III. melléklet „Az adatvédelmi keretprogram rendszeres, hivatalból végzett megfelelési felülvizsgálatai és értékelései" című szakaszát.

tevékenységei részeként a Kereskedelmi Minisztérium rendszeresen elvégezte az (53) preambulumbekezdésben említett szúrópróbaszerű ellenőrzéseket, és folyamatosan nyomon követte a nyilvános jelentéseket, ami lehetővé tette számára a megfelelési problémák azonosítását, kezelését és megoldását ([83]). Azokat a szervezeteket, amelyek tartósan nem felelnek meg az elveknek, el fogják távolítani az adatvédelmi keretben részt vevő szervezetek listájáról, és vissza kell szolgáltatniuk vagy törölniük kell a keret szerint kapott személyes adatokat ([84]).

(55) Az eltávolítás egyéb eseteiben – például a részvételből való önkéntes kilépés vagy az ismételt tanúsítás elmulasztása esetén – a szervezet köteles törölni vagy visszajuttatni az adatokat, vagy megőrizheti azokat, ha évente megerősíti a Kereskedelmi Minisztérium számára azt a kötelezettségvállalását, hogy továbbra is alkalmazza az elveket, vagy egyéb engedélyezett eszközökkel megfelelő védelmet nyújt a személyes adatok számára (pl. olyan szerződéssel, amely teljes mértékben tükrözi a Bizottság által jóváhagyott vonatkozó általános szerződési feltételeket) ([85]). Ebben az esetben a szervezetnek meg kell határoznia a szervezeten belül az EU–USA adatvédelmi kerettel kapcsolatos kérdések megválaszolására szolgáló kapcsolattartó pontot.

2.3.3. *A hamis részvételi nyilatkozatok azonosítása és kezelése*

(56) A Kereskedelmi Minisztérium mind hivatalból, mind (pl. az adatvédelmi hatóságoktól kapott) panaszok alapján nyomon fogja követni az EU–USA adatvédelmi keretben való részvételre vonatkozó hamis állításokat vagy az EU–USA adatvédelmi keret szerinti tanúsító védjegy nem megfelelő használatát ([86]). A Kereskedelmi Minisztérium folyamatosan ellenőrzi különösen azt, hogy azok a szervezetek, amelyek i. kilépnek az EU–USA adatvédelmi keretben való részvételből, ii. nem végezték el az éves újratanúsítást (azaz vagy megkezdték, de nem fejezték be időben az éves újratanúsítási folyamatot, vagy el sem kezdték azt), iii. résztvevőként eltávolításra kerülnek, különösen „tartós meg nem felelés miatt", vagy iv. nem fejezték be az első tanúsítást (azaz megkezdték, de nem fejezték be időben az első tanúsítási folyamatot), töröljék a közzétett adatvédelmi szabályzataikból az EU–USA adatvédelmi keretre vonatkozó hivatkozásokat, amelyek arra utalnak, hogy a szervezet aktívan részt vesz a keretrendszerben ([87]). A Kereskedelmi Minisztérium internetes kereséseket is végez annak érdekében, hogy azonosítsa az EU–USA adatvédelmi keretre való hivatkozásokat a szervezetek adatvédelmi szabályzataiban, többek között az olyan szervezetek hamis állításainak azonosítása céljából, amelyek soha nem vettek részt az EU–USA adatvédelmi keretben ([88]).

(57) Amennyiben a Kereskedelmi Minisztérium megállapítja, hogy az EU–USA adatvédelmi keretre való hivatkozásokat nem törölték vagy nem megfelelően használják, tájékoztatja a szervezetet az FTC/Közlekedési Minisztérium esetleges megkereséséről ([89]). Ha egy szervezet nem ad határozott választ, a Kereskedelmi Minisztérium esetleges végrehajtási intézkedés céljából az illetékes ügynökséghez utalja az ügyet ([90]). Az FTC, a Közlekedési Minisztérium vagy egyéb érintett amerikai végrehajtó hatóságok végrehajtási intézkedést hoznak, ha egy szervezet az elvek általa történő elfogadásával kapcsolatos, félrevezető nyilatkozatokkal vagy gyakorlatokkal megtéveszti a közvéleményt. A Kereskedelmi Minisztériumnak adott hamis közlések a hamis nyilatkozatokról szóló törvény (18 U.S.C. § 1001) alapján perelhetők.

([83]) Az adatvédelmi pajzs második éves felülvizsgálata során a Kereskedelmi Minisztérium arról tájékoztatott, hogy 100 szervezetnél végzett szúrópróbaszerű ellenőrzést, és 21 esetben küldött megfelelőségi kérdőívet (amelyet követően a feltárt problémákat orvosolták), lásd: SWD(2018) 497 final bizottsági szolgálati munkadokumentum, 9. o. Hasonlóképpen, a Kereskedelmi Minisztérium az adatvédelmi pajzs harmadik éves felülvizsgálata során arról számolt be, hogy a nyilvános jelentések nyomon követése révén három incidenst tárt fel, és elindította azt a gyakorlatot, hogy havonta 30 vállalatnál szúrópróbaszerű ellenőrzéseket végez, ami az esetek 28 %-ában megfelelőségi kérdőívekhez vezetett (amit követően a feltárt problémákat azonnal orvosolták, vagy három esetben figyelmeztető levelet követően megoldották), lásd: SWD(2019) 495 final bizottsági szolgálati munkadokumentum, 8. o.

([84]) I. melléklet III. szakasza 11. pontjának g. alpontja. Az előírásoknak való folyamatos meg nem felelés különösen akkor merül fel, ha a szervezet megtagadja a magánélet védelmével kapcsolatos önszabályozó, független vitarendezési vagy jogalkalmazó hatóság végső döntésének való megfelelést.

([85]) I. melléklet III. szakasza 6. pontjának f. alpontja.

([86]) Lásd a III. melléklet „Hamis részvételi nyilatkozatok keresése és kezelése" című szakaszát.

([87]) *Uo.*

([88]) *Uo.*

([89]) *Uo.*

([90]) Az adatvédelmi pajzs keretében a Kereskedelmi Minisztérium a keret harmadik éves felülvizsgálata során arról számolt be, hogy 669 hamis részvételi nyilatkozatot azonosított (2018 októbere és 2019 októbere között), amely ügyek többségét a Kereskedelmi Minisztérium figyelmeztető levele után megoldották, és 143 ügyet utaltak az FTC elé (lásd az alábbi (62) preambulumbekezdést). Lásd: SWD(2019) 495 final bizottsági szolgálati munkadokumentum, 10. o.

2.3.4. ***Végrehajtás***

(58) Az adatvédelem megfelelő szintjének gyakorlati biztosítása érdekében létre kell hozni egy független felügyeleti hatóságot, amely hatáskörrel rendelkezik az adatvédelmi szabályoknak való megfelelés nyomon követésére és kikényszerítésére.

(59) Az EU–USA adatvédelmi keretben részt vevő szervezeteknek az illetékes amerikai hatóságok – az FTC és a Kereskedelmi Minisztérium – joghatósága alá kell tartozniuk, amelyek rendelkeznek az elveknek való megfelelés hatékony biztosításához szükséges vizsgálati és végrehajtási hatáskörökkel ([91]).

(60) Az FTC független hatóság, amely öt biztosból áll, akiket az elnök nevez ki a Szenátus tanácsa alapján és egyetértésével ([92]). A biztosokat hét évre nevezik ki, és azokat az elnök csak nem hatékony munkavégzés, hivatali mulasztás vagy hivatali visszaélés miatt mentheti fel. Az FTC ugyanazon politikai pártból legfeljebb három biztossal rendelkezhet, a biztosok pedig kinevezésük ideje alatt nem folytathatnak más tevékenységet, hivatást vagy munkát.

(61) Az FTC kivizsgálhatja az elveknek való megfelelést, valamint az elvek betartására vagy az EU–USA adatvédelmi keretben való részvételre vonatkozó hamis állításokat olyan szervezetek részéről, amelyek már nem szerepelnek az adatvédelmi keret szerinti listán, vagy amelyeket soha nem tanúsítottak ([93]). Az FTC úgy érvényesítheti a megfelelést, hogy közigazgatási vagy szövetségi bírósági végzéseket (ideértve az egyezségek útján hozott „hozzájárulási végzéseket") ([94]) kér előzetes vagy állandó intézkedések vagy egyéb jogorvoslatok iránt, és rendszeresen nyomon követi az ilyen végzéseknek való megfelelést ([95]). Ha a szervezetek nem tartják be ezeket a végzéseket, az FTC polgári jogi szankciókat vagy egyéb jogorvoslatokat igényelhet, többek között a jogellenes cselekmény okozta károk megtérítését követelheti. Az EU–USA adatvédelmi keretben részt vevő szervezetek számára kiadott mindegyik hozzájárulási végzés önbejelentési rendelkezéseket tartalmaz majd ([96]), és arra fogja kötelezni a szervezeteket, hogy hozzák nyilvánosságra az FTC-hez benyújtott valamennyi megfelelési vagy értékelő jelentésnek az EU–USA adatvédelmi kerettel kapcsolatos, lényeges szakaszait. Végezetül az FTC fenntartja majd azoknak a szervezeteknek az online listáját, amelyek az FTC vagy valamely bíróság EU–USA adatvédelmi kerettel kapcsolatos ügyekben hozott végzéseinek hatálya alá tartoznak ([97]).

(62) Ami az adatvédelmi pajzsot illeti, az FTC mintegy 22 esetben tett végrehajtási intézkedést, mind a keretrendszer konkrét követelményeinek megsértése tekintetében (pl. nem erősítette meg a Kereskedelmi Minisztérium felé, hogy a szervezet a keretből való kilépését követően is alkalmazta az adatvédelmi pajzs védelmét, önértékelés vagy külső megfelelőségi felülvizsgálat útján nem tudta ellenőrizni, hogy a szervezet megfelelt-e a keretrendszernek) ([98]), mind pedig a keretrendszerben való részvételre vonatkozó hamis állítások tekintetében (pl. olyan szervezetek részéről, amelyek elmulasztották megtenni a tanúsítás megszerzéséhez szükséges lépéseket, vagy hagyták, hogy tanúsításuk lejárjon, de hamisan úgy nyilatkoztak, hogy részvételük továbbra is fennáll) ([99]). Ez a végrehajtási intézkedés többek között abból eredt, hogy a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatokat proaktívan arra használták, hogy az adatvédelmi pajzs egyes résztvevőitől anyagokat szerezzenek be az adatvédelmi pajzsban foglalt kötelezettségek lényeges megsértésének ellenőrzése céljából ([100]).

([91]) Az EU–USA adatvédelmi keretben részt vevő szervezetnek nyilvánosan közzé kell tennie azt a kötelezettségvállalását, hogy teljesíti az elveket, közzéteszi az említett elveknek megfelelő adatvédelmi szabályzatát és teljeskörűen végrehajtja azt. Az FTC-ről szóló törvény tisztességtelen vagy megtévesztő kereskedelmi vagy kereskedelmet érintő gyakorlatokat tiltó 5. szakasza (a 15 U.S.C. § 45) és a 49 U. S.C.-nek a fuvarozók és a jegyértékesítők számára a légi közlekedés vagy a légi közlekedés értékesítése során a tisztességtelen vagy megtévesztő gyakorlatok folytatásának tilalmáról szóló § 41712 alapján a teljesítés elmulasztásával szemben jogérvényesítésnek helye van.

([92]) 15 U.S.C. § 41.

([93]) IV. melléklet.

([94]) Az FTC-től származó információk szerint a Szövetségi Kereskedelmi Bizottság az adatvédelem területén nem rendelkezik hatáskörrel helyszíni vizsgálatok lefolytatására. Hatásköre azonban kiterjed arra, hogy dokumentumok és írásbeli nyilatkozatok megküldésére kötelezze a szervezeteket (lásd az FTC-ről szóló törvény 20. szakaszát), és a bírósági rendszert is igénybe veheti e végzések kikényszerítésére nem teljesítés esetén.

([95]) Lásd a IV. melléklet „Végzések keresése és nyomon követése" című szakaszát.

([96]) Az FTC vagy valamely bíróság végzései arra kötelezhetik a vállalatokat, hogy adatvédelmi programokat hajtsanak végre, és rendszeres megfelelési jelentéseket vagy a szóban forgó programokról független harmadik fél által készített értékeléseket bocsássanak az FTC rendelkezésére.

([97]) A IV. melléklet „Végzések keresése és nyomon követése" című szakasza.

([98]) SWD(2019) 495 final bizottsági szolgálati munkadokumentum, 11. o.

([99]) Lásd az FTC honlapján felsorolt ügyeket, amelyek a https://www.ftc.gov/business-guidance/privacy-security/privacy-shield címen érhetők el. Lásd továbbá: SWD(2017) 344 final bizottsági szolgálati munkadokumentum, 17. o; SWD(2018) 497 final bizottsági szolgálati munkadokumentum, 12. o., valamint SWD(2019) 495 final bizottsági szolgálati munkadokumentum, 11. o.

([100]) Lásd például Joseph Simons elnök által az adatvédelmi pajzs második éves áttekintése során készített észrevételeket (ftc.gov).

(63) Általánosabban az FTC az elmúlt években számos esetben tett végrehajtási intézkedéseket az EU–USA adatvédelmi keretben is előírt konkrét adatvédelmi követelményeknek való megfeleléssel kapcsolatban, például a célhoz kötöttség és az adatmegőrzés ([101]), az adatminimalizálás ([102]), az adatbiztonság ([103]) és az adatpontosság ([104]) elve tekintetében.

(64) A Közlekedési Minisztérium kizárólagos jogkörrel rendelkezik a légitársaságok adatvédelmi gyakorlatainak a szabályozására, és az FTC-vel közös hatásköre van a jegyértékesítők légi közlekedés értékesítése során folytatott adatvédelmi gyakorlata tekintetében. A Közlekedési Minisztérium tisztségviselőinek célja először az egyezség elérése, és amennyiben ez nem lehetséges, végrehajtási eljárást indíthatnak, amely magában foglalja a Közlekedési Minisztérium közigazgatási bírája előtt lefolytatott bizonyításfelvételt, aki jogosult megszüntető végzéseket kibocsátani és polgári jogi szankciókat kiszabni ([105]). A közigazgatási bírák a közigazgatási eljárásról szóló törvény (APA) értelmében számos módon részesülnek védelemben függetlenségük és pártatlanságuk biztosítása érdekében. Például csak megalapozott indokkal lehet őket elbocsátani; rotációs alapon vannak ügyekhez rendelve; nem láthatnak el olyan feladatokat, amelyek nem egyeztethetők össze közigazgatási bírói feladataikkal és felelősségükkel; nem állnak az őket alkalmazó hatóság (ebben az esetben a Közlekedési Minisztérium) vizsgálati csoportjának felügyelete alatt; és pártatlanul kell ellátniuk igazságszolgáltatási/végrehajtási feladataikat ([106]). A Közlekedési Minisztérium kötelezettséget vállalt arra, hogy nyomon követi a végrehajtási végzéseket, és biztosítja, hogy az EU–USA adatvédelmi keret szerinti ügyekből származó végzések elérhetők legyenek a honlapján ([107]).

2.4. **Jogorvoslat**

(65) A megfelelő védelem, és különösen a személyhez fűződő jogok érvényesítésének biztosítása érdekében az érintettnek hatékony közigazgatási és bírósági jogorvoslatot kell biztosítani.

(66) Az EU–USA adatvédelmi keret a *jogorvoslat, végrehajtás és felelősség elve* révén arra kötelezi a szervezeteket, hogy biztosítsanak jogorvoslati lehetőséget a meg nem felelés által érintett egyéneknek, és így tegyék lehetővé az uniós érintetteknek, hogy panaszt nyújtsanak be az EU–USA adatvédelmi keretben részt vevő szervezetek megfelelésének hiányával kapcsolatban, továbbá hogy szükség esetén hatékony jogorvoslatot biztosító határozatokkal kényszerítsék ki e panaszok rendezését ([108]). A szervezeteknek a tanúsításuk részeként eleget kell tenniük ennek az elvnek azáltal, hogy hatékony és könnyen igénybe vehető, független jogorvoslati mechanizmusokat biztosítanak, amelyek keretében minden egyén panaszai és jogvitái kivizsgálhatók és gyorsan megoldhatók anélkül, hogy ez költséget jelentene az egyén számára ([109]).

([101]) Lásd pl. az FTC Drizly, LLC. ügyben hozott végzését, amely többek között előírja a vállalat számára, hogy 1. semmisítse meg az általa gyűjtött olyan személyes adatokat, amelyek nem szükségesek ahhoz, hogy a fogyasztóknak termékeket vagy szolgáltatásokat nyújtson, 2. tartózkodjon a személyes adatok gyűjtésétől vagy tárolásától, kivéve, ha ez a megőrzési ütemtervben meghatározott konkrét célokból szükséges.

([102]) Lásd pl. az FTC CafePress ügyben hozott végzését (2022. március 24.), amely többek között előírja az összegyűjtött adatok mennyiségének minimalizálását.

([103]) Lásd például az FTC Drizzly, LLC és CafePress ügyben hozott jogérvényesítési intézkedését, amelyben az érintett vállalatoktól célzott biztonsági program vagy konkrét biztonsági intézkedések bevezetését írta elő. Emellett az adatvédelmi incidenseket illetően lásd még az FTC Chegg ügyben 2023. január 27-én hozott végzését, a 2019-ben az Equifaxszal kötött egyezség kapcsán (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Lásd pl. a RealPage, Inc. ügyet (2018. október 16.), amelyben az FTC végrehajtási intézkedést hozott az FCRA alapján egy olyan bérlőátvizsgáló vállalat szemben, amely magánszemélyekről szóló háttérjelentéseket nyújtott be az ingatlantulajdonosoknak és ingatlankezelő társaságoknak a bérleti előzményekből származó információk, a nyilvános nyilvántartási információk (többek között bűnügyi és kilakoltatási előzmények) és a hitelinformációk alapján, amelyek jelentéseket a lakhatásra való jogosultság megállapításához használt tényezőként alkalmaztak. Az FTC megállapította, hogy a vállalat nem tett észszerű intézkedéseket az automatikus döntéshozatali eszköze alapján szolgáltatott információk pontosságának biztosítása érdekében.

([105]) Lásd az V. melléklet „Végrehajtási gyakorlatok” című szakaszát.

([106]) Lásd: 5 U.S.C. §§ 3105, 7521(a), 554(d) és 556(b)(3).

([107]) V. melléklet, lásd „Az EU–USA adatvédelmi keret megsértésére vonatkozó hatósági végrehajtási végzések nyomon követése és végrehajtása” című szakaszt.

([108]) I. melléklet II. szakaszának 7. pontja.

([109]) I. melléklet III. szakaszának 11. pontja.

(67) A szervezetek az Unióban vagy az Egyesült Államokban található független jogorvoslati mechanizmusokat választhatják. Amint azt a (73) preambulumbekezdés részletesebben kifejti, ez magában foglalja az uniós adatvédelmi hatóságokkal való együttműködés önkéntes vállalásának lehetőségét is. Amennyiben a szervezetek emberi erőforrásokra vonatkozó adatokat kezelnek, az uniós adatvédelmi hatóságokkal való együttműködésre vonatkozó kötelezettségvállalás kötelező. A további alternatívák közé tartoznak a független, alternatív vitarendezés vagy azok a magánszektorban kidolgozott adatvédelmi programok, amelyek az elveket beépítik a szabályozásukba. Az utóbbiaknak hatékony jogérvényesítési mechanizmusokat kell tartalmazniuk a *jogorvoslat, végrehajtás és felelősség elve* követelményeinek megfelelően.

(68) Következtetésképpen az EU–USA adatvédelmi keret számos lehetőséget kínál az érintetteknek, hogy érvényesítsék a jogaikat, panaszt nyújtsanak be az EU–USA adatvédelmi keretben részt vevő szervezetek meg nem felelésével kapcsolatban, továbbá hogy szükség esetén hatékony jogorvoslatot biztosító határozatokkal kényszerítsék ki e panaszok rendezését. Az egyének közvetlenül a szervezethez, a szervezet által kijelölt független vitarendezési szervhez, a nemzeti adatvédelmi hatóságokhoz, a Kereskedelmi Minisztériumhoz vagy az FTC-hez nyújthatják be panaszukat. Ha a fenti jogorvoslati vagy jogérvényesítési mechanizmusok egyike sem vezet a panaszaik rendezéséhez, az egyének jogosultak továbbá igénybe venni a kötelező választottbíráskodást is (e határozat I. mellékletének I. melléklete). A választott bírói testület kivételével, amelynek igénybevételéhez egyes jogorvoslati lehetőségek kimerítése szükséges, az egyének szabadon döntenek arról, hogy igénybe veszik-e az összes jogorvoslati mechanizmust vagy azok valamelyikét, és nem kötelesek bármelyik mechanizmust előnyben részesíteni a többivel szemben vagy egy konkrét sorrendet követni.

(69) Az uniós érintettek először az EU–USA adatvédelmi keretben részt vevő szervezetekkel való közvetlen kapcsolatfelvétel révén indíthatnak eljárást az elvek be nem tartása miatt ([110]). A panaszok rendezésének megkönnyítése érdekében a szervezetnek hatékony jogorvoslati mechanizmust kell kialakítania az ilyen panaszok elbírálására. Az adott szervezet adatvédelmi szabályzatában tehát egyértelműen tájékoztatni kell az egyéneket a panaszokat kezelő, szervezeten belüli vagy azon kívüli kapcsolattartó pontról, (így az Unión belüli bármely érintett szervezetről, amely választ adhat a kérdésekre vagy panaszokra), valamint a kijelölt független vitarendezési szervről (lásd a (70) preambulumbekezdést). A szervezetnek 45 napos időszakon belül választ kell adnia az uniós érintettnek, miután közvetlenül az adott egyéntől vagy egy adatvédelmi hatóság utalását követően a Kereskedelmi Minisztérium közvetítésével kézhez kapta az illető panaszát ([111]). Ehhez hasonlóan a szervezetek kötelesek gyorsan választ adni a Kereskedelmi Minisztériumtól vagy egy adatvédelmi hatóságtól ([112]) (ha a szervezet kötelezettséget vállalt az adatvédelmi hatósággal való együttműködésre) érkező, az elvek általuk történő elfogadásával kapcsolatos megkeresésekre és egyéb információkérésekre.

(70) Másrészt az egyének a panaszt közvetlenül is benyújthatják ahhoz a független vitarendezési szervhez (az Egyesült Államokban vagy az Unióban), amelyet az adott szervezett azért jelölt ki, hogy kivizsgálja és rendezze az egyéni panaszokat (ha azok nem egyértelműen megalapozatlanok vagy komolytalanok) és megfelelő ingyenes jogorvoslatot biztosítson az egyének számára ([113]). Az ilyen szervek által kiszabott szankcióknak és jogorvoslatoknak eléggé szigorúaknak kell lenniük ahhoz, hogy a szervezetek betartsák az elveket, továbbá rendelkezniük kell arról, hogy a szervezetnek vissza kell fordítania vagy ki kell igazítania a megfelelés elmulasztásának hatását, valamint a körülményektől függően elő kell írniuk a szóban forgó személyes adatok további kezelésének megszüntetését vagy az adatok törlését, és a meg nem felelésre vonatkozó megállapítások nyilvánosságát ([114]). A szervezetek által kijelölt független vitarendezési szervek kötelesek feltüntetni a nyilvános weboldalaikon az EU–USA adatvédelmi kerettel kapcsolatos lényeges információkat, valamint az annak alapján általuk nyújtott szolgáltatásokat ([115]). Évente közzé kell tenniük egy éves jelentést, amelyben összesített statisztikai adatokat közölnek ezekről a szolgáltatásokról ([116]).

([110]) I. melléklet III. szakasza 11. pontja d. alpontjának (i) alpontja.
([111]) I. melléklet III. szakasza 11. pontja d. alpontjának (i) alpontja.
([112]) Ez az adatvédelmi hatóságok testülete által kijelölt ügykezelő hatóság, amelyet „az adatvédelmi hatóságok szerepéről” szóló kiegészítő elv irányoz elő (az I. melléklet III. szakaszának 5. pontja).
([113]) I. melléklet III. szakasza 11. pontjának d. alpontja.
([114]) I. melléklet II. szakaszának 7. pontja és III. szakasza 11. pontjának e. alpontja.
([115]) I. melléklet III. szakasza 11. pontja d. alpontjának (ii) alpontja.
([116]) Az éves jelentésnek az alábbiakat kell tartalmaznia: 1. a jelentéstételi év folyamán beérkezett, EU–USA adatvédelmi kerettel kapcsolatos panaszok teljes száma, 2. a beérkezett panaszok típusa, 3. a vitarendezés minőségével kapcsolatos intézkedések, például a panaszok feldolgozásához igénybe vett idő hossza, valamint 4. a beérkezett panaszok eredménye, nevezetesen az alkalmazott jogorvoslatok és szankciók száma és típusa.

(71) A Kereskedelmi Minisztérium a megfelelőség felülvizsgálatára vonatkozó eljárásai keretében ellenőrizni fogja továbbá, hogy az EU–USA adatvédelmi keretben részt vevő szervezetek valóban regisztrálták-e magukat azoknál a független jogorvoslati mechanizmusoknál, ahol állításuk szerint ezt megtették ([117]). A szervezetek és a felelős független jogorvoslati mechanizmusok egyaránt kötelesek gyorsan választ adni a Kereskedelmi Minisztériumnak az EU–USA adatvédelmi kerettel kapcsolatos információk iránti kérdéseire és kéréseire. A Kereskedelmi Minisztérium független jogorvoslati mechanizmusokkal fog működni annak ellenőrzése érdekében, hogy azok a weboldalaikon tartalmaznak-e információkat az elvekről és az EU–USA adatvédelmi keret alapján általuk nyújtott szolgáltatásokról, valamint hogy közzéteszik-e az éves jelentéseket ([118]).

(72) Azokban az esetben, amikor a szervezet nem tesz eleget a vitarendezési vagy önszabályozási szerv döntésének, az utóbbinak értesítenie kell a meg nem felelésről a Kereskedelmi Minisztériumot és az FTC-t (vagy a meg nem felelés kivizsgálására hatáskörrel rendelkező más amerikai hatóságot) vagy az illetékes bíróságot ([119]). Ha a szervezet elutasítja valamely adatvédelmi önszabályozó, független vitarendezési vagy kormányzati szerv végleges határozatának teljesítését, vagy egy ilyen szerv megállapítja, hogy a szervezet gyakran nem tartja be az elveket, ez a teljesítés tartós elmulasztásának tekinthető, aminek következtében a Kereskedelmi Minisztérium először 30 napos határidőt tűz ki és lehetőséget ad a teljesítést elmulasztó szervezetnek a válaszadásra, majd törli a szervezetet a listáról ([120]). Ha a listáról való törlést követően a szervezet továbbra is az EU–USA adatvédelmi keret szerinti tanúsítványra vonatkozó állítást tesz, a Kereskedelmi Minisztérium az FTC vagy más jogérvényesítési ügynökség elé utalja az ügyet ([121]).

(73) Harmadszor, az egyének panaszaikat az Unión belüli valamely nemzeti adatvédelmi hatósághoz is benyújthatják, amely élhet az (EU) 2016/679 rendelet szerinti vizsgálati és jogorvoslati hatáskörével. A szervezetek kötelesek együttműködni az adatvédelmi hatóság általi vizsgálat és panaszrendezés során, amennyiben az adatkezelés munkaviszony keretében gyűjtött humánerőforrás-adatokra vonatkozik, vagy ha az adott szervezet önként vállalta az adatvédelmi hatóságok általi felügyeletet ([122]). A szervezeteknek különösen meg kell válaszolniuk a kérdéseket, követniük kell az adatvédelmi hatóság által adott ajánlásokat, többek között a korrekciós vagy ellentételezési intézkedések tekintetében, valamint írásban meg kell erősíteniük az adatvédelmi hatóság számára, hogy ilyen intézkedés meghozatalára került sor ([123]). Az adatvédelmi hatóság által adott tanácsnak való meg nem felelés esetén az adatvédelmi hatóság az ilyen eseteket a Kereskedelmi Minisztériumhoz (amely eltávolíthatja a szervezeteket az EU–USA adatvédelmi keretben részt vevő szervezetek listájáról) vagy – esetleges végrehajtási intézkedés céljából – az FTC-hez vagy a Közlekedési Minisztériumhoz utalja (az adatvédelmi hatóságokkal való együttműködés vagy az elveknek való megfelelés elmulasztása az Egyesült Államok joga szerint megtámadható) ([124]).

(74) A panaszok hatékony kezelésére irányuló együttműködés megkönnyítése érdekében mind a Kereskedelmi Minisztérium, mind az FTC külön kapcsolattartó pontot hozott létre, amely felelős az adatvédelmi hatóságokkal való közvetlen kapcsolattartásért ([125]). Ezek a kapcsolattartó pontok segítséget nyújtanak az adatvédelmi hatóság arra vonatkozó megkereséseiben, hogy egy szervezet megfelel-e az elveknek.

(75) Az adatvédelmi hatóságok általi ajánlást ([126]) azután adják ki, hogy a jogvitában érdekelt mindkét fél megfelelő lehetőséget kapott a magyarázatra és a kívánt bizonyítékok benyújtására. A testület olyan gyorsan adhat ajánlást, amint ezt a jogszerű eljárás követelménye megengedi, főszabály szerint a panasz beérkezésétől számított 60 napon belül ([127]). Ha a szervezet a kézbesítésétől számított 25 napon belül nem tesz eleget az ajánlásnak, és a késedelemre vonatkozóan nem ad kielégítő indoklást, a testület értesítést ad arról a szándékáról, hogy az ügyet megküldi az FTC-hez (vagy az Egyesült Államok egyéb, hatáskörrel rendelkező jogérvényesítési hatóságához), vagy arról, hogy

([117]) I. melléklet, „Az öntanúsítási követelmények ellenőrzése" című szakasz.

([118]) Lásd a III. melléklet „Az elvekhez kapcsolódó szolgáltatásokat nyújtó, alternatív vitarendezési testületekkel való együttműködés megkönnyítése" című szakaszát. Lásd még: I. melléklet III. szakasza 11. pontja d. alpontjának (ii)–(iii) alpontjai.

([119]) Lásd: I. melléklet III. szakasza 11. pontjának e. alpontja.

([120]) Lásd az I. melléklet III. szakasza 11. pontjának g. alpontját, különösen az ii. és az iii. alpontot.

([121]) Lásd a III. melléklet „Hamis részvételi nyilatkozatok keresése és kezelése" című szakaszát.

([122]) I. melléklet II. szakasza 7. pontjának b. alpontja.

([123]) I. melléklet III. szakaszának 5. pontja.

([124]) I. melléklet, III. szakasza 5. pontja c. alpontjának (ii) alpontja.

([125]) III. melléklet (lásd „Az adatvédelmi hatóságokkal való együttműködés megkönnyítése" szakaszt) és a IV. melléklet (lásd a „A beterjesztés priorizálása és vizsgálata" és „Végrehajtási együttműködés az uniós adatvédelmi hatóságokkal" szakaszt).

([126]) Az adatvédelmi hatóságoknak a munkájuk és a közöttük kialakítandó együttműködés megszervezésére vonatkozó hatáskörük alapján meg kell állapítaniuk az adatvédelmi hatóságok nem hivatalos testületének eljárási szabályzatát.

([127]) I. melléklet III. szakasza 5. pontja c. alpontjának (i) alpontja.

megállapítja, hogy az együttműködési kötelezettségvállalást súlyosan megszegték. Az első alternatíva szerint ez az FTC-ről szóló törvény 5. szakaszán (vagy hasonló törvényen) alapuló végrehajtási intézkedéshez vezethet ([128]). A második alternatíva szerint a testület tájékoztatni fogja a Kereskedelmi Minisztériumot, amely a megfelelés tartós elmulasztásának tekinti majd, hogy a szervezet elutasítja az adatvédelmi hatóságok testülete ajánlásának teljesítését, és ennek következtében eltávolítja a szervezetet az adatvédelmi keretben részt vevő szervezetek listájáról.

(76) Az egyéni panaszosnak lehetősége van arra, hogy amennyiben az az adatvédelmi hatóság, amelyhez a panaszt intézte, nem hoz intézkedést vagy nem megfelelő intézkedést hoz a panasz kezelésére, az érintett uniós tagállam nemzeti bíróságai előtt megtámadja az ilyen intézkedést (mulasztást).

(77) Az egyének még akkor is az adatvédelmi hatóságok elé terjeszthetik panaszaikat, ha nem az adatvédelmi hatóságok testületét jelölték ki a szervezet vitarendezési szerveként. Ilyen esetekben az adatvédelmi hatóság a Kereskedelmi Minisztérium vagy az FTC elé utalhatja e panaszokat. Az egyéni panaszokkal és az EU–USA adatvédelmi keretben részt vevő szervezetek meg nem felelésével kapcsolatos ügyekben történő együttműködés megkönnyítése és fokozása érdekében a Kereskedelmi Minisztérium e célra kialakított kapcsolattartó pontot hoz létre, hogy az összekötőként járjon el és segítséget nyújtson az adatvédelmi hatóságnak egy adott szervezet elveknek való megfelelésével kapcsolatos vizsgálatai tekintetében ([129]). Az FTC hasonlóképpen kötelezettséget vállalt arra, hogy külön kapcsolattartó pontot hoz létre ([130]).

(78) Negyedrészt a Kereskedelmi Minisztérium kötelezettséget vállalt arra, hogy fogadja és felülvizsgálja az adott szervezet elveknek való meg nem feleléssel kapcsolatos panaszokat, és megteszi a legmegfelelőbb erőfeszítéseket e panaszok rendezésére ([131]). Az Egyesült Államok Kereskedelmi Minisztériuma ennek érdekében külön eljárásokat biztosít az adatvédelmi hatóságoknak, amelyek során azok az e célra létrehozott kapcsolattartó ponthoz utalhatják a panaszokat, figyelemmel kísérhetik azokat, és a rendezés elősegítése érdekében biztosíthatják a szervezeti nyomon követést ([132]). Az egyedi panaszok feldolgozásának gyorsítása érdekében a kapcsolattartó pont közvetlenül kapcsolatba lép a megfelelési kérdésekben érintett adatvédelmi hatósággal, és mindenekelőtt az utalástól számított 90 napon belül tájékoztatja a hatóságot a panasz aktuális helyzetéről ([133]). Ez lehetővé teszi, hogy az EU–USA adatvédelmi keretben részt vevő szervezetek meg nem felelésével kapcsolatos panaszokat az érintettek közvetlenül nemzeti adatvédelmi hatóságuk elé terjesszék, és e hatóság juttassa el azokat a Kereskedelmi Minisztériumhoz, amely az EU–USA adatvédelmi keret igazgatásáért felelős amerikai hatóság.

(79) Amennyiben a Kereskedelmi Minisztérium hivatalból történő ellenőrzései, panasz vagy bármely egyéb információ alapján arra a következtetésre jut, hogy egy szervezet tartósan elmulasztotta az elvek betartását, az ilyen szervezetet eltávolítja az adatvédelmi keretben részt vevő szervezetek listájáról ([134]). A megfelelés tartós elmulasztásának tekintendő, ha a szervezet elutasítja valamely adatvédelmi önszabályozó, független vitarendezési vagy kormányzati szerv (pl. adatvédelmi hatóság) végleges határozatának teljesítését ([135]).

(80) Ötödrészt az EU–USA adatvédelmi keretben részt vevő szervezeteknek az illetékes amerikai hatóságok – különösen az FTC ([136]) – joghatósága alá kell tartozniuk, amelyek rendelkeznek az elveknek való megfelelés hatékony biztosításához szükséges vizsgálati és végrehajtási hatáskörökkel. Az FTC elsőbbséget biztosít majd a független vitarendezési vagy önszabályozási szervektől, a Kereskedelmi Minisztériumtól és a (hivatalból vagy panaszok alapján eljáró) adatvédelmi hatóságoktól kapott, az elveknek való meg nem felelés ügyében elé utalt panaszok vizsgálatának, annak eldöntése érdekében, hogy sor került-e az FTC-ről szóló törvény 5. szakaszának megsértésére ([137]). Az FTC standard utalási eljárás kialakítását vállalta, amelynek keretében kapcsolattartó pontot jelöl ki a hivatalnál az adatvédelmi hatóság által elé utalt panaszok és az ezekkel kapcsolatos információcsere számára. A Szövetségi Kereskedelmi Bizottság ezenfelül elfogadhatja a közvetlenül magánszemélyektől érkező panaszokat is, valamint hivatalból végez majd vizsgálatokat az EU–USA adatvédelmi kerettel kapcsolatosan, kiváltképpen az adatvédelmi kérdésekkel kapcsolatos tágabb vizsgálatok részeként.

([128]) I. melléklet, III. szakasza 5. pontja c. alpontjának (ii) alpontja.

([129]) Lásd a III. melléklet „Az adatvédelmi hatóságokkal való együttműködés megkönnyítése” című szakaszát.

([130]) Lásd a IV. melléklet „A beterjesztés priorizálása és vizsgálata” és „Végrehajtási együttműködés az uniós adatvédelmi hatóságokkal” című szakaszát.

([131]) III. melléklet, lásd például a „Az adatvédelmi hatóságokkal való együttműködés megkönnyítése” című szakaszt.

([132]) I. melléklet II. szakasza 7. pontjának e. alpontja és III. melléklet, lásd „Az adatvédelmi hatóságokkal való együttműködés megkönnyítése” című szakaszt.

([133]) *Uo.*

([134]) I. melléklet III. szakasza 11. pontjának g. alpontja.

([135]) I. melléklet III. szakasza 11. pontjának g. alpontja.

([136]) Az EU–USA adatvédelmi keretben részt vevő szervezetnek nyilvánosan közzé kell tennie azt a kötelezettségvállalását, hogy teljesíti az elveket, nyilvánosságra hozza az említett elveknek megfelelő adatvédelmi szabályzatát és teljeskörűen végrehajtja azt. Az FTC-ről szóló törvény tisztességtelen vagy megtévesztő kereskedelmi vagy kereskedelmet érintő gyakorlatokat tiltó 5. szakasza alapján a teljesítés elmulasztásával szemben jogérvényesítésnek helye van.

([137]) Lásd még a Közlekedési Minisztérium által tett hasonló kötelezettségvállalásokat, V. melléklet.

(81) Hatodrészt abban az esetben, ha a rendelkezésre álló egyéb jogorvoslati lehetőségek egyike sem orvosolta kielégítően az egyéni panaszt, az uniós érintett „végső eszközül" szolgáló jogorvoslati mechanizmusként igénybe veheti az „EU–USA adatvédelmi kerettel foglalkozó testület" kötelező erejű választottbírósági eljárását ([138]). A szervezeteknek tájékoztatniuk kell az egyéneket arról a lehetőségről, hogy kötelező választottbíráskodást vehetnek igénybe, és amennyiben az egyének az érintett szervezetnek küldött értesítés útján élnek az említett lehetőséggel, azok kötelesek választ adni ([139]).

(82) Az EU–USA adatvédelmi kerettel foglalkozó testületet legalább tíz választott bíróból álló állomány alkotja, akiket a függetlenségük, feddhetetlenségük és az Egyesült Államok és az Unió adatvédelmi jogával kapcsolatos tapasztalataik alapján a Kereskedelmi Minisztérium és a Bizottság jelöl ki. A felek minden egyes jogvita esetén kiválasztanak ebből az állományból egy választottbírót vagy egy három ([140]) választottbíróból álló tanácsot.

(83) A Kereskedelmi Minisztérium a Nemzetközi Vitarendezési Központot (ICDR), az Amerikai Választottbírósági Szövetség (AAA) nemzetközi részlegét választotta ki a választottbírósági eljárások lebonyolítására. Az EU–USA adatvédelmi kerettel foglalkozó testület előtti eljárásokra az elfogadott választottbírósági szabályok és a kinevezett választottbírák magatartási kódexe az irányadó. Az ICDR-AAA honlapja egyértelmű és tömör tájékoztatást nyújt az egyéneknek a választottbírósági mechanizmusról és a választottbírósági eljárás megindítására vonatkozó eljárásról.

(84) A Kereskedelmi Minisztérium és a Bizottság által elfogadott választottbírósági szabályok kiegészítik az EU–USA adatvédelmi keretet, amely több olyan jellemzőt is tartalmaz, amelyek javítják e mechanizmus hozzáférhetőségét az uniós érintettek számára: i. a választottbíróság előtti követelés előkészítése során az érintett segítséget kaphat nemzeti adatvédelmi hatóságától, ii. bár a választottbírósági eljárásra az Egyesült Államokban fog sor kerülni, az uniós érintettek döntésük szerint video- vagy telefonkonferencia útján bekapcsolódhatnak az eljárásba. Ezt a lehetőséget költségmentesen kell az egyének rendelkezésére bocsátani, iii. bár a választottbíróságon főszabály szerint az angol nyelvet használják, általában észszerű, indoklással ellátott kérésre a választottbírósági tárgyalás során tolmácsot, valamint fordítást biztosítanak, és ez nem jelent költséget az érintettnek, iv. végezetül, bár a feleknek maguknak kell viselniük saját ügyvédük tiszteletdíját, ha ügyvéddel képviseltetik magukat a választottbíróság előtt, a Kereskedelmi Minisztérium az EU–USA adatvédelmi keretnem részt vevő szervezetek éves hozzájárulásaival létrehoz majd egy alapot, amely az amerikai hatóságok által – a Bizottsággal való konzultációt követően – meghatározott maximális összegek erejéig fedezni fogja a választottbírósági eljárás támogatható költségeit ([141]).

(85) Az EU–USA adatvédelmi kerettel foglalkozó testület jogosult arra, hogy az elvek be nem tartásának orvoslásához szükséges egyedi, nem pénzbeli méltányos jogorvoslatot írjon elő ([142]). Bár a testület határozatának meghozatalakor figyelembe veszi majd az EU–USA adatvédelmi keret egyéb mechanizmusaiból már megkapott más jogorvoslatokat, az egyének ennek ellenére választottbírósághoz fordulhatnak, ha úgy ítélik meg, hogy az említett egyéb jogorvoslatok nem elegendőek. Ez lehetővé teszi, hogy az uniós érintettek minden olyan esetben választottbírósághoz folyamodjanak, amikor az EU-USA adatvédelmi keretben részt vevő szervezetek, a független jogorvoslati mechanizmusok vagy az illetékes amerikai hatóságok (például az FTC) intézkedése vagy mulasztása nem rendezi kielégítően a panaszukat. Nem lehet választottbírósághoz folyamodni, ha egy adatvédelmi hatóság hatáskörrel rendelkezik egy EU–USA adatvédelmi keretben részt vevő szervezettel kapcsolatos, szóban forgó igény rendezésére, különösen azokban az esetekben, amikor a szervezet köteles együttműködni és teljesíteni az adatvédelmi hatóságok ajánlásait a munkaviszony keretében gyűjtött humánerőforrás-adatok tekintetében, vagy pedig ezt önként vállalja. Az egyének a szövetségi választottbírósági törvény alapján érvényesíthetik a választottbírósági határozatokat az Egyesült Államok bíróságain, így biztosítva jogorvoslatot, ha a szervezet nem teljesít.

([138]) Lásd az I. mellékletet, „Választottbírósági modell".
([139]) Lásd az I. mellékletet, II. szakasza 1. pontja a. alpontjának (xi) alpontja és II. szakasza 7. pontjának c. alpontja.
([140]) A feleknek meg kell állapodniuk a választott bíróságban részt vevő választott bírák számáról.
([141]) Az I. melléklet I. melléklete, G.6. szakasz.
([142]) Az egyének a választottbírósági eljárásban nem igényelhetnek kártérítést, azonban a választottbírósághoz folyamodás nem zárja ki azt a lehetőséget, hogy az Egyesült Államok rendes bíróságai előtt kártérítést követeljenek.

(86) Hetedszer, amennyiben egy szervezet nem tesz eleget az elvek és a közzétett adatvédelmi szabályzat tiszteletben tartására vonatkozó kötelezettségének, az Egyesült Államok joga alapján további jogorvoslati lehetőségek állnak rendelkezésre, ideértve a kártérítés igénylését is. Például az egyének bizonyos feltételek mellett az állami fogyasztóvédelmi jogszabályok alapján, a tisztességtelen vagy megtévesztő cselekmények vagy gyakorlatok esetén ([143]), valamint a jogellenes károkozásra vonatkozó jog alapján (különösen a kizárásra ([144]), a név vagy hasonlóság kisajátítására ([145]), valamint a magánjellegű tények nyilvánosságra hozatalára ([146]) vonatkozó jogellenes károkozás) bírósági jogorvoslatot (többek között kártérítéshez való jogot) kérhetnek.

(87) A fent ismertetett különböző jogorvoslati lehetőségek együttesen biztosítják, hogy az EU–USA adatvédelmi keret tanúsított szervezetek általi be nem tartására vonatkozó valamennyi panaszt hatékonyan elbírálják és orvosolják.

3. AZ EURÓPAI UNIÓBÓL TOVÁBBÍTOTT SZEMÉLYES ADATOKHOZ VALÓ HOZZÁFÉRÉS ÉS AZ ILYEN ADATOKNAK AZ EGYESÜLT ÁLLAMOK HATÓSÁGAI ÁLTALI FELHASZNÁLÁSA

(88) A Bizottság értékelte továbbá a korlátozásokat és biztosítékokat, többek között az Egyesült Államok jogában rendelkezésre álló felügyeleti és egyéni jogorvoslati mechanizmusokat az egyesült államokbeli adatkezelőknek és adatfeldolgozóknak közérdekből továbbított személyes adatok egyesült államokbeli hatóságok általi gyűjtése és későbbi felhasználása tekintetében, többek közt büntetőjogi és nemzetbiztonsági célokból (kormányzati hozzáférés) ([147]). Annak értékelése során, hogy azok a feltételek, amelyek mellett az e határozat alapján az Egyesült Államokba továbbított adatokhoz való kormányzati hozzáférés megfelel-e az (EU) 2016/679 rendelet 45. cikkének (1) bekezdése szerinti „lényegi egyenértékűségi" tesztnek, a Bíróságnak az Alapjogi Chartára figyelemmel adott értelmezése szerint a Bizottság számos kritériumot vette figyelembe.

(89) Különösen a személyes adatok védelméhez való jog gyakorlása csak a törvény által korlátozható, és a beavatkozást lehetővé tevő jogalapnak magának kell meghatároznia az érintett jog gyakorlásával kapcsolatos korlátozás terjedelmét ([148]). Ezenkívül, az arányosság követelményének való megfelelés érdekében, amely szerint egy demokratikus társadalomban a személyes adatok védelme alóli eltéréseknek és e védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk az Unió által elismertekkel egyenértékű általános érdekű célok teljesítéséhez, a jogalapnak egyértelmű és pontos szabályokat kell meghatároznia a szóban forgó intézkedések alkalmazási körét és alkalmazását illetően, és elő kell írnia minimumbiztosítékokat annak érdekében, hogy azok a személyek, akiknek az adatait továbbították, elegendő garanciákkal rendelkezzenek, amelyek lehetővé teszik a személyes adataiknak a visszaélések veszélyével szembeni hatékony védelmét ([149]). Ezen túlmenően ezeknek a

([143]) Lásd például az állami fogyasztóvédelmi jogot Kaliforniában (Cal. Civ. Code §§ 1750–1785 (West), a fogyasztók jogorvoslatairól szóló törvény); Columbia kerületben (D.C. Code §§ 28-3901); Florida államban (Fla. Stat. §§ 501.201–501.213, megtévesztő és tisztességtelen kereskedelmi gyakorlatokról szóló törvény); Illinois államban (815 Ill. Comp. Stat. 505/1–505/12, fogyasztókkal szembeni csalásokról és megtévesztő üzleti gyakorlatokról szóló törvény); Pennsylvania államban (73 Pa. Stat. Ann. §§ 201-1–201-9.3 (West), tisztességtelen kereskedelmi gyakorlatokról és fogyasztóvédelemről szóló törvény).

([144]) Azaz az egyén magánügyeibe vagy aggályaiba való szándékos beavatkozás esetén, amely rendkívül sértő lenne egy észszerű személy számára (Restatement (2nd) of Torts, §652(b)).

([145]) Ez a jogellenes károkozás általában akkor áll fenn, ha a magánszemély nevét vagy hasonlóságát egy vállalkozás vagy termék reklámozására vagy hasonló kereskedelmi célra használják fel (lásd: Restatement (2nd) of Torts, §652C).

([146]) Azaz amikor az egyén magánéletére vonatkozó információt nyilvánosságra hozzák, ha ez egy észszerű személy számára rendkívül sértő, és az információ a nyilvánosságot nem érinti jogszerűen (2nd) of Torts, §652D).

([147]) Ez az I. melléklet I.5. szakaszának fényében is releváns. E szakasz alapján és az általános adatvédelmi rendelethez hasonlóan az adatvédelmi elvek részét képező adatvédelmi követelményeknek és jogoknak való megfelelés korlátozható. Az ilyen korlátozások azonban nem abszolút jellegűek, hanem csak több feltétel teljesülése esetén alkalmazhatók, például a bírósági végzésnek való megfeleléshez vagy a közérdeknek, a bűnüldözésnek vagy a nemzetbiztonsági követelményeknek való megfeleléshez szükséges mértékben. Ebben az összefüggésben és az egyértelműség érdekében ez a szakasz a 14086. elnöki rendeletben meghatározott feltételekre is hivatkozik, amelyeket a (127)–(141) preambulumbekezdés értékel.

([148]) Lásd a Schrems II. ügy 174–175. pontját és a hivatkozott ítélkezési gyakorlatot. Lásd még a tagállami hatóságok hozzáférését illetően: a Bíróság ítélete, Privacy International, C-623/17, ECLI:EU:C:2020:790, 65. pont; és a Bíróság ítélete, La Quadrature du Net és társai, C-511/18, C-512/18 és C-520/18 egyesített ügyek, ECLI:EU:C:2020:791, 175. pont.

([149]) Lásd a Schrems II. ügy 176. és 181. pontját, valamint az ott hivatkozott ítélkezési gyakorlatot. Lásd még a tagállami hatóságok hozzáférését illetően a Privacy International ügy 68. pontját; és a La Quadrature du Net és társai ügy 132. pontját.

szabályoknak és biztosítékoknak jogilag kötelező erejűnek és az egyének által érvényesíthetőnek kell lenniük ([150]). Az érintetteknek különösen rendelkezniük kell azzal a lehetőséggel, hogy független és pártatlan bíróság előtt éljenek jogorvoslati lehetőségekkel abból a célból, hogy a rájuk vonatkozó személyes adatokhoz hozzáférést kapjanak, vagy az említett adatokat helyesbíttetni vagy töröltetni tudják ([151]).

3.1. **Az egyesült államokbeli közigazgatási szervek hozzáférése az adatokhoz és az adatok használata bűnüldözés céljából**

(90) Ami az EU–USA adatvédelmi keret szerint bűnüldözési célból továbbított személyes adatokba való beavatkozást illeti, az Egyesült Államok joga számos korlátozást ír elő a személyes adatokhoz való hozzáférésre és azok felhasználására vonatkozóan, valamint olyan felügyeleti és jogorvoslati mechanizmusokat biztosít, amelyek összhangban vannak az e határozat (89) preambulumbekezdésében említett követelményekkel. Az említett hozzáférés feltételeit és az e hatáskörök alkalmazására vonatkozó biztosítékokat a következő szakaszok részletesen értékelik. E tekintetben az Egyesült Államok kormánya (az Igazságügyi Minisztériumon keresztül) biztosítékokat is nyújtott az alkalmazandó korlátozásokról és biztosítékokról (e határozat VI. melléklete).

3.1.1. ***Jogalapok, korlátok és biztosítékok***

3.1.1.1. *A személyes adatok bűnüldözési célú gyűjtésére vonatkozó korlátozások és biztosítékok*

(91) A tanúsított egyesült államokbeli szervezetek által kezelt azon személyes adatokhoz, amelyeket az Unióból az EU–USA adatvédelmi keret alapján továbbítanának, az USA szövetségi ügyészei és szövetségi nyomozó tisztviselői különböző eljárások keretében bűnüldözési célból hozzáférhetnek, amint azt a (92)–(99) preambulumbekezdés részletesebben kifejti. Ezek az eljárások ugyanúgy alkalmazandók, ha az információkat bármely egyesült államokbeli szervezettől szerzik be, függetlenül az érintettek állampolgárságától vagy lakóhelyétől ([152]).

(92) Először is egy szövetségi bűnüldöző szerv tagja vagy a kormány jogi képviselőjének kérésére a bíró házkutatási vagy lefoglalási parancsot adhat ki (beleértve az elektronikusan tárolt információkat is) ([153]). Ilyen parancs csak akkor bocsátható ki, ha „alapos gyanú ([154])" áll fenn arra vonatkozóan, hogy a „lefoglalható tárgyak" (bűncselekmény bizonyítéka, jogellenesen birtokolt tárgyak vagy bűncselekmény elkövetésére szánt vagy arra használt vagyon) valószínűleg a parancsban meghatározott helyen találhatók. A parancsnak meg kell jelölnie a lefoglalandó vagyontárgyat vagy tárgyat, és meg kell jelölnie azt a bírót, akihez a parancsot vissza kell juttatni. Az a személy, akivel szemben házkutatást folytatnak, vagy akinek a vagyonát átkutatják, a jogellenes házkutatásból szerzett vagy

([150]) Lásd: Schrems II. ügy 181–182. pontja.

([151]) Lásd: Schrems I. ügy, 95. pont és a Schrems II. ügy, 194. pont. E tekintetben az EUB hangsúlyozta, hogy az Alapjogi Charta 47. cikkének való megfelelés, amely garantálja a független és pártatlan bíróság előtti, hatékony jogorvoslathoz való jogot, „szintén része az Unión belül megkövetelt védelmi szintnek, és amelynek tiszteletben tartását a Bizottságnak meg kell állapítania, mielőtt az (EU) 2016/679 rendelet 45. cikkének (1) bekezdése alapján megfelelőségi határozatot fogadna el" (Schrems II. ügy, 186. pont).

([152]) Lásd a VI. mellékletet. A telefonbeszélgetés lehallgatásáról szóló törvénnyel, a tárolt kommunikációról szóló törvénnyel és a lehallgató eszközökről szóló törvénnyel (részletesebben a (95)–(98) preambulumbekezdés ismerteti) kapcsolatban lásd például: Suzlon Energy Ltd. kontra Microsoft Corp., 671 F.3d 726, 729 (9th. Cir. 2011).

([153]) Szövetségi büntetőeljárási szabályok, 41. A Legfelsőbb Bíróság egy 2018-as ítéletében megerősítette, hogy a házkutatási parancsra vagy a parancs alóli kivételre ahhoz is szükség van, hogy a bűnüldöző hatóságok hozzáférjenek a cellahelyszín helymeghatározó adatainak előzményeihez, amelyek átfogó áttekintést nyújtanak a felhasználó mozgásairól, és hogy a felhasználónak észszerű elvárása lehet az ilyen információk tekintetében a magánélet védelme (Timothy Ivory Carpenter kontra Amerikai Egyesült Államok, 16-402. sz., 585 U.S., 2018). Következésképpen az ilyen adatok általában nem szerezhetők be egy mobiltársaságtól bírósági végzés alapján olyan megalapozott indokok alapján, amelyek szerint feltételezhető, hogy az információ releváns és lényeges a folyamatban lévő nyomozás szempontjából, hanem arra van szükség, hogy a parancs felhasználása esetén alapos gyanú álljon fenn.

([154]) A Legfelsőbb Bíróság szerint az „alapos gyanú" olyan „gyakorlati, nem technikai" norma, amely „a mindennapi élet azon ténybeli és gyakorlati szempontjaira támaszkodik, amelyek alapján az észszerű és körültekintő emberek […] eljárnak" (Illinois kontra Gates, 462 U.S. 213, 232, 1983). A házkutatási parancsok esetében akkor áll fenn alapos gyanú, ha valós a valószínűsége annak, hogy a keresés bűncselekményre utaló bizonyíték felfedezését eredményezi (uo.).

abból származó bizonyítékok kizárását indítványozhatja, ha e bizonyítékokat büntetőeljárás során bemutatják vele szemben ([155]). Ha az adattulajdonosnak (pl. egy vállalatnak) parancs alapján kell közzétennie az adatokat, akkor különösen vitathatja a közzétételre vonatkozó követelményt, mivel az indokolatlanul megterhelő ([156]).

(93) Másodszor, a vádesküdtszék (a bíróság bíró vagy főbíró által kiválasztott vizsgáló ága) bizonyos súlyos bűncselekmények kivizsgálásával összefüggésben ([157]) – általában szövetségi ügyész kérésére – parancsot adhat ki annak érdekében, hogy megkövetelje valakitől üzleti nyilvántartások, elektronikusan tárolt információk vagy egyéb tárgyi eszközök bemutatását vagy rendelkezésre bocsátását. Ezenkívül több különböző törvény ad felhatalmazást a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatok felhasználására üzleti adatok, elektronikusan tárolt információk vagy más ingók egészségügyi csalással, gyermekbántalmazással, titkosszolgálati védelemmel, ellenőrzött anyagok használatával kapcsolatos vizsgálatokban és legfőbb ügyészi vizsgálatokban történő bemutatása vagy rendelkezésre bocsátása céljából ([158]). Az információnak mindkét esetben relevánsnak kell lennie a vizsgálat szempontjából, és a parancs nem lehet észszerűtlen, azaz túlzó, elnyomó vagy megterhelő (és a parancs címzettje ezen az alapon vitathatja azt) ([159]).

(94) Nagyon hasonló feltételek vonatkoznak az egyesült államokbeli vállalatok birtokában lévő adatokhoz polgári vagy szabályozási célból („közérdek") való hozzáférés céljából kiadott, a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatokra. Az ilyen bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatokkal kapcsolatos polgári és szabályozási feladatokat ellátó szervek hatáskörét törvénybe kell foglalni. A bizonyításfelvételben való közreműködésre kötelező közigazgatási határozat használata „észszerűségi vizsgálat" tárgyát képezi, amely megköveteli, hogy a vizsgálatot törvényes célnak megfelelően folytassák le, a határozatban kért információk e célból relevánsak legyenek, az ügynökség még ne rendelkezzen a határozattal kért információkkal, és hogy a határozat kiadásához szükséges adminisztratív lépéseket betartották ([160]). A Legfelsőbb Bíróság ítélkezési gyakorlata azt is egyértelművé tette, hogy egyensúlyt kell teremteni a kért információhoz fűződő közérdek fontossága, valamint a személyes és szervezeti adatvédelmi érdekek fontossága között ([161]). Bár a közigazgatási határozat használata nem függ előzetes bírósági jóváhagyástól, az bírósági felülvizsgálat tárgyát képezi abban az esetben, ha a címzett a fent említett indokok alapján kifogást emel, vagy ha a kibocsátó szerv bírósági úton kívánja érvényesíteni a határozatot ([162]). Ezen általános, átfogó korlátozások mellett egyedi (szigorúbb) követelmények is adódhatnak az egyes alapokmányokból ([163]).

([155]) Mapp kontra Ohio, 367 U.S. 643, 1961.

([156]) Lásd az Egyesült Államoknak a 3. körzet fellebbviteli bíróságához benyújtott kérelmét, 610 F.2d 1148, 1157 (3d Cir. 1979) (amely szerint a jogszerű eljárásnak feltétele, hogy mielőtt a távközlési vállalatot házkutatásban való segítségnyújtásra kötelezték, ennek megterhelő voltáról meghallgatást kell tartani); lásd továbbá az Egyesült Államoknak a 9. körzet fellebbviteli bíróságához benyújtott kérelmét, 616 F.2d 1122 (9th Cir. 1980).

([157]) Az Egyesült Államok Alkotmányának ötödik alkotmánykiegészítése előírja, hogy minden „főbenjáró vagy egyéb módon jelentős bűncselekmény" esetén vádesküdtszéket kell alkalmazni. A vádesküdtszék 16–23 tagból áll, és megállapítja, hogy fennáll-e az alapos gyanú arra vonatkozólag, hogy bűncselekményt követtek el. E következtetés levonása érdekében a vádesküdtszéket olyan vizsgálati hatáskörökkel ruházták fel, amelyek lehetővé teszik számára, hogy határozatokat adjon ki.

([158]) Lásd a VI. mellékletet.

([159]) Szövetségi büntetőeljárási szabályok, 17.

([160]) Egyesült Államok kontra Powell, 379 U.S. 48, 1964.

([161]) Oklahoma Press Publishing Co. kontra Walling, 327 U.S. 186, 1946.

([162]) A Legfelsőbb bíróság tisztázta, hogy egy közigazgatási határozat megtámadása esetén a bíróságnak figyelembe kell vennie, hogy 1. a vizsgálat jogszerűen engedélyezett célból zajlik-e, 2. a szóban forgó határozatot kiállító hatóság a Kongresszus hatáskörébe tartozik-e, és 3. a „kért dokumentumok relevánsak-e a vizsgálat szempontjából". A Bíróság továbbá megjegyezte, hogy a közigazgatási határozatra irányuló kérelemnek „észszerűnek" kell lennie, azaz „az adott vizsgálat céljából megfelelő, de nem túlzott részletességgel kell bemutatni a dokumentumokat", beleértve „az átkutatandó hely, valamint a letartóztatandó személyek vagy a lefoglalandó dolgok leírásának sajátosságát".

([163]) Például a pénzügyi adatvédelemhez való jogról szóló törvény csak akkor biztosít hatáskört a kormányzati hatóságnak arra, hogy közigazgatási határozat alapján megszerezze a pénzügyi intézmény birtokában lévő pénzügyi nyilvántartásokat, ha 1. okkal feltételezhető, hogy a kért nyilvántartások relevánsak egy jogszerű bűnüldözési vizsgálat szempontjából, és 2. a határozat vagy idézés másolatát a vizsgálat jellegét észszerű konkrét módon feltüntető értesítéssel együtt eljuttatták az ügyfélhez (12 U.S.C. §3405). Egy másik példa a tisztességes hiteljelentésről szóló törvény, amely megtiltja a fogyasztói bejelentő ügynökségeknek, hogy közigazgatási határozati kérelmekre válaszolva közzétegyék a fogyasztói jelentéseket (és csak azt teszi lehetővé számukra, hogy válaszoljanak az esküdtszék határozati kérelmeire vagy bírósági végzéseire, 15 U.S.C. §1681 és azt követő bekezdések). Ami a kommunikációs információkhoz való hozzáférést illeti, a tárolt kommunikációról szóló törvény különös követelményei alkalmazandók, többek között a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatok használatának lehetősége tekintetében (a részletes áttekintést lásd a (96)–(97) preambulumbekezdésben).

(95) Harmadszor számos jogalap lehetővé teszi a bűnüldöző hatóságok számára, hogy hozzáférjenek a kommunikációs adatokhoz. A bíróság elrendelheti a telefonszámra vagy e-mailre vonatkozó valós idejű, nem tartalmi tárcsázási, útvonal-, cím- és jelzési adatok összegyűjtését (bejövő és kimenő hívásokat rögzítő eszközök segítségével), ha megállapítja, hogy a hatóság igazolta, hogy a valószínűleg megszerzendő információ egy folyamatban lévő nyomozás szempontjából releváns ([164]). A végzésnek tartalmaznia kell többek között a gyanúsított személyazonosságát, amennyiben ismert; a hatálya alá tartozó kommunikációk attribútumait, valamint annak a bűncselekménynek a megjelölését, amelyre a gyűjtendő információk vonatkoznak. A hívásrögzítő és lehallgató eszközök használata legfeljebb hatvan napra engedélyezhető, amely időtartam csak új bírósági végzéssel hosszabbítható meg.

(96) Emellett az internetszolgáltatók, telefontársaságok és egyéb harmadik fél szolgáltatók birtokában lévő előfizetői információkhoz, forgalmi adatokhoz és a kommunikáció tárolt tartalmához való bűnüldözési célú hozzáférés a tárolt kommunikációról szóló törvény alapján is megszerezhető ([165]). Az elektronikus kommunikáció tárolt tartalmának megszerzéséhez a büntető ügyekben eljáró bűnüldöző hatóságoknak elvben az arra vonatkozó alapos gyanú alapján kell bírói parancsot beszerezniük, hogy a szóban forgó felhasználói fiók bűncselekmény bizonyítékát tartalmazza ([166]). Az előfizetői regisztrációs adatok, az IP-címek és a kapcsolódó időbélyegzők, valamint a számlainformációk esetében a bűnüldöző hatóságok idézést használhatnak. A legtöbb egyéb tárolt, tartalmat nem felfedő információ – így a tárgy nélküli e-mail-fejlécek – esetében a bűnüldöző hatóságoknak konkrét bírósági végzést kell szerezniük, amelyet akkor állítanak ki, ha a bíró meggyőződött arról, hogy észszerű okok alapján lehet úgy vélni, hogy a kért információ releváns és lényeges egy folyamatban levő bűnügyi nyomozásban.

(97) Azok a szolgáltatók, amelyek a tárolt kommunikációról szóló törvény alapján megkeresést kapnak, önkéntesen értesíthetik azt az ügyfelet vagy előfizetőt, akinek az adatait kérik, kivéve, ha az illetékes bűnüldöző hatóság az értesítést tiltó védelmi határozatot kap ([167]). Az ilyen védelmi határozat olyan bírósági határozat, amely arra kötelezi az elektronikus hírközlési szolgáltatásokat vagy távoli számítástechnikai szolgáltatásokat nyújtó szolgáltatót, akire a parancs, idézés vagy bírósági végzés irányul, hogy a bíróság által megfelelőnek ítélt ideig ne értesítsen más személyeket a parancs, idézés vagy bírósági végzés létezéséről. Védelmi határozatot akkor adnak ki, ha a bíróság úgy ítéli meg, hogy okkal feltételezhető, hogy az értesítés súlyosan veszélyeztetné a nyomozást vagy indokolatlanul késleltetné a tárgyalást, például azért, mert veszélyeztetné egy egyén életét vagy testi épségét, vagy a büntetőeljárás előli szökést, a potenciális tanúk megfélemlítését stb. eredményezné. A főügyészhelyettesi nyilatkozat (amely az Igazságügyi Minisztérium valamennyi jogászára és megbízottjára nézve kötelező) előírja az ügyészek számára, hogy részletesen határozzák meg a védelmi határozat szükségességét, és indokolják meg a bíróság számára, hogy az adott ügyben hogyan teljesülnek a védelmi határozat elrendelésének törvényes feltételei ([168]). A nyilatkozat azt is előírja, hogy a védelmi határozat iránti kérelmek általában nem irányulhatnak az értesítés egy évnél hosszabb késleltetésére. Amennyiben kivételes körülmények között hosszabb időtartamú határozatra lehet szükség, ilyen határozat csak az Egyesült Államok ügyésze vagy a megfelelő főügyészhelyettes által kijelölt felügyelő írásbeli hozzájárulásával kérhető. Ezen túlmenően az ügyésznek a nyomozás lezárásakor haladéktalanul értékelnie kell, hogy van-e alapja a folyamatban lévő védelmi határozatok fenntartásának, és amennyiben nem ez a helyzet, meg kell szüntetnie a védelmi határozatot, és gondoskodnia kell arról, hogy erről a szolgáltatót értesítsék ([169]).

([164]) 18 U.S.C. §3123.

([165]) 18 U.S.C. §§ 2701-2713.

([166]) 18 U.S.C. §§ 2701(a)–(b)(1)(A). Ha az érintett előfizetőt vagy ügyfelet értesítik (akár előzetesen, akár bizonyos körülmények között késedelmes értesítéssel), a 180 napot meghaladóan tárolt tartalmi információk közigazgatási határozat vagy vádesküdtszéki parancs (18 U.S.C. §§ 2701(b)(1)(B)) vagy bírósági végzés alapján is beszerezhetők (amennyiben alapos okkal feltételezhető, hogy a folyamatban lévő nyomozás szempontjából releváns és lényeges információról van szó (18 U.S.C. §§ 2701(d)). A szövetségi fellebbviteli bíróság ítéletével összhangban azonban a kormányzati nyomozók általában házkutatási parancsokat kapnak a bíráktól a magánjellegű kommunikáció tartalmának vagy a tárolt adatoknak a kereskedelmi kommunikációs szolgáltatótól való beszerzése érdekében. Egyesült Államok kontra Warshak, 631 F.3d 266 (6th Cir. 2010).

([167]) 18 U.S.C. § 2705(b).

([168]) Lásd Rod Rosenstein főügyészhelyettes 2017. október 19-i feljegyzését a védelmi (vagy titoktartási) határozatok iránti kérelmekre vonatkozó szigorúbb politikáról, elérhető a következő internetcímen: https://www.justice.gov/criminal-ccips/page/file/1005791/download

([169]) Lisa Moncao főügyészhelyettes 2022. május 27-i feljegyzése a 18 U.S.C. §2705(b) szerinti, védelmi határozat iránti kérelmekre vonatkozó kiegészítő politikáról.

(98) A bűnüldöző hatóságok valós idejű telefonos, szóbeli vagy elektronikus kommunikációt is lehallgathatnak bírósági határozat alapján, amelyben a bíró egyebek között megállapítja, hogy alaposan gyanítható, hogy a telefonos vagy elektronikus lehallgatás szövetségi bűncselekményt vagy a büntetőeljárás elől menekülő tartózkodási helyére vonatkozó bizonyítékot nyújt ([170]).

(99) További védelmet nyújtanak az Igazságügyi Minisztérium különböző szabályzatai és iránymutatásai, többek között a belföldi FBI-műveletekre vonatkozó főügyészi iránymutatás (Attorney General Guidelines for domestic FBI Operations – AGG-DOM) is, amely egyebek mellett előírja, hogy a Szövetségi Nyomozóirodának (FBI) a lehető legkisebb beavatkozással járó vizsgálati módszereket kell alkalmaznia, figyelembe véve a magánéletre és a polgári szabadságjogokra gyakorolt hatást ([171]).

(100) Az Egyesült Államok kormánya által tett nyilatkozatok szerint azonos vagy magasabb szintű, fent ismertetett védelmi normák vonatkoznak az állami szintű bűnügyi nyomozásokra (a tagállamok joga alapján végzett nyomozások tekintetében) ([172]). Különösen az alkotmányos rendelkezések, valamint az állami szintű törvények és ítélkezési gyakorlat erősítik meg a fent említett védelmet az indokolatlan házkutatással és lefoglalással szemben azáltal, hogy házkutatási parancs kibocsátását írják elő ([173]). A szövetségi szinten biztosított védelemhez hasonlóan a házkutatási parancsot csak valószínű ok bemutatása esetén lehet kiadni, és annak tartalmaznia kell a házkutatás helyét és a letartóztatandó személyt vagy a lefoglalandó dolgot ([174]).

([170]) 18 U.S.C. §§ 2510-2522.

([171]) A belföldi FBI-műveletekre vonatkozó főügyészi iránymutatás (Attorney General's Guidelines for Domestic Federal Bureau of Investigation [FBI] Operations) (2008. szeptember), elérhető itt: http://www.justice.gov/archive/opa/docs/guidelines.pdf A szövetségi ügyészek nyomozati tevékenységének korlátait ismertető további szabályokat és szabályzatokat az Egyesült Államok ügyészségi kézikönyve fekteti le, amely elérhető itt: http://www.justice.gov/usam/united-states-attorneys-manual Ezen iránymutatásoktól való eltéréshez az FBI igazgatójától, igazgatóhelyettesétől vagy az általa kijelölt ügyvezetőigazgató-helyettestől előzetes jóváhagyást kell kérni, kivéve, ha ez a jóváhagyás nem szerezhető meg a személyek vagy vagyontárgyak biztonságát vagy a nemzetbiztonságot fenyegető közvetlen vagy súlyos veszély miatt (ebben az esetben az igazgatót vagy más engedélyező személyt a lehető leghamarabb értesíteni kell). Amennyiben az iránymutatást nem követik, az FBI értesíti erről az Igazságügyi Minisztériumot, amely pedig tájékoztatja a legfőbb ügyészt és a főügyész-helyettest.

([172]) VI. melléklet, 2. lábjegyzet. Lásd még például: Arnold kontra Cleveland város, 67 Ohio St.3d 35, 616 N.E.2d 163, 169, 1993 („Az egyéni jogok és a polgári szabadságjogok területén az Egyesült Államok alkotmánya – ahol az államokra alkalmazandó – olyan alsó határt ír elő, amely alá az állami bírósági határozatok nem eshetnek"); Cooper kontra California, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L. Ed.2d 730, 1967 („Törlésünk természetesen nem érinti az állam azon jogát, hogy a szövetségi alkotmány által előírtnál szigorúbb követelményeket írjon elő a házkutatásokra és lefoglalásokra, ha úgy dönt."); Petersen kontra Mesa város, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Bár Arizona alkotmánya előírhat szigorúbb normákat a házkutatásokkal és lefoglalásokkal kapcsolatban, mint a szövetségi alkotmány, az arizonai bíróságok nem biztosíthatnak kevesebb védelmet, mint a negyedik alkotmánykiegészítés").

([173]) Az államok többsége alkotmányában átvette a negyedik alkotmánykiegészítés által biztosított védelmet. Lásd: Alabama alkotmánya, I. cikk, § 5; Alaska alkotmánya, I. cikk, § 14; 1; Arkansas alkotmánya, II. cikk, § 15; Kalifornia alkotmánya, I. cikk, § 13; Colorado alkotmánya, II. cikk, § 7; Connecticut alkotmánya, I. cikk, § 7; Delaware alkotmánya, I. cikk, § 6; Florida alkotmánya, I. cikk, § 12; Georgia alkotmánya, I. cikk, § I, XIII. bekezdés; Hawaii alkotmánya, I. cikk, § 7; Idaho alkotmánya, I. cikk, § 17; Illinois alkotmánya, I. cikk, § 6; Indiana alkotmánya, I. cikk, § 11; Iowa alkotmánya, I. cikk, § 8; Kansas alkotmánya, Bill of Rights, § 15; Kentucky alkotmánya, § 10; Louisiana alkotmánya, I. cikk, § 5; Maine alkotmánya, I. cikk, § 5; Massachusets alkotmánya, Decl. of Rights, 14. cikk; Michigan alkotmánya, I. cikk, § 11; Minnesota alkotmánya, I. cikk, § 10; Mississippi alkotmánya, III. cikk, § 23; Missouri alkotmánya, I. cikk, § 15; Montana alkotmánya, II. cikk, § 11; Nebraska alkotmánya, I. cikk, § 7; Nevada alkotmánya, I. cikk, § 18; New Hampshire alkotmánya. 1. pont, 19. cikk; N.J. alkotmánya, II. cikk, § 7; Új-Mexikó alkotmánya, II. cikk, § 10; New York alkotmánya, I. cikk, § 12; Észak-Dakota alkotmánya, I. cikk, § 8; Ohio alkotmánya, I. cikk, § 14; Oklahoma alkotmánya, II. cikk, § 30; Oregon alkotmánya, I. cikk, § 9; Pennsylvania alkotmánya, I. cikk, § 8; Rhode Island alkotmánya, I. cikk, § 6; Dél-Karolina alkotmánya, I. cikk, § 10; Dél-Dakota alkotmánya, VI. cikk, § 11; Tennessee alkotmánya, I. cikk, § 7; Texas alkotmánya, I. cikk, § 9; Utah alkotmánya, I. cikk, § 14; Vermont alkotmánya, I. fejezet, 11. cikk; Nyugat-Virginia alkotmánya, III. cikk, § 6; Wisconsin alkotmánya, I. cikk, § 11; Wyoming alkotmánya, I. cikk, § 4. Mások (pl. Maryland, Észak-Karolina és Virginia) alkotmányukba belefoglalták azokat a parancsokat, amely bírósági értelmezésük szerint a negyedik alkotmánykiegészítéshez hasonló vagy magasabb szintű védelmet nyújtanak (lásd Maryland Decl. of Rights, 26. cikk; Észak-Karolina alkotmánya, I. cikk, § 20; Virginia alkotmánya. I. cikk, § 10 és a vonatkozó ítélkezési gyakorlat, pl. Hamel kontra állam, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; Állam kontra Johnson, 861 S.E.2d 474, 483 (N.C. 2021) és Lowe kontra Commonwealth, 337 S.E.2d 273, 274 (Va. 1985). Végül Arizona és Washington olyan alkotmányos rendelkezésekkel rendelkezik, amelyek általánosabban védik a magánéletet (Arizona alkotmánya, 2. cikk, § 8; Washington alkotmánya, I. cikk, § 7), amely a bíróságok értelmezése szerint több védelmet nyújt, mint a negyedik alkotmánykiegészítés (lásd pl. Állam kontra Bolt, 689 P.2d 519, 523 [Ariz. 1984], Állam kontra Ault, 759 P.2d 1320, 1324 [Ariz. 1988], Állam kontra Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155, 1984 , Állam kontra Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598, 1994).

([174]) Lásd például: kaliforniai büntető törvénykönyv, § 1524.3(b); 3.6–3.13. szabály, Alabamai büntetőeljárási szabályzat; 10.79.035. szakasz; Felülvizsgált washingtoni kódex; 5. fejezet 19.2–59. szakasz, 19.2. cím, büntetőeljárási jog, virginiai kódex.

3.1.1.2. *A gyűjtött adatok további felhasználása*

(101) Ami a szövetségi bűnüldöző hatóságok által gyűjtött adatok további felhasználását illeti, a különböző törvények, iránymutatások és előírások különleges biztosítékokat írnak elő. Az FBI tevékenységeire alkalmazandó konkrét eszközök (az AGG-DOM és az FBI belföldi vizsgálatokra és műveletekre vonatkozó útmutatója) kivételével az e szakaszban ismertetett követelmények általában az adatok bármely szövetségi hatóság általi további felhasználására vonatkoznak, beleértve a polgári vagy szabályozási célból hozzáférhető adatokat is. Ez magában foglalja az Irányítási és Költségvetési Hivatal feljegyzéseiből/rendeleteiből, a szövetségi információbiztonsági irányítás korszerűsítéséről szóló törvényből, az e-kormányzatról szóló törvényből és a szövetségi nyilvántartásokról szóló törvényből eredő követelményeket.

(102) A Clinger-Cohen törvény (P.L. 104–106., Division E) és a számítógép-biztonságról szóló 1987. évi törvény (P.L. 100–235) által adott felhatalmazásnak megfelelően az Irányítási és Költségvetési Hivatal (OMB) kiadta az A-130. sz. körlevelet, amely valamennyi szövetségi ügynökségre (beleértve a bűnüldöző hatóságokat is) vonatkozik, amikor személyazonosító adatokat kezelnek ([175]). A körlevél különösen azt írja elő valamennyi szövetségi ügynökség számára, hogy „a személyesen azonosítható információk létrehozását, gyűjtését, felhasználását, feldolgozását, tárolását, karbantartását, terjesztését és nyilvánosságra hozatalát a jogilag engedélyezett, releváns és a felhatalmazott ügynökség feladatainak megfelelő ellátásához észszerűen szükségesnek ítélt adatokra korlátozzák” ([176]). Ezen túlmenően a szövetségi ügynökségeknek – az észszerűen megvalósítható mértékig – biztosítaniuk kell, hogy a személyesen azonosítható információk pontosak, relevánsak, időszerűek és hiánytalanok legyenek, és az ügynökség feladatainak megfelelő ellátásához szükséges minimumra korlátozódjanak. Általánosabban fogalmazva, a szövetségi ügynökségeknek átfogó adatvédelmi programot kell létrehozniuk az alkalmazandó adatvédelmi követelményeknek való megfelelés biztosítása, az adatvédelmi szabályzatok kidolgozása és értékelése, valamint az adatvédelmi kockázatok kezelése érdekében; eljárásokat kell fenntartaniuk a magánélet védelmével kapcsolatos incidensek észlelésére, dokumentálására és bejelentésére; adatvédelmi tudatosságnövelő és képzési programokat kell kidolgozniuk a munkavállalók és a vállalkozók számára; valamint szabályzatokat és eljárásokat kell bevezetniük annak biztosítására, hogy a személyzet elszámoltatható legyen a magánélet védelmére vonatkozó követelményeknek és szabályzatoknak való megfelelés tekintetében ([177]).

(103) Emellett az e-kormányzatról szóló törvény ([178]) előírja valamennyi szövetségi ügynökség (beleértve a bűnüldöző hatóságokat is) számára, hogy olyan információbiztonsági védelmet vezessenek be, amely arányban áll a jogosulatlan hozzáférésből, felhasználásból, nyilvánosságra hozatalból, zavarból, módosításból vagy megsemmisítésből eredő kár kockázatával és nagyságrendjével; hogy információs főtisztviselővel rendelkezzenek az információbiztonsági követelményeknek való megfelelés biztosítása érdekében, és évente független értékelést végezzenek (pl. egy főellenőr segítségével, lásd a (109) preambulumbekezdést) információbiztonsági programjukról és gyakorlataikról ([179]). Hasonlóképpen, a szövetségi nyilvántartásról szóló törvény (FRA) ([180]) és a kiegészítő rendeletek ([181]) előírják, hogy a szövetségi ügynökségek birtokában lévő információkra az információk fizikai épségét és a jogosulatlan hozzáféréssel szembeni védelmét biztosító biztosítékoknak kell vonatkozniuk.

(104) A szövetségi törvényhozó hatóság, többek között az információbiztonság korszerűsítéséről szóló 2014. évi szövetségi törvény alapján az OMB és a National Institute of Standards and Technology (NIST) olyan szabványokat dolgozott ki, amelyek kötelező erejűek a szövetségi ügynökségekre (többek között a bűnüldöző hatóságokra) nézve, és amelyek tovább pontosítják a bevezetendő információbiztonsági minimumkövetelményeket, beleértve a hozzáférés-ellenőrzést, a tudatosság és képzés biztosítását, a vészhelyzeti tervezést, az eseményekre való reagálást, az ellenőrzést és az elszámoltathatóságot, a rendszer és az információs integritás biztosítását, a magánélet védelmét és a biztonsági kockázatok értékelését stb. ([182]) Ezen túlmenően valamennyi szövetségi ügynökségnek (beleértve a

([175]) Azaz „olyan információk, amelyek felhasználhatók az egyén személyazonosságának megkülönböztetésére vagy nyomon követésére, akár önmagukban, akár egy adott egyénhez kapcsolódó vagy kapcsolható más információval kombinálva”, lásd az OMB A-130. sz. körlevelének 33. oldalát (a „személyazonosító adatok” fogalommeghatározása).

([176]) Az OMB A-130. sz. körlevele, Managing Information as a Strategic Resource [Az információ mint stratégiai erőforrás kezelése], II. függelék, Responsibilities for Managing Personally Identifiable Information (A személyazonosító adatok kezelésére vonatkozó felelősségi körök), 81 Fed. Reg. 49,689 (2016. július 28.), 17. o.

([177]) II. függelék, §5(a)–(h).

([178]) 44 U.S.C. 36. fejezet.

([179]) 44 U.S.C. §§ 3544–3545.

([180]) FAC, 44 U.S.C. § 3105.

([181]) 36 C.F.R. §§ 1228.150 és azt követő szakaszok, 1228.228 és A. függelék.

([182]) Lásd például: az OMB A-130. sz. körlevele; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Információs rendszerek és szervezetek biztonsági és adatvédelmi ellenőrzései) (2020. december 10.); és a NIST 200. szövetségi információfeldolgozási szabványa: A szövetségi információkra és információs rendszerekre vonatkozó biztonsági minimumkövetelmények.

bűnüldöző hatóságokat is) az OMB iránymutatásaival összhangban tervet kell fenntartania és végrehajtania az adatvédelmi incidensek kezelésére, beleértve az ilyen jogsértésekre való reagálást és a kárkockázatok értékelését is ([183]).

(105) Ami az adatmegőrzést illeti, a FRA ([184]) előírja az Egyesült Államok szövetségi ügynökségei (köztük a bűnüldöző hatóságok) számára, hogy határozzanak meg adatmegőrzési időszakokat (amelyeket követően ezeket a nyilvántartásokat meg kell semmisíteni), amelyeket a Nemzeti Irattár és Nyilvántartási Hivatalnak jóvá kell hagynia ([185]). E megőrzési időszak hosszát különböző tényezők figyelembevételével határozzák meg, mint például a vizsgálat típusa, az, hogy a bizonyítékok továbbra is relevánsak-e a vizsgálat szempontjából stb. Az FBI tekintetében az AGG-DOM előírja, hogy az FBI-nak rendelkeznie kell ilyen nyilvántartás-megőrzési tervvel, és olyan rendszert kell fenntartania, amelyből azonnal kinyerhető a vizsgálatok állapota és alapja.

(106) Végül az OMB A-130. sz. körlevele is tartalmaz bizonyos követelményeket a személyazonosító adatok terjesztésére vonatkozóan. A személyesen azonosítható információk terjesztésének és közzétételének elvben arra kell korlátozódnia, ami jogilag engedélyezett, releváns és észszerűen szükségesnek tekinthető az ügynökség feladatainak megfelelő ellátásához ([186]). A személyazonosító adatok más kormányzati szervezetekkel való megosztásakor az Egyesült Államok szövetségi ügynökségeinek adott esetben olyan feltételeket kell előírniuk (beleértve a konkrét biztonsági és adatvédelmi ellenőrzések végrehajtását), amelyek szabályozzák az információk írásbeli megállapodások (többek között szerződések, adatfelhasználási megállapodások, információcsere-megállapodások és egyetértési megállapodások) útján történő kezelését ([187]). Az információk terjesztésének indokai tekintetében például az AGG-DOM és az FBI belföldi vizsgálatokról és műveletekről szóló útmutatója ([188]) úgy rendelkezik, hogy az FBI-t jogi kötelezettség terhelheti erre (pl. nemzetközi megállapodás alapján), vagy bizonyos körülmények között továbbíthat információkat, például más egyesült államokbeli ügynökségeknek, amennyiben a nyilvánosságra hozatal összeegyeztethető azzal a céllal, amelyre az információt gyűjtötték, és kapcsolódik a felelősségi körükhöz; kongresszusi bizottságoknak; külföldi ügynökségeknek, amennyiben az információ a felelősségi körükhöz kapcsolódik, és az információ terjesztése összhangban áll az Egyesült Államok érdekeivel; a terjesztés különösen a személyek vagy a vagyon biztonságának védelme, illetve a bűncselekményekkel vagy a nemzetbiztonságot fenyegető veszélyekkel szembeni védelem vagy azok megelőzése érdekében szükséges, és a közlés összeegyeztethető azzal a céllal, amelyre az információt gyűjtötték ([189]).

3.1.2. *Felügyelet*

(107) A szövetségi bűnüldöző szervek tevékenységét különböző szervek felügyelik ([190]). A (92)–(99) preambulumbekezdésben kifejtettek szerint ez a legtöbb esetben magában foglalja az igazságszolgáltatás általi előzetes felügyeletet is, amelynek engedélyeznie kell az egyedi gyűjtési intézkedéseket, mielőtt azok alkalmazhatók lennének. Ezenkívül más szervek felügyelik a bűnüldöző hatóságok tevékenységeinek különböző szakaszait, beleértve a személyes adatok gyűjtését és kezelését. Ezek az igazságügyi és nem igazságügyi szervek együttesen biztosítják, hogy a bűnüldöző hatóságok független felügyelet alá tartozzanak.

([183]) 17-12. feljegyzés, „Preparing for and Responding to a Breach of Personally Identifiable Information" [Személyazonosító adatokkal kapcsolatos incidensre való felkészülés és reakció], elérhető itt: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf és az OMB A-130. sz. körlevele. Például az Igazságügyi Minisztérium adatvédelmi incidensekre való reagálási eljárásait *lásd*: https://www.justice.gov/file/4336/download

([184]) FRA, 44 U.S.C. §§3101 és azt követő szakaszok.

([185]) A Nemzeti Irattár és Nyilvántartási Hivatal hatáskörrel rendelkezik az ügynökségi iratkezelési gyakorlatok értékelésére, és megállapíthatja, hogy indokolt-e bizonyos nyilvántartások megőrzése (44 U.S.C. §§ 2904(c), 2906).

([186]) Az OMB A-130. sz. körlevele, 5.f.1.(d) szakasz.

([187]) Az OMB A-130. sz. körlevele, I. függelék, § 3(d).

([188]) Lásd még az FBI belföldi vizsgálatokról és műveletekről szóló útmutatójának (DIOG) 14. szakaszát.

([189]) AGG-DOM VI. szakasz, B. és C.; az FBI belföldi vizsgálatokról és műveletekről szóló útmutatójának (DIOG) 14. szakasza.

([190]) Az e szakaszban említett mechanizmusok a szövetségi hatóságok által polgári és szabályozási célból végzett adatgyűjtésre és -felhasználásra is vonatkoznak. A szövetségi polgári és szabályozási ügynökségeket saját felügyelőik ellenőrzik, a Kongresszus pedig felügyeli őket, ideértve a Kormányzati Ellenőrzési Hivatalt, a Kongresszus ellenőrzési és vizsgálati ügynökségét is. Amennyiben az ügynökség nem rendelkezik kijelölt adatvédelmi és polgári szabadságjogi tisztviselővel – ez a beosztás jellemzően olyan ügynökségeknél található, mint az Igazságügyi Minisztérium és a Belbiztonsági Minisztérium (DHS) bűnüldözési és nemzetbiztonsági feladataik miatt –, ezek a feladatok az ügynökség vezető adatvédelmi tisztviselőjét (SAOP) terhelik. Valamennyi szövetségi ügynökség jogilag kötelezett arra, hogy SAOP-ot nevezzen ki, aki felelős annak biztosításáért, hogy az ügynökség megfeleljen az adatvédelmi jogszabályoknak és felügyelje a kapcsolódó ügyeket. Lásd például: OMB M-16–24, Role and Designation of Senior Agency Officials for Privacy, 2016.

(108) Egyrészt számos, bűnüldözéssel kapcsolatos feladatkörökkel rendelkező szervezeti egységen belül vannak adatvédelmi és polgári szabadságjogi tisztségviselők ([191]). Bár e tisztségviselők konkrét hatásköre a felhatalmazó törvénytől függően némileg eltér egymástól, általában felöleli az eljárások felügyeletét annak érdekében, hogy a megfelelő minisztérium/ügynökség megfelelően figyelembe vegye az adatvédelmi és polgári szabadságjogi megfontolásokat, valamint megfelelő eljárásokat alakítson ki az olyan egyénektől érkező panaszok kezelésére, akik úgy vélik, hogy megsértették az adatvédelemhez fűződő vagy polgári szabadságjogaikat. Az egyes szervezeti egységek vagy ügynökségek vezetőinek gondoskodniuk kell arról, hogy a magánélet védelmével és az állampolgári szabadságjogokkal foglalkozó tisztviselők rendelkezzenek a megbízatásuk teljesítéséhez szükséges eszközökkel és erőforrásokkal, hozzáférjenek a feladataik ellátásához szükséges valamennyi anyaghoz és személyzethez, továbbá tájékoztatást kapjanak a javasolt szakpolitikai változásokról, és konzultáljanak velük azokról ([192]). A polgári szabadságjogi és adatvédelmi tisztségviselők időszakonként beszámolnak a Kongresszusnak többek között a minisztériumhoz/ügynökséghez beérkezett panaszok számáról és jellegéről, valamint az ilyen panaszok rendezésének összefoglalásáról, a tisztviselő által lefolytatott felülvizsgálatokról és vizsgálatokról és az általa végzett tevékenység hatásáról ([193]).

(109) Másrészt egy független főellenőr felügyeli az Igazságügyi Minisztérium tevékenységét, beleértve az FBI tevékenységét is ([194]). A főellenőrök törvény erejénél fogva függetlenek ([195]), és felelősek a Minisztérium programjainak és műveleteinek független vizsgálatáért, auditjáért és ellenőrzéséért. Betekinthetnek valamennyi nyilvántartásba, jelentésbe, ellenőrzésbe, felülvizsgálatba, dokumentumba, iratba, ajánlásba vagy egyéb vonatkozó anyagba, ha szükséges bizonyítási cselekményben való közreműködésre kötelező közigazgatási határozat révén, és tanúvallomást vehetnek fel ([196]). Bár a főellenőrök korrekciós intézkedésekre vonatkozó, jogilag nem kötelező ajánlásokat adhatnak ki, jelentéseiket – többek között a nyomonkövetési intézkedésekről (vagy azok hiányáról) szóló jelentéseiket ([197]) – nyilvánosságra hozzák, és emellett elküldik a Kongresszusnak, amely ezek alapján gyakorolhatja felügyeleti funkcióját (lásd a (111) preambulumbekezdést) ([198]).

([191]) Lásd: 42 U.S.C. § 2000ee-1. Ez magában foglalja például az Igazságügyi Minisztériumot, a Belbiztonsági Minisztériumot és az FBI-t. A Belbiztonsági Minisztériumban emellett adatvédelmi főtisztviselő felel a magánélet védelmének megőrzéséért és javításáért, valamint az átláthatóság előmozdításáért a minisztériumon belül (6 U.S.C. 142, 222. szakasz). Minden olyan, Belbiztonsági Minisztériumon belüli rendszer, technológia, űrlap és program, amely személyes adatokat gyűjt vagy kihat a magánélet védelmére, az adatvédelmi főtisztviselő felügyelete alá tartozik, aki hozzáfér a Minisztérium rendelkezésére álló valamennyi nyilvántartáshoz, jelentéshez, ellenőrzéshez, felülvizsgálathoz, dokumentumhoz, irathoz, ajánláshoz és egyéb anyaghoz, szükség esetén idézés révén. Az adatvédelmi tisztviselőnek évente jelentést kell tennie a Kongresszusnak a Minisztérium magánéletet érintő tevékenységeiről, beleértve a magánélet megsértésével kapcsolatos panaszokat is.

([192]) 42 U.S.C. § 2000ee-1(d).

([193]) Lásd: 42 U.S.C. §§ 2000ee-1 (f)(1)–(2). Például az Igazságügyi Minisztérium adatvédelmi és polgári szabadságjogi főtisztviselőjének, valamint az adatvédelmi és polgári szabadságjogi hivatalának a 2020. október és 2021. március közötti időszakra vonatkozó jelentése szerint 389 adatvédelmi felülvizsgálatra került sor, többek között információs rendszerek és egyéb programok tekintetében (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Hasonlóképpen, a belbiztonságról szóló 2002. évi törvény létrehozta a Belbiztonsági Minisztérium Főellenőri Hivatalát.

([195]) A főellenőrök biztos hivatali megbízatással rendelkeznek, és csupán az elnök mentheti fel őket, akinek írásban közölni kell a Kongresszussal e felmentés indokait.

([196]) Lásd a főellenőrről szóló 1978. évi törvény 6. §-át.

([197]) E tekintetben lásd például az Igazságügyi Minisztérium Hivatala által a főellenőrről készített áttekintést az általa tett ajánlásokról, valamint arról, hogy azokat milyen mértékben hajtották végre a szervezeti egységek és ügynökségek nyomonkövetési intézkedései révén, https://oig.justice.gov/sites/default/files/reports/22-043.pdf

([198]) Lásd a főellenőrről szóló 1978. évi törvény 4. §-ának (5) bekezdését és 5. §-át. Például az Igazságügyi Minisztérium Főellenőrének Hivatala nemrégiben tette közzé féléves jelentését a Kongresszusnak (2021. október 1-jétől 2022. március 31-ig, https://oig.justice.gov/node/23596), amely áttekintést nyújt az Igazságügyi Minisztérium programjainak és műveleteinek ellenőrzéseiről, értékeléséről, auditjairól, különleges felülvizsgálatáról és vizsgálatairól. E tevékenységek közé tartozott egy korábbi vállalkozónak az elektronikus megfigyelés (egy egyén lehallgatása) jogellenes nyilvánosságra hozatalával kapcsolatos vizsgálata egy folyamatban lévő nyomozás során, amely a vállalkozó elítéléséhez vezetett. A Főellenőri Hivatal az Igazságügyi Minisztérium ügynökségeinek információbiztonsági programjait és gyakorlatait is megvizsgálta, amely magában foglalta az ügynökségi rendszerek reprezentatív alcsoportja információbiztonsági szabályzatainak, eljárásainak és gyakorlatainak hatékonyságát.

(110) Harmadszor, amennyiben terrorizmusellenes tevékenységeket végeznek, a bűnüldözési feladatokat ellátó szervezeti egységek az adatvédelmi és polgári szabadságjogi felügyelő tanács (PCLOB) felügyelete alá tartoznak, amely a végrehajtó ágon belül egy független ügynökség, amely egy kétpárti, öttagú igazgatótanácsból áll, akit az elnök határozott hatéves időtartamra nevez ki, a szenátus jóváhagyásával ([199]). Alapító okirata szerint a PCLOB a magánélet és a polgári szabadságjogok védelme érdekében hatáskörrel rendelkezik a terrorizmusellenes politikák és azok végrehajtása terén. A tanács a felülvizsgálata során hozzáférhet az összes érintett ügynökség nyilvántartásaihoz, ellenőrzéseihez, felülvizsgálataihoz, dokumentumaihoz, irataihoz és ajánlásaihoz – ideértve a minősített adatokat –, meghallgatásokat folytathat és tanúvallomásokat vehet fel ([200]). Jelentéseket kap a különböző minisztériumok/ügynökségek polgári szabadságjogi és adatvédelmi tisztviselőitől ([201]), ajánlásokat ad ki a kormányzatnak és a bűnüldöző hatóságoknak, és rendszeresen jelentést tesz a kongresszusi bizottságoknak és az elnöknek ([202]). A testület jelentéseit, beleértve a Kongresszusnak szóló jelentéseket is, a lehető legnagyobb mértékben nyilvánosan hozzáférhetővé kell tenni ([203]).

(111) Végezetül a bűnüldözési tevékenységeket az Egyesült Államok Kongresszusának egyes bizottságai (a Ház és a Szenátus igazságügyi bizottságai) felügyelik. Az igazságügyi bizottságok különböző módokon végeznek rendszeres felügyeletet, különösen meghallgatások, vizsgálatok, felülvizsgálatok és jelentések révén ([204]).

3.1.3. *Jogorvoslat*

(112) A fentieknek megfelelően a bűnüldöző hatóságoknak a legtöbb esetben előzetes bírósági engedélyt kell beszerezniük a személyes adatok gyűjtéséhez. Bár ez nem szükséges a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatok esetében, ezek konkrét helyzetekre korlátozódnak, és legalább akkor független bírósági felülvizsgálat tárgyát fogják képezni, ha a kormány bírósági végrehajtást kér. Különösen a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatok címzettjei megtámadhatják azokat a bíróságon azzal az indokkal, hogy azok nem észszerűek, vagy túlzott a hatókörük, elnyomóak vagy terhesek ([205]).

(113) Az egyének először is kérelmeket vagy panaszokat nyújthatnak be a bűnüldöző hatóságokhoz személyes adataik kezelésével kapcsolatban. Ez magában foglalja a személyes adatokhoz való hozzáférés kérelmezésének és azok helyesbítésének lehetőségét is ([206]). A terrorizmus elleni küzdelemmel kapcsolatos tevékenységek tekintetében az egyének panaszt nyújthatnak be a bűnüldöző hatóságok adatvédelmi és polgári jogi tisztviselőinél (vagy más adatvédelmi tisztviselőknél) is ([207]).

(114) Továbbá az amerikai jog számos bírósági jogorvoslati lehetőséget biztosít az egyéneknek a hatóságokkal vagy azok tisztviselőivel szemben, amennyiben ezek a hatóságok személyes adatokat kezelnek ([208]). A különösen az államigazgatási eljárásról szóló törvényre (APA), az információkhoz való szabad hozzáférésről szóló törvényre (FOIA) és az elektronikus kommunikáció adatvédelméről szóló törvényre (ECPA) kiterjedő, szóban forgó jogorvoslati lehetőségek állampolgárságtól függetlenül mindenki számára nyitva állnak az esetleges vonatkozó feltételekkel.

([199]) A testület tagjait kizárólag szakmai képesítésük, eredményeik, közéleti tevékenységük, a polgári szabadságjogok és a magánélet védelme terén szerzett szakértelmük, valamint releváns tapasztalataik alapján, politikai hovatartozásuktól függetlenül lehet kiválasztani. A testületnek egyetlen esetben sem lehet háromnál több olyan tagja, aki ugyanahhoz a politikai párthoz tartozik. A testületbe kinevezett személy a testületben betöltött tisztségének ideje alatt nem lehet a szövetségi kormány választott tisztviselője, tisztségviselője vagy alkalmazottja, kivéve az igazgatótanács tagjaként betöltött tisztségét. Lásd: 42 U.S.C. § 2000ee (h).

([200]) 42 U.S.C. § 2000ee (g).

([201]) Lásd: 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Ezek közé tartozik legalább az Igazságügyi Minisztérium, a Védelmi Minisztérium, a Belbiztonsági Minisztérium, valamint a megfelelő lefedettség érdekében a PCLOB által kijelölt bármely egyéb végrehajtó hatalmi szervezeti egység, ügynökség vagy szervezet.

([202]) 42 U.S.C. §2000ee, (e).

([203]) 42 U.S.C. § 2000ee (f).

([204]) A bizottságok például tematikus meghallgatásokat szerveznek (lásd például a Képviselőház igazságügyi bizottságának nemrégiben tartott meghallgatását a „digitális dragnetekről", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), valamint rendszeres felügyeleti meghallgatásokat, pl. az FBI és az Igazságügyi Minisztérium tekintetében, lásd https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 és https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899

([205]) Lásd a VI. mellékletet.

([206]) Az OMB A-130. sz. körlevele, II. függelék, 3. szakasz a) és f) pontja, amely előírja a szövetségi ügynökségek számára, hogy magánszemélyek kérésére biztosítsák a megfelelő hozzáférést és helyesbítést, valamint alakítsanak ki eljárásokat a magánélet védelmével kapcsolatos panaszok és kérelmek fogadására és kezelésére.

([207]) Lásd: 42 U.S.C. § 2000ee-1, például az Igazságügyi Minisztérium és a Belbiztonsági Minisztérium tekintetében. Lásd még: az OMB M-16-24. feljegyzése, *Role and Designation of Senior Agency Officials for Privacy*.

([208]) Az e szakaszban említett jogorvoslati mechanizmusok a szövetségi hatóságok által polgári és szabályozási célból végzett adatgyűjtésre és -felhasználásra is vonatkoznak.

(115) Általában véve az államigazgatási eljárásról szóló törvény ([209]) bírósági felülvizsgálatra vonatkozó rendelkezései szerint „egy hivatal tevékenysége miatt jogellenesen kárt szenvedő, vagy egy hivatal tevékenysége révén hátrányos helyzetbe kerülő vagy sérelmet szenvedő személyek" jogosultak bírósági jogorvoslatot igényelni ([210]). Ez többek között azt jelenti, hogy kérhetik a bíróságtól „az önkényesnek, kiszámíthatatlannak, mérlegelési jogkörrel való visszaélésnek vagy egyébként a joggal ellentétesnek talált […] hivatali intézkedés megállapítás és következtetések jogellenességének kimondását és azok hatályon kívül helyezését" ([211]).

(116) Közelebbről az ECPA ([212]) II. címe meghatározza a magánélethez fűződő törvényes jogok rendszerét, és így szabályozza a bűnüldözési célú hozzáférést a harmadik fél szolgáltatók által tárolt vezetékes, szóbeli vagy elektronikus kommunikációhoz ([213]). A törvény büntetni rendeli a jogellenes (vagyis bíróság által nem engedélyezett vagy egyébként nem megengedhető) hozzáférést az ilyen kommunikációhoz, és jogorvoslati lehetőséget biztosít az érintett személyeknek, akik az Egyesült Államok szövetségi bíróságán tényleges és büntető jellegű kártérítés iránti polgári jogi igényt, illetve méltányossági vagy megállapítási keresetet terjeszthetnek elő azzal a kormányzati tisztviselővel szemben, aki szándékosan ilyen jogellenes cselekményt követett el, vagy pedig az Egyesült Államokkal szemben.

(117) Ezenfelül több más törvény biztosítja az egyéneknek azt a jogot, hogy keresetet indítsanak az Egyesült Államok hatósága vagy tisztviselője ellene a személyes adataik kezelése tekintetében; így például a lehallgatásról szóló törvény ([214]), a számítógépes csalásról és visszaélésről szóló törvény ([215]), a kártérítési követelésekről szóló szövetségi törvény ([216]), a pénzügyi adatok védelméről szóló törvény ([217]), valamint a méltányos hitelminősítésről szóló törvény ([218]).

([209]) 5 U.S.C. § 702.

([210]) Általában csupán a „végleges" ügynökségi intézkedés – nem pedig az „előzetes" vagy „közbenső" ügynökségi intézkedés – tartozik bírósági felülvizsgálat hatálya alá. Lásd 5 U.S.C. § 704.

([211]) 5 U.S.C. § 706(2)(A).

([212]) 18 U.S.C. §§ 2701–2712.

([213]) Az ECPA védelmet nyújt a hálózati szolgáltatók két meghatározott csoportja – konkrétan az alábbi szolgáltatásokat nyújtók – birtokában lévő kommunikáció számára: i. elektronikus hírközlési szolgáltatások, például telefónia vagy e-mail, ii. távoli számítástechnikai szolgáltatások, mint számítógépes adattárolási és kezelési szolgáltatások.

([214]) 18 U.S.C. §§ 2510 és azt követő rendelkezések. A lehallgatásról szóló törvény (18 U.S.C. § 2520) értelmében az a személy, akinek a vezetékes, szóbeli vagy elektronikus kommunikációját megszerezték, nyilvánosságra hozták vagy szándékosan felhasználták, polgári jogi keresetet indíthat a lehallgatási törvény megsértése miatt, bizonyos körülmények között egy egyéni kormányzati tisztviselővel vagy az Egyesült Államokkal szemben is. A nem tartalmi információk (pl. IP-címek, a címről/címre küldött e-mailek) tekintetében lásd továbbá a 18. cím lehallgató- és nyomkövető készülékekről szóló fejezetét (18 U.S.C. §§ 3121–3127, valamint a polgári jogi keresetek tekintetében § 2707).

([215]) 18 U.S.C. § 1030. A számítógépes csalásról és visszaélésről szóló törvény értelmében egy adott személy bárki ellen – beleértve egyéni kormányzati tisztviselőket – keresetet indíthat amiatt, hogy szándékosan engedély nélküli hozzáférést létesítenek (vagy túllépik az engedélyezett hozzáférést), hogy adatokat szerezzenek egy pénzügyi intézményhez tartozó vagy amerikai kormányzati számítógépről vagy egyéb konkrét számítógépről.

([216]) 28 U.S.C. §§ 2671 és azt követő rendelkezések. A kártérítési követelésekről szóló szövetségi törvény értelmében egy adott személy bizonyos körülmények között keresetet indíthat az Egyesült Államokkal szemben „a kormányzat hivatali vagy alkalmazotti hatáskörben eljáró valamely alkalmazottjának gondatlan vagy jogellenes cselekménye vagy mulasztása tekintetében".

([217]) 12 U.S.C. §§ 3401 és azt követő rendelkezések. A pénzügyi adatok védelméről szóló törvény értelmében egy adott személy bizonyos körülmények között keresetet indíthat az Egyesült Államokkal szemben amiatt, hogy a törvény megsértésével szereznek meg vagy hoznak nyilvánosságra védett pénzügyi nyilvántartásokat. A védett pénzügyi nyilvántartásokhoz való kormányzati hozzáférés általában véve tilos, kivéve, ha a kormány jogszerű bizonyítási cselekményben való közreműködésre kötelező határozat vagy kutatási parancs hatálya alá tartozó kérelmet vagy bizonyos korlátozásoktól függően hivatalos írásbeli kérelmet terjeszt elő, és az a személy, akinek az információit meg kívánják szerezni, értesítést kap az ilyen kérelemről.

([218]) 15 U.S.C. §§ 1681–1681x. A méltányos hitelminősítésről szóló törvény értelmében egy adott személy keresetet indíthat bárkivel – bizonyos körülmények között akár kormányzati ügynökséggel – szemben, aki/amely nem tesz eleget a fogyasztói hitelminősítések beszerzésével, terjesztésével és használatával kapcsolatos követelményeknek (különösen a jogszerű engedélyezés szükségességének).

(118) A FOIA ([219]) 5 U.S.C. § 552 értelmében továbbá bármely személynek joga van hozzáférni a szövetségi ügynökségek nyilvántartásaihoz, beleértve azokat az eseteket is, amikor azok az egyén személyes adatait tartalmazzák. A közigazgatási jogorvoslati lehetőségek kimerítését követően az egyén a bíróság előtt érvényesítheti a hozzáféréshez való jogát, kivéve, ha e nyilvántartásokat mentesség vagy különleges bűnüldözési célú kizárás védi a nyilvánosságra hozatallal szemben ([220]). Ebben az esetben a bíróság értékeli, hogy van-e mentesség, vagy arra az illetékes hatóság jogszerűen hivatkozott-e.

3.2. **Az amerikai hatóságok nemzetbiztonsági célokból történő adathozzáférése és -használata**

(119) Az Egyesült Államok törvényei számos korlátozást állapítanak meg a személyes adatokhoz való hozzáférésre és azok bűnüldözési célokra történő felhasználására, és ezen a területen felügyeleti és jogorvoslati mechanizmusokat biztosítanak, amelyek összhangban állnak az e határozat (89) preambulumbekezdésében említett követelményekkel. Az említett hozzáférés feltételeit és az e hatáskörök alkalmazására vonatkozó biztosítékokat a következő szakaszok részletesen értékelik.

3.2.1. ***Jogalapok, korlátok és biztosítékok***

3.2.1.1. *Az alkalmazandó jogi keret*

(120) Az Unióból az EU–USA adatvédelmi keretben részt vevő szervezeteknek továbbított személyes adatokat az Egyesült Államok hatóságai nemzetbiztonsági célokból különböző jogi eszközök alapján, meghatározott feltételek és biztosítékok mellett gyűjthetik.

(121) Azt követően, hogy az Egyesült Államokban található szervezetek megkapták a személyes adatokat, az Egyesült Államok hírszerző ügynökségei nemzetbiztonsági célokból csak a törvény által engedélyezett módon kérhetnek hozzáférést az Egyesült Államokban található szervezeteknek továbbított személyes adatokhoz, különösen a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (FISA) vagy a nemzetbiztonsági levelek (NSL) révén történő hozzáférést engedélyező jogszabályi rendelkezések alapján ([221]). A FISA számos olyan jogalapot tartalmaz, amely felhasználható az uniós érintettek EU–USA adatvédelmi keret alapján továbbított személyes adatainak gyűjtésére (és későbbi kezelésére) (a FISA 105. szakasza ([222]), a FISA 302. szakasza ([223]), a FISA 402. szakasza ([224]), a FISA 501. szakasza ([225]), valamint a FISA 702. szakasza ([226])), amint azt a (142)–(152) preambulumbekezdése részletesebben ismerteti.

([219]) 5 U.S.C. § 552.

([220]) Ezek a kivételek azonban korlátozottak. Például az 5 U.S.C. § 552 (b)(7) szerint a FOIA szerinti jogok nem érvényesíthetők „a bűnüldözési célokból összeállított nyilvántartások vagy információk esetében, hanem csupán akkor, ha e bűnüldözési nyilvántartások vagy információk közlése A) megalapozottan feltételezhetően sértené a bűnüldözési eljárást, B) megfosztana egy személyt a tisztességes eljáráshoz vagy a pártatlan elbíráláshoz való jogtól, C) megalapozottan feltételezhetően egy személy magánéletébe történő indokolatlan beavatkozást jelentene, D) megalapozottan feltételezhetően bizalmas információforrás kilétének felfedésével járna, ideértve az állami, helyi vagy külföldi ügynökségeket, illetve hatóságokat, vagy bármely magánintézményt, amely bizalmasan információkat szolgáltatott, valamint bűnüldöző hatóság által bűnügyi nyomozás során, vagy törvényes nemzetbiztonsági hírszerzési nyomozást folytató ügynökség által összeállított nyilvántartást vagy információkat, vagy bizalmas forrásból szolgáltatott információkat, E) nyilvánosságra kerülnének a bűnügyi nyomozás és büntetőeljárás technikái és eljárásai, vagy nyilvánosságra kerülnének a bűnügyi nyomozásokra és büntetőeljárásokra vonatkozó iránymutatások, ha e nyilvánosságra jutás megalapozottan feltételezhetően a jog kijátszásának veszélyével járna, vagy F) megalapozottan feltételezhetően veszélyeztetné valamely személy életét vagy testi épségét.” Továbbá „ha bármikor olyan kérelmet terjesztettek elő, amely nyilvántartásokhoz való hozzáférést érint [aminek teljesítése megalapozottan feltételezhetően sértené a bűnüldözési eljárást], valamint A) a nyomozás vagy eljárás a büntetőjog esetleges megsértésére vonatkozik; és B) alaposan feltételezhető, hogy i. a nyomozás vagy eljárás tárgyát képező személy nem tud a vele szembeni eljárásról, továbbá ii. a nyilvántartások létének közlése észszerűen feltételezhetően sértené a bűnüldözési eljárást, az ügynökség – kizárólag e körülmények folyamatos fennállása során – úgy kezelheti e nyilvántartásokat, mint amelyek nem tartoznak az e szakaszba foglalt követelmények hatálya alá.” (5 U.S.C. § 552 (c)(1)).

([221]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u–1681v; és 18 U.S.C. § 2709. Lásd a (153) preambulumbekezdést.

([222]) 50 U.S.C. § 1804, amely a hagyományos személyre szabott elektronikus felügyeletet érinti.

([223]) 50 U.S.C. §1822, amely a külföldi hírszerzési célokból végzett fizikai keresésekre vonatkozik.

([224]) 50 U.S.C. § 1842, valamint § 1841(2) és a 18. cím 3127. szakasza, amely a kimenő hívások adatait rögzítő eszközök és a bejövő hívások adatait rögzítő eszközök telepítésére vonatkozik.

([225]) 50 U.S.C. § 1861, amely lehetővé teszi az FBI számára, hogy „olyan végzésre irányuló kérelmet nyújtson be, amely engedélyezi egy közös fuvarozó, nyilvános szálláshely, fizikai raktározási létesítmény vagy gépjárműkölcsönző létesítmény számára, hogy külföldi hírszerzési információ gyűjtésére irányuló nyomozás vagy nemzetközi terrorizmusra vonatkozó nyomozás céljából átadja a birtokában lévő nyilvántartásokat”.

([226]) 50 U.S.C. § 1881a, amely lehetővé teszi, hogy az Egyesült Államok Hírszerző Közösségének elemei hozzáférést kérjenek az egyesült államokbeli vállalatoktól olyan információkhoz, beleértve az internetes kommunikáció tartalmát is, amelyek bizonyos, az Egyesült Államokon kívüli nem egyesült államokbeli személyeket céloznak meg, az elektronikus hírközlési szolgáltatók jogilag kötelező segítségével.

(122) Az Egyesült Államok hírszerző ügynökségeinek lehetőségük van arra is, hogy az Egyesült Államokon kívül személyes adatokat gyűjtsenek, amelyek magukban foglalhatják az Unió és az Egyesült Államok között továbbított személyes adatokat is. Az Egyesült Államokon kívüli adatgyűjtés az elnök ([227]) által kiadott 12333. sz. elnöki rendeleten ([228]) alapul.

(123) A jelfelderítés gyűjtése a hírszerzési adatgyűjtés azon formája, amely a legrelevánsabb a jelenlegi megfelelőségi megállapítás szempontjából, mivel az elektronikus kommunikáció és az információs rendszerekből származó adatok gyűjtésére vonatkozik. Az ilyen adatgyűjtést az Egyesült Államok hírszerző ügynökségei végezhetik mind az Egyesült Államokban (a FISA alapján), mind pedig addig, amíg az adatok továbbításra kerülnek az Egyesült Államokba (a 12333. elnöki rendelet alapján).

(124) 2022. október 7-én az Egyesült Államok elnöke kiadta az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről szóló 14086. elnöki rendeletet, amely korlátozásokat és biztosítékokat határoz meg valamennyi egyesült államokbeli jelfelderítési tevékenységre vonatkozóan. Ez az elnöki rendelet nagymértékben felváltja az elnöki politikai irányelvez (PPD-28) ([229]), megerősíti azokat a feltételeket, korlátozásokat és biztosítékokat, amelyek valamennyi jelfelderítési tevékenységre vonatkoznak (azaz a FISA és a 12333. elnöki rendelet alapján), függetlenül azok helyétől ([230]), és új jogorvoslati mechanizmust hoz létre, amelyen keresztül az egyének hivatkozhatnak ezekre a biztosítékokra és érvényesíthetik azokat ([231]) (lásd részletesebben a (176)–(194) preambulumbekezdést). Ennek során az Egyesült Államok jogában végrehajtja az EU és az USA között azt követően folytatott tárgyalások eredményét, hogy a Bíróság érvénytelenítette az adatvédelmi pajzsra vonatkozó bizottsági megfelelőségi határozatot (lásd a (6) preambulumbekezdést). Ezért ez az e határozatban értékelt jogi keret különösen fontos eleme.

(125) A 14086. elnöki rendelet által bevezetett korlátozások és biztosítékok kiegészítik a FISA 702. szakaszát és a 12333. rendeletben foglaltakat. Az alábbiakban (a 3.2.1.2. és 3.2.1.3. szakaszban) leírt követelményeket a hírszerző ügynökségeknek alkalmazniuk kell a FISA 702. szakasza és a 12333. elnöki rendelet szerinti jelfelderítési tevékenységek végzésekor, például a FISA 702. szakasza szerint megszerzendő külföldi hírszerzési információk kategóriáinak kiválasztása/azonosítása; a 12333. elnöki rendelet alapján külföldi hírszerzési információk gyűjtése vagy kémelhárítás; valamint a FISA 702. szakasza és a 12333. rendelet alapján egyedi célzott döntések meghozatala során.

(126) Az elnök által kiadott elnöki rendeletben meghatározott követelmények a Hírszerző Közösség egészére nézve kötelezőek. Ezeket továbbra is végre kell hajtani olyan ügynökségi politikák és eljárások révén, amelyek azokat a napi működésre vonatkozó konkrét irányokba ültetik át. E tekintetben a 14086. elnöki rendelet az amerikai hírszerző ügynökségek számára legfeljebb egy évet biztosít meglévő szabályzataik és eljárásaik naprakésszé tételére (azaz 2023. október 7-ig) annak érdekében, hogy összhangba hozzák azokat az elnöki rendelet követelményeivel. Ezeket az aktualizált szabályzatokat és eljárásokat a főügyésszel, a nemzeti hírszerzési igazgató polgári szabadságjogi tisztviselőjével (ODNI CLPO) és a PCLOB-vel konzultálva kell kidolgozni és nyilvánosságra hozni, mely utóbbi testület független felügyeleti szerv, amely a magánélet és a polgári szabadságjogok védelme érdekében jogosult felülvizsgálni a végrehajtói ág szabályzatait és azok végrehajtását (a PCLOB szerepe és jogállása tekintetében lásd a (110) preambulumbekezdést) ([232]). Emellett a frissített szabályzatok és eljárások bevezetését követően a PCLOB felülvizsgálatot végez annak biztosítása érdekében, hogy azok összhangban legyenek az elnöki rendelettel. Az ilyen

([227]) Az Egyesült Államok Alkotmányának II. cikke értelmében a nemzetbiztonság biztosításának felelőssége, beleértve különösen a külföldi hírszerzési információk gyűjtését, az elnöknek mint a fegyveres erők főparancsnokának hatáskörébe tartozik.

([228]) 12333. elnöki rendelet: Egyesült Államok hírszerzési tevékenységei, Federal Register Vol. 40, No 235 (1981. december 8., módosítva 2008. július 30-án). A 12333. elnöki rendelet általánosabban meghatározza az Egyesült Államok hírszerzési erőfeszítéseinek céljait, irányait, kötelezettségeit és felelősségét (beleértve a Hírszerző Közösség különböző elemeinek szerepét), és meghatározza a hírszerzési tevékenységek végzésének általános paramétereit.

([229]) A 14086. elnöki rendelet hatályon kívül helyezi a korábbi elnöki irányelvet, a PPD-28-at, annak 3. szakasza és egy azt kiegészítő melléklet kivételével (amely előírja a hírszerző ügynökségek számára, hogy évente vizsgálják felül jelfelderítési prioritásaikat és követelményeiket, figyelembe véve a jelfelderítési tevékenységeknek az Egyesült Államok nemzeti érdekei számára nyújtott előnyeit, valamint az e tevékenységekből eredő kockázatokat), továbbá a 6. szakasz kivételével (amely általános rendelkezéseket tartalmaz), lásd a 28. elnöki politikai irányelv részleges visszavonásáról szóló nemzetbiztonsági feljegyzést, amely a https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/ internetcímen érhető el.

([230]) Lásd: 14086. elnöki rendelet, 5(f) szakasz, amely kifejti, hogy az elnöki rendelet alkalmazási köre megegyezik a PPD-28 alkalmazási körével, amely a 3. lábjegyzet szerint a kommunikáció vagy kommunikációval kapcsolatos információk gyűjtése céljából végzett jelfelderítési tevékenységekre vonatkozott, kivéve a jelfelderítési képességek tesztelése vagy fejlesztése céljából végzett jelfelderítési tevékenységeket.

([231]) E tekintetben lásd például a 14086. elnöki rendelet 5. szakaszának h) pontját, amely egyértelművé teszi, hogy a gazdasági szereplő biztosítékai jogi jogosultságot keletkeztetnek, és azokat magánszemélyek a jogorvoslati mechanizmuson keresztül érvényesíthetik.

([232]) Lásd: 14086. elnöki rendelet 2. szakasza (c) pontja (iv) alpontjának (C) szakasza.

felülvizsgálatnak a PCLOB általi befejezését követő 180 napon belül minden hírszerző ügynökségnek gondosan meg kell vizsgálnia és végre kell hajtania a PCLOB valamennyi ajánlását, vagy más módon kell kezelnie azokat. Az Egyesült Államok kormánya 2023. július 3-án közzétettte ezeket az aktualizált szabálytazokat és eljárásokat ([233]).

3.2.1.2. *A személyes adatok nemzetbiztonsági célú gyűjtésére vonatkozó korlátozások és biztosítékok*

(127) A 14086. elnöki rendelet számos átfogó követelményt határoz meg, amelyek valamennyi jelfelderítési tevékenységre vonatkoznak (személyes adatok gyűjtése, felhasználása, terjesztése stb.).

(128) Először is az ilyen tevékenységeknek törvényen vagy elnöki felhatalmazáson kell alapulniuk, és azokat az Egyesült Államok jogával, többek között az alkotmánnyal összhangban kell végezni ([234]).

(129) Másodszor, megfelelő biztosítékokat kell bevezetni annak biztosítására, hogy az adatvédelem és a polgári szabadságjogok szerves részét képezzék az ilyen tevékenységek tervezésének ([235]).

(130) Jelfelderítési tevékenységet csak azt követően lehet végezni, hogy „valamennyi releváns tényező észszerű értékelése alapján megállapítást nyert, hogy a tevékenységek szükségesek egy validált hírszerzési prioritás előmozdításához" (a „validált hírszerzési prioritás" fogalmát illetően lásd a (135) preambulumbekezdést) ([236]).

(131) Ezenkívül az ilyen tevékenységeket csak „az engedélyezett hírszerzési prioritással arányos mértékben és módon" lehet végezni ([237]). Más szóval megfelelő egyensúlyt kell teremteni „az elérni kívánt hírszerzési prioritás fontossága és az érintett személyek magánéletére és polgári szabadságaira gyakorolt hatás között, állampolgárságuktól vagy tartózkodási helyüktől függetlenül" ([238]).

(132) Végezetül, ezen – a jogszerűség, a szükségesség és az arányosság elvét tükröző – általános követelményeknek való megfelelés biztosítása érdekében a jelfelderítési tevékenységek felügyelet alá tartoznak (lásd részletesebben a 3.2.2. szakaszt) ([239]).

(133) Ezeket az átfogó követelményeket a jelfelderítés gyűjtése tekintetében számos feltétel és korlátozás támasztja alá, amelyek biztosítják, hogy az egyének jogaiba való beavatkozás a jogszerű cél eléréséhez szükséges és arányos mértékre korlátozódjon.

(134) Először is, az elnöki rendelet kétféleképpen korlátozza azokat az indokokat, amelyek alapján a jelfelderítési tevékenységek keretében adatokat lehet gyűjteni. Egyrészt a gazdasági szereplő meghatározza azokat a jogszerű célokat, amelyeket a jelfelderítési adatgyűjtés követhet, például az Egyesült Államok nemzetbiztonságára jelenleg vagy potenciálisan veszélyt jelentő külföldi szervezetek – köztük a nemzetközi terrorista szervezetek – képességeinek, szándékainak vagy tevékenységeinek megértése vagy értékelése céljából; a külföldi katonai képességekkel és tevékenységekkel szembeni védelem céljából; a globális biztonságot befolyásoló transznacionális fenyegetések, például az éghajlatváltozás és más ökológiai változások, a közegészségügyi kockázatok és a humanitárius fenyegetések megértése vagy értékelése érdekében ([240]). Másrészről az elnöki rendelet felsorol bizonyos

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) 14086. elnöki rendelet 2. szakasza (a) alpontjának (i) alpontja.

([235]) 14086. elnöki rendelet 2. szakasza (a) alpontjának (ii) alpontja.

([236]) 14086. elnöki rendelet 2. szakasza (a) pontjának (ii) alpontjának (A) szakasza. Ez nem mindig követeli meg, hogy a jelfelderítés legyen az egyetlen eszköz a validált hírszerzési prioritás szempontjainak előmozdítására. Például a jelfelderítés gyűjtése felhasználható alternatív érvényesítési módok biztosítására (pl. más hírszerzési forrásokból kapott információk megerősítésére) vagy az ugyanazon információkhoz való megbízható hozzáférés fenntartására (14086. elnöki rendelet 2. szakasza (c) pontja (i) alpontjának (A) szakasza).

([237]) 14086. elnöki rendelet 2. szakasza (a) pontja (ii) alpontjának (B) szakasza.

([238]) 14086. elnöki rendelet 2. szakasza (a) pontja (ii) alpontjának (B) szakasza.

([239]) A 2. szakasz (a) pontjának (iii) alpontja, összefüggésben a 14086. elnöki rendelet 2. szakaszának (d) pontjával.

([240]) 14086. elnöki rendelet 2. szakasza (b) pontjának (i) alpontja. Mivel az elnöki rendelet a jogos célkitűzéseket – amelyek nem tartalmazzák a lehetséges jövőbeli fenyegetéseket – korlátozottan sorolja fel, lehetővé teszi az elnök számára, hogy frissítse ezt a listát, ha új nemzetbiztonsági követelmények merülnek fel, mint például a nemzetbiztonságot érintő új fenyegetések. Az ilyen frissítéseket főszabály szerint nyilvánosan közzé kell tenni, kivéve, ha az elnök úgy ítéli meg, hogy önmagában a közzététel veszélyeztetné az Egyesült Államok nemzetbiztonságát (14086. elnöki rendelet 2. szakasza (b) pontja (i) alpontjának (B) szakasza).

célkitűzéseket, amelyeket a jelfelderítési tevékenységek soha nem követhetnek, például a kritika, az eltérő vélemény, vagy az eszmék vagy politikai vélemények egyének vagy sajtó általi szabad kifejezésének akadályozása érdekében; emberek személyek etnikai hovatartozásuk, fajuk, nemük, nemi identitásuk, szexuális irányultságuk vagy vallásuk alapján történő hátrányos megkülönböztetése céljából; vagy versenyelőny biztosítása érdekében az egyesült államokbeli vállalatok számára ([241]).

(135) Ezenkívül a hírszerző ügynökségek önmagukban nem hivatkozhatnak a 14086. elnöki rendeletben meghatározott jogszerű célokra a jelfelderítési adatgyűjtés igazolása érdekében, hanem azokat operatív célból további konkrét prioritásokra kell alapozni, amelyek tekintetében jelfelderítés gyűjthető. Más szóval a tényleges gyűjtésre csak egy konkrétabb prioritás előmozdítása érdekében kerülhet sor. Ezeket a prioritásokat egy célzott folyamat keretében határozzák meg, amelynek célja az alkalmazandó jogi követelményeknek való megfelelés biztosítása, beleértve az adatvédelemre és a polgári szabadságjogokra vonatkozó követelményeket is. Konkrétabban, a hírszerzési prioritásokat először a nemzeti hírszerzési igazgató dolgozza ki (az úgynevezett nemzeti hírszerzési prioritások keretrendszerén keresztül), és jóváhagyásra benyújtja az elnöknek ([242]). Mielőtt hírszerzési prioritásokat javasolna az elnöknek, az igazgatónak a 14086. elnöki rendelettel összhangban be kell szereznie az ODNI CLPO-tól az egyes prioritásokra vonatkozó értékeléseket azzal kapcsolatban, hogy 1. azok az elnöki rendeletben felsorolt egy vagy több jogszerű célkitűzést valósítanak-e meg, 2. nem arra a célra tervezték, hogy jelfelderítési adatgyűjtést eredményezzen az elnöki rendeletben felsorolt tiltott cél érdekében, és ez az eredmény előzetesen nem is várható, és 3. azt követően hozták létre, hogy megfelelően figyelembe vették valamennyi személy magánéletét és polgári szabadságjogait, állampolgárságuktól vagy tartózkodási helyüktől függetlenül ([243]). Amennyiben az igazgató nem ért egyet a CLPO értékelésével, mindkét véleményt ismertetni kell az elnökkel ([244]).

(136) Ezért ez a folyamat különösen azt biztosítja, hogy a magánélet védelmével kapcsolatos megfontolásokat már a hírszerzési prioritások kidolgozásának kezdeti szakaszától figyelembe vegyék.

(137) Másodszor, a hírszerzési prioritás megállapítását követően számos követelmény szabályozza annak eldöntését, hogy gyűjthető-e jelfelderítés e prioritás előmozdítása érdekében, és ha igen, milyen mértékben. Ezek a követelmények működőképessé teszik az elnöki rendelet 2. szakaszának (a) pontjában meghatározott átfogó szükségességi és arányossági normákat.

(138) Jelfelderítést csak „annak megállapítását követően lehet gyűjteni, hogy az összes releváns tényező észszerű értékelése alapján az adatgyűjtés szükséges egy konkrét hírszerzési prioritás előmozdításához” ([245]). Annak meghatározásakor, hogy szükség van-e konkrét jelfelderítési adatgyűjtési tevékenységre egy validált hírszerzési prioritás előmozdítása érdekében, az Egyesült Államok hírszerző ügynökségeinek figyelembe kell venniük más, kevésbé beavatkozó források és módszerek rendelkezésre állását, megvalósíthatóságát és megfelelőségét, beleértve a diplomáciai és nyilvános forrásokat is ([246]). Amennyiben rendelkezésre állnak, előnyben kell részesíteni az ilyen alternatív, kevésbé beavatkozó forrásokat és módszereket ([247]).

(139) Ha az ilyen kritériumok alkalmazása során szükségesnek ítélik a jelfelderítési adatok gyűjtését, annak olyan „testreszabottnak kell lennie, amennyire lehetséges”, és „nem befolyásolhatja aránytalanul a magánéletet és a polgári szabadságjogokat” ([248]). Annak biztosítása érdekében, hogy a magánéletet és a polgári szabadságjogokat ne érintsék aránytalanul – azaz megfelelő egyensúlyt teremtve a nemzetbiztonsági igények, valamint a magánélet és a polgári szabadságjogok védelme között – minden releváns tényezőt megfelelően figyelembe kell venni, mint például a kitűzött cél jellegét; a gyűjtési tevékenység beavatkozó jellegét, beleértve annak időtartamát; a gyűjtésnek a kitűzött célhoz való várható hozzájárulását; az egyéneket érintő, előre látható következményeket; valamint a gyűjtendő adatok jellegét és érzékenységét ([249]).

([241]) 14086. elnöki rendelet 2. szakasza (b) pontjának (ii) alpontja.
([242]) A nemzetbiztonsági törvény 102A. szakasza és a 14086. elnöki rendelet 2. szakasza (b) pontjának (iii) alpontja.
([243]) Kivételes esetekben (különösen, ha ez a folyamat új vagy változó hírszerzési követelmény miatt nem hajtható végre), ezeket a prioritásokat közvetlenül az elnök vagy a Hírszerző Közösség valamely elemének vezetője határozhatja meg, akinek elvben ugyanazokat a kritériumokat kell alkalmaznia, mint amelyeket a 2. szakasz (b) pontja (iii) alpontja (A) szakasza (1)–(3) alpontja, lásd az EO 14086 4. szakaszának (n) pontját.
([244]) 14086. elnöki rendelet 2. szakasza (b) pontja (iii) alpontjának (C) szakasza.
([245]) 14086. elnöki rendelet 2. szakasza (b) és (c) pontja (i) alpontjának (A) szakasza.
([246]) 14086. elnöki rendelet, 2. szakasza (c) pontja (i) alpontjának (A) szakasza.
([247]) 14086. elnöki rendelet, 2. szakasza (c) pontja (i) alpontjának (A) szakasza.
([248]) 14086. elnöki rendelet 2. szakasza (c) pontja (i) alpontjának (B) szakasza.
([249]) 14086. elnöki rendelet 2. szakasza (c) pontja (i) alpontjának (B) szakasza.

(140) Ami a jelfelderítési adatgyűjtés típusát illeti, az Egyesült Államokon belüli adatgyűjtést, amely a jelen megfelelőségi megállapítás szempontjából a legrelevánsabb, mivel az egyesült államokbeli szervezeteknek továbbított adatokra vonatkozik, mindig célzottnak kell tekinteni, amint azt a (142)–(153) preambulumbekezdés részletesebben kifejti.

(141) „Tömeges adatgyűjtés" ([250]) csak az Egyesült Államokon kívül, a 12333. elnöki rendelet alapján végezhető. Ebben az esetben is a 14086. elnöki rendelet szerint a célzott gyűjtést kell előnyben részesíteni ([251]). Ezzel szemben a tömeges adatgyűjtés csak akkor megengedett, ha a validált hírszerzési prioritás előmozdításához szükséges információk célzott gyűjtéssel észszerűen nem szerezhetők be ([252]). Amennyiben tömeges adatgyűjtésre van szükség az Egyesült Államokon kívül, a 14086. elnöki rendelet szerinti különleges biztosítékok alkalmazandók ([253]). Először is módszereket és technikai intézkedéseket kell alkalmazni annak érdekében, hogy az összegyűjtött adatok csak arra korlátozódjanak, ami egy validált hírszerzési prioritás előmozdításához szükséges, ugyanakkor minimálisra kell csökkenteni a nem releváns információk gyűjtését ([254]). Másodszor, az elnöki rendelet hat konkrét célkitűzésre korlátozza a tömegesen gyűjtött információk felhasználását (beleértve a lekérdezést is), beleértve a terrorizmus elleni védelmet, a túszejtést, valamint a külföldi kormány, szervezet vagy személy által vagy nevében fogva tartott személyek fogva tartását; a külföldi kémkedés, szabotázs vagy gyilkosság elleni védelmet; a tömegpusztító fegyverek vagy a kapcsolódó technológiák és fenyegetések fejlődéséből vagy elterjedéséből eredő fenyegetésekkel szembeni védelmet ([255]). Végezetül a tömegesen szerzett jelfelderítési adatok lekérdezésére csak akkor kerülhet sor, ha ez egy validált hírszerzési prioritás előmozdítása érdekében szükséges, e hat célkitűzés megvalósítása érdekében, valamint azon szabályzatokkal és eljárásokkal összhangban, amelyek megfelelően figyelembe veszik a lekérdezéseknek az összes személy magánéletére és polgári szabadságaira gyakorolt hatását, állampolgárságuktól vagy tartózkodási helyüktől függetlenül ([256]).

(142) A 14086. elnöki rendelet követelményein túlmenően az egyesült államokbeli szervezetnek továbbított adatok jelfelderítési gyűjtésére a FISA 702. szakasza által szabályozott egyedi korlátozások és biztosítékok vonatkoznak ([257]). A FISA 702. szakasza lehetővé teszi a külföldi hírszerzési információk gyűjtését olyan nem amerikai személyek megcélzása révén, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak, az Egyesült Államok elektronikus hírközlési szolgáltatóinak kötelező segítségével ([258]). A FISA 702. szakasza szerinti külföldi hírszerzési információk gyűjtése érdekében a legfőbb ügyész és a nemzeti hírszerzés igazgatója éves tanúsítványokat nyújt be a Külföldi Hírszerzést Felügyelő Bíróságnak (FISC), amelyek meghatározzák

([250]) Azaz nagy mennyiségű jelfelderítés gyűjtése, amelyet műszaki vagy üzemeltetési megfontolások miatt megkülönböztető eszközök (például egyedi azonosítók vagy kiválasztási kritériumok használata) nélkül szereznek be, lásd az EO 14086 4. szakaszának (b) pontját. A 14086. elnöki rendeletben és a (141) preambulumbekezdésben kifejtettek szerint a 12333. elnöki rendelet szerinti tömeges adatgyűjtésre csak akkor kerül sor, ha az egyedi validált hírszerzési prioritások előmozdításához szükséges, és arra számos korlátozás és biztosíték vonatkozik, amelyek célja annak biztosítása, hogy az adatokhoz különbségtétel nélkül ne férjenek hozzá. A tömeges gyűjtést ezért össze kell vetni az általános és különbségtétel nélküli gyűjtéssel („tömeges megfigyelés"), korlátozások és biztosítékok nélkül.

([251]) 14086. elnöki rendelet 2. szakasza (c) pontja ii. alpontjának (A) szakasza.

([252]) 14086. elnöki rendelet 2. szakasza (c) pontja ii. alpontjának (A) szakasza.

([253]) A 14086. elnöki rendelet tömeges gyűjtésre vonatkozó különös szabályai olyan célzott jelfelderítési tevékenységre is vonatkoznak, amely ideiglenesen megkülönböztető elemek (pl. konkrét kiválasztási kifejezések vagy azonosítók) nélkül szerzett, azaz tömeges adatokat használ fel (ami csak az Egyesült Államok területén kívül lehetséges). Nem ez a helyzet akkor, ha ezeket az adatokat csak a célzott jelfelderítési adatgyűjtési tevékenység kezdeti technikai szakaszának támogatására használják fel, és csak a szakasz befejezéséhez szükséges rövid ideig őrzik meg, majd azt követően azonnal törlik (14086. elnöki rendelet, 2. szakasz, (c) pont, (ii) alpont, (D) szakasz). Ebben az esetben a megkülönböztető elemet nem tartalmazó első adatgyűjtés egyetlen célja az információk célzott gyűjtésének lehetővé tétele egy adott azonosító vagy kiválasztási kritérium alkalmazásával. Ilyen forgatókönyv esetén csak azokat az adatokat viszik be a kormányzati adatbázisokba, amelyek egy bizonyos diszkrimináns alkalmazására reagálnak, míg a fennmaradó adatokat megsemmisítik. Az ilyen célzott adatgyűjtésre ezért a jelfelderítési adatgyűjtésre vonatkozó általános szabályok irányadók, beleértve a 14086. elnöki rendelet 2. szakaszának (a) és (b) pontját, valamint 2. szakasza (c) pontjának (i) alpontját.

([254]) 14086. elnöki rendelet 2. szakasza (c) pontja ii. alpontjának (A) szakasza.

([255]) 14086. elnöki rendelet 2. szakasza (c) pontja (ii) alpontjának (B) szakasza. Amennyiben új nemzetbiztonsági követelmények, például új nemzetbiztonsági fenyegetések merülnek fel, az elnök frissítheti ezt a listát. Az ilyen frissítéseket főszabály szerint nyilvánosan közzé kell tenni, kivéve, ha az elnök megállapítja, hogy ez önmagában kockázatot jelentene az Egyesült Államok nemzetbiztonságára nézve (a 14086. elnöki rendelet 2. szakasza (c) pontja (i) alpontjának (C) szakasza). A tömegesen gyűjtött adatok lekérdezése tekintetében lásd a 14086. elnöki rendelet 2. szakasz (c) pontja (iii) alpontjának (D) szakasza.

([256]) A 2. szakasz (a) pontjának (iii) alpontjának (A) szakasza, összefüggésben a 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontjának (D) szakaszával. Lásd továbbá a VII. mellékletet.

([257]) 50 U.S.C. § 1881.

([258]) 50 U.S.C. § 1881a (a). Különösen, amint azt a PCLOB megjegyezte, a 702. szakasz szerinti megfigyelés „teljes egészében olyan konkrét [nem egyesült államokbeli] személyek megcélzásából áll, akikről egyedi döntést hoztak" (Adatvédelmi és Polgári Szabadságjogi Felügyeleti Testület, Jelentés a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. cikke szerint működtetett felügyeleti programról, 2014. július 2., 702. szakaszra vonatkozó jelentés, 111. o.). Lásd még: NSA CLPO, A külföldi hírszerzői tevékenységről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014. április 16. Az „elektronikus hírközlési szolgáltató" fogalmának meghatározása megtalálható itt: 50 U.S.C. § 1881 (a)(4).

a beszerzendő külföldi hírszerzési információk kategóriáit ([259]). A tanúsítványokat célzott, minimalizáló és lekérdezési eljárásoknak kell kísérniük, amelyeket a Bíróság is jóváhagyott, és amelyek jogilag kötelező erejűek az Egyesült Államok hírszerző ügynökségeire nézve.

(143) A FISC szövetségi törvény által létrehozott független bíróság ([260]), amelynek határozatai ellen fellebbezést lehet benyújtani a Külföldi Hírszerzést Felügyelő Fellebbviteli Bírósághoz ([261]) (FISCR), és végső soron az Egyesült Államok Legfelsőbb Bíróságához ([262]). A FISC (és a FISCR) munkáját öt jogászból és öt külső szakértőből álló állandó testület segíti, akik nemzetbiztonsági ügyekben, valamint a polgári szabadságjogok terén rendelkeznek szaktudással ([263]). A bíróság e csoportból kijelölt egy személyt, aki az *amicus curiae* szerepében segíti az olyan végzés vagy felülvizsgálat iránti kérelmek elbírálását, amelyek a bíróság véleménye szerint a törvény újszerű vagy jelentős értelmezését tartalmazzák, kivéve ha a bíróság megállapítja, hogy a kijelölés nem helyénvaló ([264]). Ez különösen azt biztosítja, hogy az adatvédelmi megfontolások kellőképpen tükröződjenek a bíróság értékelésében. A bíróság egyént vagy szervezetet is kijelölhet az amicus curiae szerepére, többek között technikai szakértelem biztosítására minden olyan esetben, amikor ezt helyénvalónak ítéli, vagy kérelemre lehetővé teheti, hogy egy egyén vagy szervezet *amicus curiae* levelet terjesszen elő ([265]).

(144) A FISC felülvizsgálja a tanúsítványokat és a kapcsolódó eljárásokat a FISA követelményeinek való megfelelés szempontjából (különösen a célkiválasztási és -minimalizálási eljárásokat). Amennyiben úgy ítéli meg, hogy a követelmények nem teljesülnek, részben vagy egészben megtagadhatja a tanúsítást, és kérheti az eljárások módosítását ([266]). E tekintetben a FISC ismételten megerősítette, hogy a 702. szakasz szerinti célkiválasztási és -minimalizálási eljárások felülvizsgálata nem korlátozódik az írásbeli eljárásokra, hanem kiterjed arra is, hogy a kormány hogyan hajtja végre az eljárásokat ([267]).

(145) Az egyedi célkiválasztást a Nemzetbiztonsági Ügynökség (NSA, a FISA 702. szakasza szerint a célkiválasztásért felelős hírszerző ügynökség) végzi a FISC által jóváhagyott célkiválasztási eljárásokkal összhangban, amelyek értelmében az NSA-nak a körülmények összessége alapján értékelnie kell, hogy egy adott személy megcélzásával valószínűleg megszerezhető-e a tanúsítványban azonosított külföldi hírszerzési információk egy kategóriája ([268]). Ennek az értékelésnek specifikusnak és tényeken alapulónak kell lennie, analitikus megítélésen, az elemző speciális

([259]) 50 U.S.C. § 1881a (g).

([260]) A FISC az Egyesült Államok főbírája által kinevezett bírókból áll, akiket korábban az elnök által a Szenátus megerősítésével kinevezett, egyesült államokbeli kerületi bíróságokban ülésező bírák közül választanak ki. A határozatlan időre szóló kinevezéssel rendelkező bírák, akik csak indokolt esetben menthetők fel, különböző időpontokban kezdve hétéves hivatali ideig látják el beosztásukat a FISC-en. A FISA előírja, hogy a bírákat legalább hét különböző amerikai fellebbviteli bíróságról kell választani. Lásd: 50 U.S.C. § 1803 (a). A bírákat tapasztalt bírósági tisztségviselők segítik. Ők alkotják a bíróság jogi személyzetét, amely jogi elemzést készít az adatgyűjtési kérelmekről. Lásd: Reggie B. Walton, a Külföldi Hírszerzést Felügyelő Bíróság elnöklő bírójának levele Patrick J. Leahyhez, az Egyesült Államok szenátusa igazságügyi bizottságának elnökéhez (2013. július 29.) (Walton-levél) 2. o., elérhető itt: https://fas.org/irp/news/2013/07/fisc-leahy.pdf

([261]) A FISCR az Egyesült Államok főbírája által kinevezett három bíróból áll, akiket az Egyesült Államok kerületi bíróságairól és kerületi fellebbviteli bíróságairól választanak ki, és különböző időpontokban kezdve hétéves hivatali ideig látják el beosztásukat. Lásd: 50 U.S. C. § 1803 (b).

([262]) Lásd: 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([263]) 50 U.S.C. § 1803 (i)(1),(3)(A).

([264]) 50 U.S.C. § 1803 (i)(2)(A).

([265]) 50 U.S.C. § 1803 (i)(2)(B).

([266]) Lásd például a FISC 2018. október 18-i véleményét, amely elérhető a https://www.intelligence.gov/assets/documents/702% 20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf oldalon, amint azt a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróság 2019. július 12-i véleményében megerősítette, amely elérhető itt: https://www. intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf

([267]) Lásd pl. FISC, Memorandum Opinion and Order, 35 (2020. november 18.) (A nyilvános közzététel engedélyezése: 2021. április 26.) (D. melléklet).

([268]) 50 U.S.C. § 1881a(a), a Nemzetbiztonsági Ügynökség által a külföldi hírszerzői tevékenység megfigyeléséről szóló, 2018. márciusban módosított, 1978. évi törvény 702. szakasza szerinti külföldi hírszerzési információk megszerzése céljából az Egyesült Államok területén kívül található nem egyesült államokbeli személyek célkiválasztására alkalmazott eljárások (az NSA célkiválasztási eljárásai), elérhető itt: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19. pdf–4. o., további magyarázat a PCLOB-jelentés 41–42. oldalán.

képzésén és tapasztalatán, valamint a beszerzendő külföldi hírszerzési információk jellegén kell alapulnia ([269]). A célkiválasztást olyan úgynevezett választók azonosításával hajtják végre, amelyek azonosítják a konkrét kommunikációs eszközöket, például a célpont e-mail-címét vagy telefonszámát, de soha nem kulcsszavakat vagy az egyének nevét ([270]).

(146) Először az NSA elemzői azonosítják azt a külföldön tartózkodó nem amerikai célszemélyt, akinek a megfigyelése az elemzők értékelése alapján elvezet a tanúsítványban meghatározott, releváns külföldi hírszerzési információkhoz ([271]). Az NSA célkiválasztási eljárásaiban foglaltak szerint az NSA csak akkor irányíthatja a megfigyelést egy célpontra, ha már megtudott valamit a célpontról ([272]). Ez különböző forrásokból származó információkból eredhet, például emberi hírszerzésből származó információkból. Ezen egyéb források révén az elemzőnek meg kell ismernie a potenciális célpont által használt konkrét kiválasztási tényezőt (azaz kommunikációs fiókot). Másodsorban, miután azonosították a szóban forgó, egyénileg megjelölt személyeket, és az NSA-n belüli, kiterjedt felülvizsgálati mechanizmus jóváhagyta a célkiválasztást ([273]), „rádolgoznak" a célszemély által használt kommunikációs eszközöket (például email címeket) azonosító, kiválasztási tényezőkre (vagyis kidolgozzák és alkalmazzák azokat) ([274]).

(147) Az NSA-nak dokumentálnia kell a célkiválasztás ténybeli alapját ([275]), és a kezdeti célkiválasztást követően rendszeres időközönként meg kell erősítenie, hogy a célmeghatározási előírás továbbra is teljesül ([276]). Ha a célmeghatározási előírás már nem teljesül, a gyűjtést meg kell szüntetni ([277]). Az Igazságügyi Minisztérium hírszerzési felügyeleti hivatalainak tisztviselői kéthavonta felülvizsgálják az egyes célpontok NSA általi kiválasztását, valamint az általuk rögzített célkiválasztási értékelésekről és indokokról készült feljegyzéseket a célkiválasztási eljárásoknak való megfelelés szempontjából, és kötelesek jelenteni a FISC-nek és a Kongresszusnak az esetleges jogsértéseket ([278]). A (173)–(174) preambulumbekezdésben ismertetett felügyeleti hatáskörével összhangban az NSA írásbeli dokumentációja megkönnyíti a FISC számára annak felügyeletét, hogy a FISA 702. szakasza alapján egyes személyeket megfelelően megcéloznak-e ([279]). Végezetül a nemzeti hírszerzési igazgatónak a nyilvános éves statisztikai átláthatósági jelentésekben minden évben be kell számolnia a FISA 702. szakasza szerinti célok teljes számáról. A FISA-irányelvek 702. szakaszának hatálya alá tartozó vállalatok összesített adatokat tehetnek közzé (átláthatósági jelentések útján) a hozzájuk beérkezett kérelmekről ([280]).

([269]) Az NSA célkiválasztási eljárásai, 4. o.

([270]) Lásd: PCLOB, a 702. szakaszra vonatkozó jelentés, 32–33., 45. o., további hivatkozásokkal. Lásd még: a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakasza szerint kiadott eljárások és iránymutatások betartásának a legfőbb ügyész és a nemzeti hírszerzés igazgatója által benyújtott féléves értékelését, jelentési időszak: 2016. december 1. – 2017. május 31., 41. o., (2018. október), elérhető itt: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([271]) PCLOB, a 702. szakaszra vonatkozó jelentés, 42–43. o.

([272]) Az NSA célkiválasztási eljárásai, 2. o.

([273]) PCLOB, a 702. szakaszra vonatkozó jelentés, 46. o. Az NSA-nak például ellenőriznie kell a célpont és a kiválasztási tényező közötti kapcsolatot, dokumentálnia kell a várhatóan megszerezhető külföldi hírszerzési információt, továbbá az NSA két magas rangú elemzőjének felül kell vizsgálnia és jóvá kell hagynia ezeket az információkat, valamint az ODNI és az Egyesült Államok Igazságügyi Minisztériuma által végzett későbbi megfelelőségi felülvizsgálatok céljából nyomon kell követnie az egész folyamatot. Lásd: NSA CLPO, A külföldi hírszerzői tevékenységről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014. április 16.

([274]) 50 U.S.C. § 1881a (h).

([275]) Az NSA célkiválasztási eljárásai, 8. o. Lásd még a PCLOB 702. szakaszról szóló jelentését, 46. o. Az írásbeli indokolás elmulasztása a dokumentációnak való megfeleléssel kapcsolatos incidensnek minősül, amelyet jelenteni kell a FISC-nek és a Kongresszusnak. Lásd: a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakasza szerint kiadott eljárások és iránymutatások betartásának a legfőbb ügyész és a nemzeti hírszerzés igazgatója által benyújtott féléves értékelését, jelentési időszak: 2016. december 1. – 2017. május 31., 41. o. (2018. október), DOJ/ODNI megfelelőségi jelentés a FISC számára a 2016. december és 2017. május közötti időszakra vonatkozóan, A-6. o., elérhető itt: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf

([276]) Lásd az Egyesült Államok kormányának beadványát a Külföldi Hírszerzést Felügyelő Bírósághoz, 2015. évi összefoglaló a 702. szakasz követelményeiről, 2–3. pont (2015. július 15.) és a VII. mellékletben megadott információkat.

([277]) Lásd: az Egyesült Államok kormányának 2015. évi beadványa a Külföldi Hírszerzést Felügyelő Bírósághoz, Összefoglaló a 702. szakasz szerinti követelményekről, 2–3. pont, (2015. július 15.), amely kimondja, hogy a kormány, „ha a kormány később úgy értékeli, hogy a célpont kiválasztásának folytatása várhatóan nem vezet külföldi hírszerzési információk megszerzéséhez, azonnali eltávolításra van szükség, és a késedelem bejelentendő megfelelési incidenst eredményezhet". Lásd még a VII. mellékletben megadott információkat.

([278]) PCLOB, a 702. szakaszra vonatkozó jelentés, 70–72. o.; Az Egyesült Államok Külföldi Hírszerzést Felügyelő Bírósága eljárási szabályzata 13. cikkének b) pontja, elérhető a következő internetcímen: https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([279]) Lásd még a DOJ/ODNI 2016. december – 2017. május közötti időszakra vonatkozó megfelelőségi jelentését a FISC számára, A-6. o.

([280]) 50 U.S.C. § 1874.

(148) Az egyesült államokbeli szervezeteknek továbbított személyes adatok gyűjtésének egyéb jogalapjai tekintetében különböző korlátozások és biztosítékok alkalmazandók. A tömeges adatgyűjtés általában kifejezetten tilos a FISA 402. szakasza (kimenő és a bejövő hívások adatait rögzítő eszközökért felelős hatóság) és az NSL alkalmazása révén, ehelyett konkrét „kiválasztási kritériumok" használata szükséges ([281]).

(149) A hagyományos egyedi elektronikus megfigyeléshez (a FISA 105. szakasza szerint) a hírszerző ügynökségeknek kérelmet kell benyújtaniuk a FISC-hez, amelyben nyilatkoznak azokról a tényekről és körülményekről, amelyek alapján feltételezhető, hogy alaposan gyanítható, hogy a létesítményt külföldi hatalom vagy külföldi hatalom megbízottja használja vagy használni fogja ([282]). A FISC többek között megvizsgálja, hogy az ismertetett tények alapján valószínűsíthető-e, hogy valóban ez a helyzet ([283]).

(150) A FISA 301. szakasza alapján a helyiségek vagy ingatlanok olyan átkutatásához, amelynek célja információk, anyagok vagy vagyontárgyak (pl. számítógépes eszköz) vizsgálata, lefoglalása stb., a FISC általi végzésre irányuló kérelem szükséges ([284]). Az ilyen kérelemnek többek között bizonyítania kell, hogy alaposan gyanítható, hogy a keresés célpontja külföldi hatalom vagy külföldi hatalom megbízottja; az átkutatandó helyiség vagy vagyon külföldi hírszerzési információt tartalmaz, és az átkutatandó helyiség külföldi hatalom (vagy annak megbízottja) tulajdonában van, azt használja, birtokolja vagy hozzá vagy tőle úton van ([285]).

(151) Hasonlóképpen, a kimenő és bejövő hívások adatait rögzítő eszközök telepítéséhez (a FISA 402. szakasza szerint) a FISC (vagy egy egyesült államokbeli főbíró) végzésére irányuló kérelem és egy konkrét kiválasztási kritérium használata szükséges, azaz olyan kritérium használata, amely kifejezetten azonosít egy személyt, fiókot stb., és amelyet a kért információ terjedelmének lehető legnagyobb mértékű korlátozására használnak ([286]). Az említett felhatalmazás nem a kommunikáció tartalmára vonatkozik, hanem a szolgáltatást igénybe vevő ügyféllel vagy előfizetővel kapcsolatos információkra (például név, cím, előfizetési szám, az igénybe vett szolgáltatás hossza/típusa, a fizetési forrás/mechanizmus).

(152) A FISA 501. szakasza ([287]), amely lehetővé teszi egy közös fuvarozó (azaz bármely személy vagy szervezet, aki vagy amely kompenzáció fejében személyeket vagy vagyontárgyakat szállít szárazföldön, vasúton, vízen vagy légi úton), nyilvános szálláshely (pl. szálloda, motel vagy fogadó), gépjármű-bérbeadó létesítmény vagy fizikai raktározási létesítmény üzleti adatainak gyűjtését ([288]), szintén előírja a FISC-hez vagy a főbíróhoz intézett kérelmet. A kérelemben fel kell tüntetni a keresett nyilvántartásokat, valamint azokat a konkrét és felfogható tényeket, amelyek alapján feltételezhető, hogy az a személy, akire a nyilvántartás vonatkozik, külföldi hatalom vagy külföldi hatalom megbízottja ([289]).

(153) Végezetül az NSL-eket különböző alapszabályok engedélyezik, és lehetővé teszik a nyomozó ügynökségek számára, hogy bizonyos, a hiteljelentésekben, a pénzügyi nyilvántartásokban, valamint az elektronikus előfizetői és tranzakciós nyilvántartásokban szereplő információkat megszerezzenek bizonyos szervezetektől (pl. pénzügyi intézményektől, hitelintézetektől, elektronikus hírközlési szolgáltatóktól) ([290]). Az NSL-ről szóló törvényt, amely engedélyezi az elektronikus hírközléshez való hozzáférést, csak az FBI használhatja, és előírja, hogy olyan kritériumot kell alkalmazni, amely kifejezetten azonosít egy személyt, szervezetet, telefonszámot vagy fiókot, és amely igazolja, hogy az információ a nemzetközi terrorizmussal vagy titkos hírszerzési tevékenységekkel szembeni védelem érdekében végzett engedélyezett nemzetbiztonsági nyomozás szempontjából releváns ([291]). A nemzetbiztonsági levelek címzettjei azokat bíróság előtt megtámadhatják ([292]).

([281]) 50 U.S. Code § 1842(c)(3) és az NSL tekintetében, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); és 18 U.S.C. § 2709(a).

([282]) A „külföldi hatalom megbízottjai" olyan nem amerikai személyek is lehetnek, akik nemzetközi terrorizmusban vagy tömegpusztító fegyverek nemzetközi elterjedésében vesznek részt (az előkészítő aktusokat is beleértve) (50 U.S.C. § 1801 (b)(1)).

([283]) 50 U.S.C. § 1804. A kiválasztási kritériumok megválasztásával kapcsolatban lásd még az § 1841 (4) bekezdését.

([284]) 50 U.S.C. § 1821(5).

([285]) 50 U.S.C. § 1823(a).

([286]) Az 50 U.S.C. 1842 §., 1841 §. (2) bekezdés, valamint a 18. cím 3127. szakasza.

([287]) 50 U.S.C. § 1862.

([288]) 50 U.S.C. §§ 1861–1862.

([289]) 50 U.S.C. § 1862(b).

([290]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u–1681v; és 18 U.S.C. § 2709.

([291]) 18 U.S.C. § 2709(b).

([292]) Pl. 18 U.S.C. § 2709(d).

3.2.1.3. *A gyűjtött adatok további felhasználása*

(154) Az amerikai hírszerző ügynökségek által jelfelderítés útján gyűjtött személyes adatok kezelésére számos biztosíték vonatkozik.

(155) Először is, minden hírszerző ügynökségnek biztosítania kell a megfelelő adatbiztonságot, és meg kell akadályoznia, hogy illetéktelen személyek hozzáférjenek a jelfelderítés útján gyűjtött személyes adatokhoz. E tekintetben a különböző eszközök, köztük a törvény, az iránymutatások és a szabványok tovább pontosítják a bevezetendő információbiztonsági minimumkövetelményeket (pl. többtényezős hitelesítés, titkosítás stb.) ([293]). Az összegyűjtött adatokhoz való hozzáférést az engedéllyel rendelkező, képzett személyzetre kell korlátozni, akinek ismernie kell a feladata teljesítéséhez szükséges információkat ([294]). Általánosabban fogalmazva, a hírszerző ügynökségeknek megfelelő képzést kell biztosítaniuk alkalmazottaik számára, többek között a jogszabályok (beleértve a 14086. elnöki rendeletet) megsértésének bejelentésére és kezelésére vonatkozó eljárásokról ([295]).

(156) Másodszor, a hírszerző ügynökségeknek meg kell felelniük a Hírszerző Közösség pontosságra és objektivitásra vonatkozó normáinak, különös tekintettel az adatok minőségének és megbízhatóságának biztosítására, az alternatív információforrások figyelembevételére és az elemzések tárgyilagosságára ([296]).

(157) Harmadszor, ami az adatmegőrzést illeti, a 14086. elnöki rendelet egyértelművé teszi, hogy a nem egyesült államokbeli személyek személyes adataira ugyanazok a megőrzési időszakok vonatkoznak, mint az egyesült államokbeli személyek adataira ([297]). A hírszerző ügynökségeknek meg kell határozniuk a konkrét megőrzési időszakokat és/vagy azokat a tényezőket, amelyeket figyelembe kell venni az alkalmazandó megőrzési időszakok hosszának meghatározásakor (pl. hogy az információ bűncselekmény bizonyítéka-e; az információ külföldi hírszerzési információnak minősül-e; az információ szükséges-e személyek vagy szervezetek biztonságának védelméhez, ideértve a nemzetközi terrorizmus áldozatait vagy célpontjait is), amelyeket különböző jogi eszközök határoznak meg ([298]).

(158) Negyedrészt, külön szabályok alkalmazandók a jelfelderítésen keresztül gyűjtött személyes adatok terjesztésére. Általános követelményként a nem egyesült államokbeli személyekre vonatkozó személyes adatok csak akkor terjeszthetők, ha ugyanolyan típusú információkat tartalmaznak, mint amelyek terjeszthetők az egyesült államokbeli személyekről, például egy személy vagy szervezet biztonságának védelméhez szükséges információkat (például a nemzetközi terrorista szervezetek célpontjairól, áldozatairól vagy túszairól) ([299]). Ezenkívül a személyes adatok nem terjeszthetők kizárólag az adott személy állampolgársága vagy lakóhelye szerinti ország miatt vagy a 14086. elnöki rendelet előírásainak megkerülése céljából ([300]). Az Egyesült Államok kormányán belüli terjesztésre csak akkor kerülhet sor, ha egy engedéllyel rendelkező és képzett személy megalapozottan feltételezi, hogy a

([293]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (B). szakaszának (1) alszakasza. Lásd még a nemzetbiztonsági törvény VIII. címét (amely a minősített adatokhoz való hozzáférésre vonatkozó követelményeket részletezi), a 12333. elnöki rendelet 1.5. szakaszát (amely előírja a Hírszerző Közösség ügynökségeinek, hogy tartsák be az információmegosztási és -biztonsági irányelveket, az információs önrendelkezési jogot, valamint egyéb jogi előírásokat), a nemzetbiztonságról szóló, 42. iránymutatást, a nemzetközi távközlési és információs rendszerek biztonságára vonatkozó nemzeti rendeletet (amely arra utasítja a nemzetbiztonsági rendszerekkel foglalkozó bizottságot, hogy nyújtson a nemzetbiztonsági rendszerekre vonatkozó rendszerbiztonsági iránymutatást a minisztériumok és hivatalok számára), valamint „A nemzetbiztonság, a Védelmi Minisztérium és a Hírszerző Közösség rendszerei kiberbiztonságának javítása” c. 8. nemzetbiztonsági feljegyzést (amely időrendi áttekintést és iránymutatást nyújt azzal kapcsolatban, hogy a nemzetbiztonsági rendszerekre vonatkozó kiberbiztonsági előírások végrehajtása miként történik, beleértve a többtényezős hitelesítést, a titkosítást, a felhőtechnológiákat és a végpontérzékelő szolgáltatásokat).

([294]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontjának (B) szakaszának (2) alszakasza. Ezenkívül azokhoz a személyes adatokhoz, amelyekre vonatkozóan nem született végleges megőrzési megállapítás, csak e megállapítás megtétele vagy támogatása, illetve engedélyezett adminisztratív, tesztelési, fejlesztési, biztonsági vagy felügyeleti feladatok ellátása céljából lehet hozzáférni (a 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (B) szakaszának (3) alszakasza).

([295]) 14086. elnöki rendelet 2. szakasza (d) pontjának (ii) alpontja.

([296]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontjának (C) szakasza.

([297]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (A) szakasza (2) alszakaszának (a)–(c) pontja. Általánosabban fogalmazva, minden ügynökségnek olyan szabályzatokat és eljárásokat kell bevezetnie, amelyek célja a jelfelderítés útján gyűjtött személyes adatok terjesztésének és megőrzésének minimalizálása (14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontjának (A) szakasza).

([298]) Lásd pl.: a 2015-ös költségvetési évre vonatkozó hírszerzési engedélyezési törvény 309. szakasza; az egyes hírszerző ügynökségek által a FISA 702. szakasza alapján elfogadott és a FISC által engedélyezett minimalizálási eljárások; a legfőbb ügyész és az FRA által jóváhagyott eljárások (amelyek előírják, hogy az Egyesült Államok szövetségi ügynökségei, beleértve a nemzetbiztonsági ügynökségeket is, adatmegőrzési időszakokat állapítsanak meg, amelyeket a Nemzeti Irattár és Nyilvántartási Hivatalnak jóvá kell hagynia).

([299]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (A) szakasza (1) alszakaszának (a) pontja és 5. szakaszának (d) pontja, összefüggésben a 12333. elnöki rendelet 2.3. szakaszával.

([300]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (A) szakasza (1) alszakaszának (b) és (e) pontja.

címzettnek ismernie kell az információt ([301]), és azt megfelelően védeni fogja ([302]). Annak meghatározásához, hogy a személyes adatok továbbíthatók-e az Egyesült Államok kormányán kívüli címzetteknek (ideértve a külföldi kormányt vagy nemzetközi szervezetet is), figyelembe kell venni a terjesztés célját, a terjesztett adatok jellegét és mértékét, valamint az érintett személy(ek)re gyakorolt lehetséges káros hatást ([303]).

(159) Végezetül, többek között az alkalmazandó jogi követelményeknek való megfelelés felügyeletének és a hatékony jogorvoslatnak a megkönnyítése érdekében a 14086. elnöki rendelet szerint minden hírszerző ügynökségnek megfelelő dokumentációt kell vezetnie a jelfelderítési adatgyűjtésről. A dokumentációs követelmények olyan elemekre terjednek ki, mint például annak tényszerű alapja, hogy egy adott adatgyűjtési tevékenységre szükség van-e egy validált hírszerzési prioritás előmozdításához ([304]).

(160) A 14086. elnöki rendeletnek a jelfelderítés által gyűjtött adatok használatára vonatkozó, fent említett garanciák mellett az Egyesült Államok valamennyi ügynökségére általánosabb követelmények vonatkoznak a célhoz kötöttség, az adattakarékosság, a pontosság, a biztonság, a megőrzés a terjesztés tekintetében, ami különösen az A-130. OMB-körlevélből, az e-közigazgatásról szóló törvényből, a szövetségi nyilvántartásokról szóló törvényből (lásd a (101)–(106) preambulumbekezdést) és a nemzetbiztonsági rendszerekkel foglalkozó bizottság CNSS) iránymutatásából ([305]) ered.

3.2.2. ***Felügyelet***

(161) Az amerikai hírszerző ügynökségek tevékenységét különböző szervek felügyelik.

(162) Először is, a 14086. elnöki rendelet megköveteli, hogy minden hírszerző ügynökség rendelkezzen magas szintű jogi, felügyeleti és megfelelési tisztviselőkkel az alkalmazandó egyesült államokbeli jogszabályoknak való megfelelés biztosítása érdekében ([306]). El kell végezniük különösen a jelfelderítési tevékenységek rendszeres felügyeletét, és biztosítaniuk kell, hogy minden meg nem felelést orvosoljanak. A hírszerző ügynökségeknek felügyeleti feladataik ellátása érdekében biztosítaniuk kell az ilyen tisztviselők számára az összes releváns információhoz való hozzáférést, és nem tehetnek semmilyen intézkedést felügyeleti tevékenységük akadályozására vagy nem megfelelő befolyásolására ([307]). Ezenkívül a felügyeleti tisztviselő vagy bármely más alkalmazott által azonosított jelentős meg nem felelési incidenseket ([308]) haladéktalanul jelenteni kell a hírszerző ügynökség vezetőjének és a nemzeti hírszerzés igazgatójának, akiknek gondoskodniuk kell arról, hogy minden szükséges intézkedést megtegyenek a jelentős meg nem felelési incidens orvoslására és megismétlődésének megelőzésére ([309]).

(163) Ezt a felügyeleti funkciót kijelölt megfelelési szerepkörrel rendelkező tisztviselők, valamint adatvédelmi és polgári jogi tisztviselők és főellenőrök töltik be ([310]).

([301]) Lásd pl. az AGG-DOM úgy rendelkezik, hogy az FBI csak akkor oszthat meg információkat, ha a címzettnek azokról tudnia kell a címzett küldetésének teljesítéséhez vagy a nyilvánosság védelméhez.

([302]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (A) szakasza (1) alszakaszának (c) pontja. A hírszerző ügynökségek például bűnügyi nyomozással vagy bűncselekménnyel kapcsolatos körülmények között terjeszthetnek információkat, például gyilkossággal, súlyos testi sértéssel vagy emberrablással való fenyegetésre vonatkozó figyelmeztetések terjesztése; kiberfenyegetések, incidensek vagy behatolással kapcsolatos válaszintézkedésekre információk terjesztése; és az áldozatok értesítése vagy a bűncselekmények potenciális áldozatainak figyelmeztetése révén.

([303]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontja (A) szakasza (1) alszakaszának (d) pontja.

([304]) 14086. elnöki rendelet 2. szakasza (c) pontja (iii) alpontjának (E) szakasza.

([305]) Lásd a CNSS 22. sz. szabályzatát (Kiberbiztonsági kockázatkezelési politika) és a CNSS 1253. sz. utasítását, amely részletes iránymutatást nyújt a nemzeti biztonsági rendszerek számára bevezetendő biztonsági intézkedésekről.

([306]) 14086. elnöki rendelet 2. szakasza (d) pontja (i) alpontjának (A)–(B) szakasza.

([307]) 14086. elnöki rendelet 2. szakasza (d) pontja (i) alpontjának (B)–(C) szakasza.

([308]) Azaz az alkalmazandó egyesült államokbeli jognak való megfelelés olyan rendszerszintű vagy szándékos elmulasztása, amely veszélyeztetheti a Hírszerző Közösség valamely elemének jó hírnevét vagy integritását, vagy más módon megkérdőjelezheti a Hírszerző Közösség tevékenységének megfelelőségét, többek között az érintett személy vagy személyek magánéletére és polgári szabadságjogaira gyakorolt jelentős hatás fényében, lásd a 14086. elnöki rendelet 5. szakaszának (l) pontját.

([309]) 14086. elnöki rendelet 2. szakasza (d) pontjának (iii) alpontja.

([310]) 14086. elnöki rendelet 2. szakasza (d) pontja (i) alpontjának (B) szakasza.

(164) A bűnüldöző hatóságokhoz hasonlóan az adatvédelmi és az állampolgári szabadságjogi tisztviselők is jelen vannak valamennyi hírszerző ügynökségnél ([311]). E tisztségviselők hatásköre általában felöleli az eljárások felügyeletét annak érdekében, hogy a megfelelő minisztérium/ügynökség megfelelően figyelembe vegye az adatvédelmi és polgári szabadságjogi megfontolásokat, valamint megfelelő eljárásokat alakítson ki az olyan egyénektől érkező panaszok kezelésére, akik úgy vélik, hogy megsértették az adatvédelemhez fűződő vagy polgári szabadságjogaikat (és egyes esetekben, például a Nemzeti Hírszerzési Igazgatóság (ODNI) esetében, hatáskörük a panaszok kivizsgálására is kiterjedhet ([312])). Az egyes hírszerzési ügynökségek vezetőinek gondoskodniuk kell arról, hogy a magánélet védelmével és az állampolgári szabadságjogokkal foglalkozó tisztviselők rendelkezzenek a megbízatásuk teljesítéséhez szükséges erőforrásokkal, hozzáférjenek a feladataik ellátásához szükséges valamennyi anyaghoz és személyzethez, továbbá tájékoztatást kapjanak a javasolt szakpolitikai változásokról, és konzultáljanak velük azokról ([313]). Az adatvédelmi és polgári szabadságjogi tisztségviselők időszakonként beszámolnak a Kongresszusnak és a PCLOB-nak többek között a minisztériumhoz/ügynökséghez beérkezett panaszok számáról és jellegéről, valamint az ilyen panaszok rendezésének összefoglalásáról, a tisztviselő által lefolytatott felülvizsgálatokról és vizsgálatokról és az általa végzett tevékenység hatásáról ([314]).

(165) Másodszor, minden hírszerző ügynökség rendelkezik egy független főellenőrrel, akinek feladata többek között a külföldi hírszerzési tevékenységek felügyelete. Így többek között az ODNI keretében működő, a Hírszerző Közösség főellenőri hivatala átfogó hatáskörrel rendelkezik a teljes hírszerzés felett, és jogosult kivizsgálni a jogellenes tevékenységgel vagy hatalommal való visszaéléssel kapcsolatos – az ODNI és/vagy a hírszerzési szervezetek programjait és tevékenységét érintő – panaszokat vagy információkat ([315]). A bűnüldöző hatóságokhoz hasonlóan (lásd a (109) preambulumbekezdést), az ilyen főellenőrök független jogállású szervezeti egységek ([316]), amelyek a megfelelő ügynökség által végzett, nemzetbiztonsági célú programokkal és műveletekkel – így a törvénysértésekkel és visszaélésekkel – kapcsolatos ellenőrzések és vizsgálatok elvégzésért felelősek ([317]). Betekinthetnek valamennyi

([311]) Lásd: 42 U.S.C. § 2000ee-1. Ez magában foglalja például a Külügyminisztériumot, az Igazságügyi Minisztériumot, a Belbiztonsági Minisztériumot, a Védelmi Minisztériumot, az NSA-t, a Központi Hírszerző Ügynökséget (CIA), és az ODNI-t.

([312]) Lásd: 14086. elnöki rendelet 3. szakaszának (c) pontja.

([313]) 42 U.S.C. § 2000ee-1(d).

([314]) Lásd: 42 U.S.C. § 2000ee-1 (f)(1),(2). Például az NSA Állampolgári Jogi, Adatvédelmi és Átláthatósági Hivatalának 2021. január és 2021. június közötti időszakra vonatkozó jelentése azt mutatja, hogy 591 felülvizsgálatot végzett a polgári szabadságjogokra és a magánélet védelmére gyakorolt hatások tekintetében különböző kontextusokban, például a gyűjtési tevékenységek, az információmegosztási megállapodások és határozatok, az adatmegőrzési határozatok stb. tekintetében, figyelembe véve különböző tényezőket, például a tevékenységhez kapcsolódó információk mennyiségét és típusát, az érintett egyéneket, az adatok célját és tervezett felhasználását, a magánéletet fenyegető potenciális kockázatok mérséklésére szolgáló biztosítékokat stb. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Hasonlóképpen, a CIA Adatvédelmi és Állampolgári Jogi Hivatalának 2019. január–júniusi jelentései tájékoztatást nyújtanak a Hivatal felügyeleti tevékenységeiről, pl. a 12333. elnöki rendelet szerinti főügyészi iránymutatásoknak való megfelelés felülvizsgálatáról az információk megőrzése és terjesztése tekintetében, iránymutatást adnak a PPD-28 végrehajtásáról, és követelményeket fogalmaznak meg az adatvédelmi incidensek azonosítására és kezelésére, valamint a személyes adatok felhasználásának és kezelésének felülvizsgálatára vonatkozóan (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Ezt a főellenőrt az elnök nevezi ki a Szenátus jóváhagyásával, és csak az elnök mentheti fel beosztásából.

([316]) A főellenőrök biztos hivatali megbízatással rendelkeznek, és csupán az elnök mentheti fel őket, akinek írásban közölni kell a Kongresszussal e felmentés indokait. Ez nem feltétlenül jelenti azt, hogy senki sem utasíthatja őket. Egyes esetekben a minisztérium vezetője megtilthatja a főellenőrnek, hogy ellenőrzést vagy vizsgálatot indítson, végezzen vagy fejezzen be, amennyiben ezt szükségesnek ítéli fontos nemzeti (nemzetbiztonsági) érdekek megóvásához. A Kongresszust azonban tájékoztatni kell e jogkör gyakorlásáról, és ennek alapján az érintett igazgató felelősségre vonható. Lásd pl. A főellenőrről szóló 1978. évi törvény § 8-a (a Védelmi Minisztérium főellenőre); § 8E (az Igazságügyi Minisztérium főellenőre), § 8G (2)(A),(B) (az NSA főellenőre); 50. U.S.C. § 403q (b) (a CIA esetében); a 2010-es költségvetési évre vonatkozó hírszerzési engedélyezési törvény, 405(f) szak., (a hírszerzési szervezet főellenőre).

([317]) A főellenőrről szóló 1978. évi módosított törvény, Pub. L. 117-108, 2022. április 8. Például, amint azt a Kongresszusnak a 2021. április 1. és 2022. március 31. közötti időszakra vonatkozóan benyújtott féléves jelentéseiben kifejtette, az NSA főellenőre értékelte az egyesült államokbeli személyekre vonatkozó, a 12333. elnöki rendelet alapján gyűjtött információk kezelését, a jelfelderítési adatok törlésének folyamatát, az NSA által használt automatizált célkövető eszközt, valamint a FISA 702. szakaszára vonatkozó dokumentációs és lekérdezési szabályoknak való megfelelést, és ezzel összefüggésben számos ajánlást adott ki (lásd: https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, 5–8. o. és https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, 10–13. o.). Lásd még a Hírszerző Közösség főellenőre által az információbiztonsággal és a minősített nemzetbiztonsági információk jogosulatlan közlésével kapcsolatban a közelmúltban végzett ellenőrzéseket és vizsgálatokat (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, 8. és 11. o. és https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, 19–20. o.).

nyilvántartásba, jelentésbe, ellenőrzésbe, felülvizsgálatba, dokumentumba, iratba, ajánlásba vagy egyéb vonatkozó anyagba, ha szükséges bizonyítási cselekményben való közreműködésre kötelező közigazgatási határozat révén, és tanúvallomást vehetnek fel ([318]). A főellenőrök büntetőeljárást kezdeményeznek a feltételezett bűncselekmények eseteinél, és korrekciós intézkedésekre vonatkozó ajánlásokat tesznek az ügynökség vezetőinek ([319]). Bár a főellenőrök jogilag nem kötelező ajánlásokat adhatnak ki, jelentéseiket – többek között a nyomonkövetési intézkedésekről (vagy azok hiányáról) szóló jelentéseiket ([320]) – nyilvánosságra hozzák, és emellett elküldik a Kongresszusnak, amely ezek alapján gyakorolhatja felügyeleti funkcióját (lásd a (168)–(169) preambulum-bekezdést) ([321]).

(166) Harmadrészt a hírszerzési felügyeleti testület (IOB), amely az elnöki hírszerzési tanácsadó testületen (PIAB) belül jött létre, azt felügyeli, hogy az Egyesült Államok hírszerző hatóságai betartják-e az Alkotmányt és az összes alkalmazandó szabályt ([322]). A PIAB az elnök végrehajtó hivatalának tanácsadó szerve, amely az elnök által az Egyesült Államok kormányán kívülről kinevezett 16 tagból áll. Az IOB legfeljebb öt tagból áll, akiket az elnök nevez ki a PIAB tagjai közül. A 12333. elnöki rendelet ([323]) szerint valamennyi hírszerző ügynökség vezetői kötelesek bejelenteni az IOB-nak minden olyan hírszerzési tevékenységet, amelyről okkal feltételezhető, hogy az jogellenes vagy ellentétes lehet valamely elnöki rendelettel vagy elnöki irányelvvel. Annak biztosítása érdekében, hogy az IOB hozzáférjen a feladatai ellátásához szükséges információkhoz, a 13462. elnöki rendelet arra utasítja a nemzeti hírszerzési igazgatót és a hírszerző ügynökségek vezetőit, hogy adjanak meg minden olyan információt és segítséget, amelyet az IOB a feladatai ellátásához a törvény által megengedett mértékben szükségesnek ítél ([324]). Az IOB-nak pedig tájékoztatnia kell az elnököt azokról a hírszerzési tevékenységekről, amelyekről úgy véli, hogy sérthetik az Egyesült Államok jogát (beleértve az elnöki rendeleteket is), és amelyekkel a főügyész, a nemzeti hírszerzés igazgatója vagy egy hírszerző ügynökség vezetője nem foglalkozik megfelelően ([325]). Ezen túlmenően az IOB köteles tájékoztatni a legfőbb ügyészt a büntetőjog esetleges megsértéséről.

(167) Negyedszer, a hírszerző ügynökségek a PCLOB felügyelete alá tartoznak. Alapító okirata szerint a PCLOB a magánélet és a polgári szabadságjogok védelme érdekében hatáskörrel rendelkezik a terrorizmusellenes politikák és azok végrehajtása terén. A tanács a hírszerzési ügynökségek tevékenységeinek felülvizsgálata során hozzáférhet az összes érintett ügynökség nyilvántartásaihoz, ellenőrzéseihez, felülvizsgálataihoz, dokumentumaihoz, irataihoz és ajánlásaihoz – ideértve a minősített adatokat –, meghallgatásokat folytathat és tanúvallomásokat vehet fel ([326]). Jelentéseket kap a különböző minisztériumok/ügynökségek polgári szabadságjogi és adatvédelmi tisztviselőitől ([327]), ajánlásokat ad ki a kormányzatnak és a hírszerző ügynökségeknek, és rendszeresen jelentést tesz a kongresszusi bizottságoknak és az elnöknek ([328]). A testület jelentéseit, beleértve a Kongresszusnak szóló jelentéseket is, a lehető legnagyobb mértékben nyilvánosan hozzáférhetővé kell tenni ([329]). A PCLOB számos felügyeleti és nyomonkövetési jelentést adott ki, többek között a FISA 702. szakasza alapján működtetett programok és ezzel összefüggésben a magánélet védelmének, valamint a PPD-28 és a 12333. elnöki rendelet végrehajtásának elemzését ([330]). A PCLOB

([318]) Lásd a főellenőrről szóló 1978. évi törvény 6. §-át.

([319]) Lásd uo. §§ 4, 6-5.

([320]) A főellenőrök jelentéseihez és ajánlásaihoz nyújtott nyomon követéssel kapcsolatban lásd például az Igazságügyi Minisztérium főellenőrének jelentésére adott választ, amely megállapította, hogy az FBI nem volt kellően átlátható a FISC-vel szemben a 2014 és 2019 közötti kérelmekben, ami az FBI-n belüli megfelelés, felügyelet és elszámoltathatóság javítását célzó reformokhoz vezetett (pl. az FBI igazgatója több mint 40 korrekciós intézkedést rendelt el, köztük 12 kifejezetten a dokumentációval, felügyelettel, iratkarbantartással, képzéssel és ellenőrzésekkel kapcsolatos FISA-folyamatra vonatkozott) (lásd https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance és https://oig.justice.gov/reports/2019/o20012.pdf). Lásd például az FBI főellenőrének az FBI Hivatalának az FBI nemzetbiztonsági tevékenységeire vonatkozó jogszabályoknak, szabályzatoknak és eljárásoknak való megfelelés felügyeletével kapcsolatos szerepei és feladatai tekintetében végzett ellenőrzését, valamint a 2. függeléket, amely tartalmazza az FBI valamennyi ajánlást elfogadó levelét. E tekintetben a 3. függelék áttekintést nyújt a nyomon követésről és azokról az információkról, amelyekre a főellenőrnek szüksége van az FBI-tól annak érdekében, hogy le tudja zárni ajánlásait (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Lásd a főellenőrről szóló 1978. évi törvény 4. §-ának (5) bekezdését és 5. §-át.

([322]) Lásd a 13462. elnöki rendeletet.

([323]) A 12333. elnöki rendelet 1.6. szakaszának (c) pontja.

([324]) A 13462. elnöki rendelet 8. szakaszának (a) pontja.

([325]) A 13462. elnöki rendelet 6. szakaszának (b) pontja.

([326]) 42 U.S.C. § 2000ee (g).

([327]) Lásd: 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Ezek közé tartozik legalább az Igazságügyi Minisztérium, a Védelmi Minisztérium, a Belbiztonsági Minisztérium, a nemzeti hírszerzés igazgatója és a Központi Hírszerző Ügynökség (CIA), valamint a megfelelő lefedettség érdekében a PCLOB által kijelölt bármely egyéb végrehajtó hatalmi szervezeti egység, ügynökség vagy szervezet.

([328]) 42 U.S.C. §2000ee (e).

([329]) 42 U.S.C. § 2000ee (f).

([330]) Elérhető itt: https://www.pclob.gov/Oversight

feladata továbbá a 14086. elnöki rendelet végrehajtásával kapcsolatos konkrét felügyeleti feladatok ellátása, különösen annak felülvizsgálata révén, hogy az ügynökség eljárásai összhangban vannak-e a gazdasági szereplővel (lásd a (126) preambulumbekezdést), valamint a jogorvoslati mechanizmus korrekciós működésének értékelése (lásd a (194) preambulumbekezdést).

(168) Ötödrészt a végrehajtó hatalmon belüli, említett felülvizsgálati mechanizmusok mellett az Egyesült Államok Kongresszusának meghatározott bizottságai (a Képviselőház és a Szenátus, valamint az igazságügyi bizottságok) rendelkeznek felügyeleti feladatkörökkel az Egyesült Államok külföldi hírszerzési tevékenységei tekintetében. E bizottságok tagjai hozzáférnek a minősített adatokhoz, valamint a hírszerzési módszerekhez és programokhoz ([331]). A bizottságok különböző módokon végzik felügyeleti feladataikat, különösen meghallgatások, vizsgálatok, felülvizsgálatok és jelentések révén ([332]).

(169) A kongresszusi bizottságok rendszeres jelentéseket kapnak a hírszerzési tevékenységekről, többek között a főügyésztől, a nemzeti hírszerzés igazgatójától, a hírszerző ügynökségektől és más felügyeleti szervektől (pl. főellenőröktől), lásd a (164)–(165) preambulumbekezdést. Különösen a nemzetbiztonsági törvény értelmében „az elnök gondoskodik arról, hogy a kongresszusi hírszerzési bizottságok teljes körű és aktuális tájékoztatást kapjanak az Egyesült Államok hírszerzési tevékenységeiről, ideértve az ezen alfejezet által előírt bármely jelentős, előreláthatóhírszerzési tevékenységet" ([333]). Ezenkívül „az elnök biztosítja, hogy minden jogellenes hírszerzési tevékenységről, valamint az ilyen jogellenes tevékenységgel kapcsolatos, bármely megtett vagy tervezett korrekciós intézkedésről haladéktalanul beszámoljanak a kongresszusi hírszerzési bizottságoknak" ([334]).

(170) Emellett az egyes alapszabályokból további jelentéstételi követelmények következnek. A FISA nevezetesen előírja, hogy a legfőbb ügyész „maradéktalanul tájékoztassa" a szenátus és a képviselőház hírszerzési és igazságügyi bizottságait a FISA bizonyos szakaszain alapuló kormányzati tevékenységekről ([335]). Kötelezi továbbá a kormányt, hogy juttassa el a kongresszusi bizottságokhoz a FISC, illetve a FISCR valamennyi olyan határozatának, végzésének vagy véleményének másolatát, amely kiterjed a FISA-rendelkezések jelentős „kiegészítésére vagy értelmezésére". Ami a FISA 702. szakasza alapján történő megfigyelést illeti, a parlamenti felügyeletet a Hírszerzési és Igazságügyi Bizottságoknak szóló, törvényileg előírt jelentések, valamint gyakori tájékoztatók és meghallgatások útján gyakorolják. Ezek közé tartozik a legfőbb ügyésznek a FISA 702. szakaszának alkalmazását ismertető féléves jelentése, amelyet igazoló dokumentumok – többek között az Igazságügyi Minisztérium és az ODNI megfelelőségi jelentései és a meg nem feleléssel kapcsolatos bármely esemény leírása – kísérnek ([336]), valamint a legfőbb ügyész és a DNI külön féléves jelentése, amely dokumentálja a célzottá tételre és az adatminimalizációra vonatkozó eljárások betartását ([337]).

([331]) 50 U.S.C. § 3091.

([332]) A bizottságok például tematikus meghallgatásokat szerveznek (lásd például a Képviselőház igazságügyi bizottságának nemrégiben tartott meghallgatását a „digitális dragnetekről", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 és a Képviselőház hírszerzési bizottságának meghallgatását a mesterséges intelligencia Hírszerző Közösség általi használatáról, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), valamint rendszeres felügyeleti meghallgatásokat, pl. az FBI és az Igazságügyi Minisztérium tekintetében, lásd https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 és https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. A vizsgálat egyik példájaként lásd a Szenátus hírszerzési bizottságának a 2016-os egyesült államokbeli választásokba való orosz beavatkozással kapcsolatos vizsgálatát, lásd: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. A jelentéstételt illetően lásd például a Szenátus hírszerzési bizottságának 2019. január 4. és 2021. január 3. közötti időszakra vonatkozó, a Szenátusnak címzett jelentésében a bizottság (felügyeleti) tevékenységeinek áttekintését, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4

([333]) Lásd: 50 U.S.C. § 3091(a)(1). Ez a rendelkezés általános követelményeket tartalmaz a nemzetbiztonság területére vonatkozó kongresszusi felügyelet tekintetében.

([334]) Lásd: 50 U.S.C. §3091(b).

([335]) Lásd: 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

([336]) Lásd: 50 U.S.C. § 1881f.

([337]) Lásd: 50 U.S.C. § 1881a(l)(1).

(171) Ezenkívül a FISA előírja az Egyesült Államok kormányának, hogy évente közölje a Kongresszussal (és a nyilvánossággal) a kért és megkapott FISA-végzések és -irányelvek számát, valamint többek között a megfigyelt amerikai és nem amerikai célszemélyek becsült számát ([338]). A törvény emellett további nyilvános jelentéstételt ír elő az amerikai és nem amerikai személyek tekintetében kiadott nemzetbiztonsági levelek (NSL) számáról (ugyanakkor lehetővé téve a FISA-végzések és tanúsítványok, valamint NSL-kérelmek címzettjeinek, hogy bizonyos feltételek mellett átláthatósági jelentéseket bocsássanak ki) ([339]).

(172) Általánosabban fogalmazva, az Egyesült Államok Hírszerző Közössége különböző erőfeszítéseket tesz annak érdekében, hogy biztosítsa a (külföldi) hírszerzési tevékenységeinek átláthatóságát. Például 2015-ben az ODNI elfogadta a hírszerzés átláthatóságának elveit és az átláthatóságra vonatkozó végrehajtási tervet, és utasította az egyes hírszerző ügynökségeket, hogy jelöljenek ki egy hírszerzési átláthatósági tisztviselőt az átláthatóság előmozdítása és az átláthatósági kezdeményezések irányítása érdekében ([340]). Ezen erőfeszítések részeként a Hírszerző Közösség nyilvánosságra hozta és rendszeresen nyilvánosságra hozza a FISA 702. szakasza és a 12333. elnöki rendelet szerinti szabályzatok, eljárások, felügyeleti jelentések, a FISC-határozatok és egyéb anyagok titkosított részeit, többek között az ODNI által kezelt „IC on the Record" elnevezésű weboldalon ([341]).

(173) Végezetül a személyes adatoknak a FISA 702. szakasza szerinti gyűjtése – a (162)–(168) preambulumbekezdésben említett felügyeleti szervek általi felügyelet mellett – a FISC felügyelete alá tartozik ([342]). A FISC eljárási szabályzatának 13. szabálya értelmében az egyesült államokbeli hírszerző ügynökségek megfelelésért felelős tisztviselőinek jelenteniük kell a FISA 702. szakasza szerinti célkiválasztással, minimalizálással és lekérdezéssel kapcsolatos eljárások megsértéseit az Igazságügyi Minisztériumnak és az ODNI-nak, amelyek ezeket jelentik a FISC-nek. Ezen túlmenően az Igazságügyi Minisztérium és az ODNI féléves közös felügyeleti értékelő jelentéseket nyújt be a FISC-nek, amelyek meghatározzák a megfeleléssel kapcsolatos tendenciákat; statisztikai adatokat bocsátanak rendelkezésre; ismertetik a megfelelési események kategóriáit; részletesen ismertetik azokat az okokat, amelyek bizonyos megfelelési incidenseket céloztak, és vázolják azokat az intézkedéseket, amelyeket a hírszerző ügynökségek az újbóli előfordulás elkerülése érdekében hoztak ([343]).

(174) Szükség esetén (pl. ha a célkiválasztási eljárások megsértését állapítják meg) a Bíróság felszólíthatja az érintett hírszerző ügynökséget, hogy hozzon korrekciós intézkedéseket ([344]). A szóban forgó jogorvoslatok az egyedi intézkedésektől a strukturális intézkedésekig terjedhetnek, például az adatgyűjtés befejezésétől és a jogellenesen szerzett adatok törlésétől az adatgyűjtési gyakorlat megváltoztatásáig, többek között a személyzetnek nyújtott iránymutatás és képzés tekintetében ([345]). Ezen túlmenően a 702. szakasz szerinti tanúsítványok éves felülvizsgálata

([338]) 50 U.S.C. § 1873(b). Ezenfelül a 402. szakasz szerint „a nemzeti hírszerzési igazgató a legfőbb ügyésszel konzultálva elvégzi a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság, illetve a Külföldi Hírszerzést Felügyelő Fellebbviteli Bíróság által kibocsátott egyes határozatok, végzések vagy vélemények minősítésének feloldására irányuló felülvizsgálatot (a 601(e) szakasz meghatározása szerint), amely kiterjed bármely jogi rendelkezés jelentős kiegészítésére vagy értelmezésére, többek között az" egyedi kiválasztási kritérium „fogalmának bármely új szempontjára vagy jelentős kiegészítésére, illetve értelmezésére, valamint a felülvizsgálatnak megfelelően, a megvalósítható legnagyobb mértékben nyilvánosságra hozza az ilyen határozatot, végzést vagy véleményt".

([339]) 50 U.S.C. §§ 1873(b)(7) és 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic

([341]) Lásd az „IC on the Record" weboldalt, amely elérhető itt: https://icontherecord.tumblr.com/

([342]) A FISC korábban arra a következtetésre jutott, hogy „a Bíróság számára nyilvánvaló, hogy a végrehajtó ügynökségek, valamint az [ODNI] és az [Igazságügyi Minisztérium nemzetbiztonsági részlege] jelentős erőforrásokat fordítanak a 702. szakasz szerinti megfelelési és felügyeleti feladataikra. Általános szabályként a meg nem felelés eseteit azonnal azonosítják, és meghozzák a megfelelő korrekciós intézkedéseket, amelyek magukban foglalják a nem megfelelően megszerzett vagy az alkalmazandó eljárások szerinti megsemmisítési követelmények hatálya alá tartozó információk eltávolítását is". A FISA bírósága, Memorandum Opinion and Order [szerkesztett felirat] (2014), elérhető a következő internetcímen: https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf

([343]) Lásd pl. a DOJ/ODNI FISA 702. szakasz szerinti megfelelőségi jelentését a FISC számára a 2018. június és 2018. november közötti időszakra vonatkozóan, 21–65.

([344]) 50 U.S.C. § 1803(h). Lásd még a PCLOB 702. szakaszról szóló jelentését, 76. o. Ezenkívül lásd a FISC 2011. október 3-i véleményét és határozatát, mint a hiányossági végzés példáját, amelyben a kormányt arra kötelezték, hogy 30 napon belül orvosolja a feltárt hiányosságokat. Elérhető itt: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf–11. o. Lásd még a FISC 2018. október 18-i véleményét, amely a https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf címen érhető el, és amelyet a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróság megerősített 2019. július 12-i véleményében, amely elérhető itt: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, amelyben a FISC többek között arra kötelezte a kormányt, hogy tegyen eleget bizonyos, a FISC-re vonatkozó értesítési, dokumentációs és jelentéstételi követelményeknek.

([345]) Lásd pl. FISC véleményét és határozatát, 76 (2019. december 6.) (nyilvános közzététel engedélyezése 2020. szeptember 4-én), amelyben a FISC arra utasította a kormányt, hogy 2020. február 28-ig nyújtson be írásbeli jelentést azokról a lépésekről, amelyeket a kormány a megfelelés érdekében visszahívott FISA 702. szakasz szerinti információk azonosítására és törlésére irányuló folyamatok javítása érdekében tett, valamint egyéb kérdésekről. Lásd továbbá a VII. mellékletet.

során a FISC figyelembe veszi a meg nem felelési eseteket annak megállapítása érdekében, hogy a benyújtott tanúsítványok megfelelnek-e a FISA-követelményeknek. Hasonlóképpen, ha a FISC megállapítja, hogy a kormány tanúsítványai – többek között bizonyos megfelelési incidensek miatt – nem voltak elégségesek, úgynevezett „hiányossági végzést" adhat ki, amely előírja a kormány számára, hogy 30 napon belül orvosolja a jogsértést, vagy arra kötelezi a kormányt, hogy szüntesse meg vagy ne kezdje meg a 702. szakasz szerinti tanúsítás végrehajtását. Végezetül a FISC értékeli a megfelelési kérdésekben megfigyelt tendenciákat, és a megfelelési tendenciák kezelése érdekében szükségessé teheti az eljárások módosítását vagy további felügyeletet és jelentéstételt ([346]).

3.2.3. ***Jogorvoslat***

(175) Amint azt ez a szakasz részletesebben kifejti, az Egyesült Államokban számos lehetőség áll az uniós érintettek rendelkezésére, hogy keresetet nyújtsanak be egy kötelező erejű hatáskörrel rendelkező független és pártatlan bírósághoz. Ezek együttesen lehetővé teszik az egyének számára, hogy hozzáférjenek személyes adataikhoz, felülvizsgálják az adataikhoz való kormányzati hozzáférés jogszerűségét, és amennyiben jogsértést állapítanak meg, az ilyen jogsértést orvosolják, többek között személyes adataik helyesbítése vagy törlése révén.

(176) Először is külön jogorvoslati mechanizmust hoznak létre a 14086. elnöki rendelet alapján, amelyet az adatvédelmi felülvizsgálati bíróságot létrehozó főügyészi rendelet egészít ki, az egyénektől érkező, az Egyesült Államok jelfelderítési tevékenységeivel kapcsolatos panaszok kezelésére és rendezésére. Az EU-ban bármely egyénnek jogában áll panaszt benyújtani a jogorvoslati mechanizmushoz a jelfelderítési tevékenységekre vonatkozó egyesült államokbeli jogszabályok (pl. a 14086. elnöki rendelet, a FISA 702. szakasza, a 12333. elnöki rendelet) állítólagos megsértése miatt, amely hátrányosan érinti a magánélethez és a polgári szabadságjogokhoz fűződő érdekeit ([347]). Ez a jogorvoslati mechanizmus az Egyesült Államok legfőbb ügyésze által „minősített államként" kijelölt országokból származó magánszemélyek vagy regionális gazdasági integrációs szervezetek számára áll rendelkezésre ([348]). 2023. június 30-án az Európai Uniót és az Európai Szabadkereskedelmi Társulás három országát, amelyek együtt alkotják az Európai Gazdasági Térséget, a legfőbb ügyész a 14086 elnöki rendelet 3. szakaszának f) pontja alapján „minősített államként" jelölte ki ([349]). Ez a kijelölés nem érinti az Európai Unióról szóló szerződés 4. cikkének (2) bekezdését.

(177) Annak az uniós érintettnek, aki ilyen panaszt kíván benyújtani, azt a személyes adatok kezelésének hatóságok általi felügyeletéért felelős uniós tagállam felügyeleti hatóságához kell benyújtania ([350]). Ez biztosítja a jogorvoslati mechanizmushoz való könnyű hozzáférést azáltal, hogy lehetővé teszi az egyének számára, hogy olyan hatósághoz forduljanak, amely „lakóhelyhez közeli", és amellyel saját nyelvükön kommunikálhatnak. A (178) preambulumbekezdésben említett panaszbenyújtási követelmények ellenőrzését követően az illetékes adatvédelmi hatóság az Európai Adatvédelmi Testület titkárságán keresztül továbbítja a panaszt a jogorvoslati mechanizmushoz.

(178) A jogorvoslati mechanizmushoz való panaszbenyújtásra alacsony elfogadhatósági követelmények vonatkoznak, mivel az egyéneknek nem kell bizonyítaniuk, hogy adataik valóban amerikai jelfelderítési tevékenységek tárgyát képezték ([351]). Ugyanakkor a felülvizsgálat elvégzéséhez szükséges jogorvoslati mechanizmus kiindulópontjának biztosítása érdekében meg kell adni bizonyos alapvető információkat, például azokról a személyes adatokról, amelyekről észszerűen feltételezhető, hogy azokat továbbították az Egyesült Államoknak, valamint azokról az eszközökről, amelyekkel feltételezhetően továbbították azokat; azon egyesült államokbeli kormányzati szervek azonosításáról, amelyekről feltételezhető, hogy részt vesznek az állítólagos jogsértésben (amennyiben ismertek); az Egyesült Államok jogának megsértésére vonatkozó állítás alapjáról (bár ez szintén nem követeli meg annak bizonyítását, hogy a személyes adatokat az Egyesült Államok hírszerző ügynökségei ténylegesen gyűjtötték), valamint a kereset jellegéről.

([346]) Lásd a VII. mellékletet.

([347]) Lásd: 14086. elnöki rendelet, 4. szakasz (k) pont (iv) alpont, amely előírja, hogy a jogorvoslati mechanizmussal szembeni panaszt a saját nevében (azaz kormányzati, nem kormányzati vagy kormányközi szervezetet nem képviselve) eljáró panaszosnak kell benyújtania. A „hátrányosan érintett" fogalma nem követeli meg, hogy a panaszos egy bizonyos küszöbértéket teljesítsen ahhoz, hogy igénybe vehesse a jogorvoslati mechanizmust (lásd e tekintetben a (178) preambulumbekezdést). Ehelyett egyértelművé teszi, hogy az ODNI CLPO és a DPRC hatáskörrel rendelkezik arra, hogy orvosolja az Egyesült Államok jelfelderítési tevékenységekre vonatkozó jogszabályainak megsértését, amely hátrányosan érinti a panaszos egyéni magánélethez és polgári szabadságjogokhoz fűződő érdekeit. Ezzel szemben az alkalmazandó amerikai jog szerinti azon követelmények megsértése, amelyek célja nem az egyének védelme (pl. költségvetési követelmények), kívül esne az ODNI CLPO és a DPRC joghatóságán.

([348]) 14086. elnöki rendelet 3. szakaszának (f) pontja.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) 14086. elnöki rendelet 4. szakasza (d) pontjának (v) alpontja.

([351]) Lásd: 14086. elnöki rendelet 4. szakasza (k) pontjának (i)–(iv) alpontja.

(179) Az e jogorvoslati mechanizmussal szembeni panaszok első kivizsgálását az ODNI CLPO végzi, amelynek meglévő jogszabályi szerepét és hatáskörét kiterjesztették a 14086. elnöki rendelet alapján hozott konkrét intézkedésekre ([352]). A Hírszerző Közösségen belül a CLPO feladata többek között annak biztosítása, hogy a polgári szabadságjogok és a magánélet védelme megfelelően beépüljön az ODNI és a hírszerző ügynökségek szabályzataiba és eljárásaiba; annak felügyelete, hogy az ODNI megfelel-e az alkalmazandó polgári szabadságjogoknak és adatvédelmi követelményeknek; valamint adatvédelmi hatásvizsgálatok elvégzése ([353]). Az ODNI CLPO-t csak a nemzeti hírszerzés igazgatója mentheti fel megfelelő indokkal, azaz kötelességszegés, hivatali visszaélés, biztonság megsértése, hivatali mulasztás vagy cselekvőképtelenség esetén ([354]).

(180) A felülvizsgálat során az ODNI CLPO az értékelés céljából hozzáfér az információkhoz, és igénybe veheti a különböző hírszerző ügynökségek adatvédelmi és polgári jogi tisztviselőinek kötelező segítségét ([355]). A hírszerző ügynökségek számára tilos az ODNI CLPO által végzett felülvizsgálatok akadályozása vagy nem megfelelő befolyásolása. Ez magában foglalja a nemzeti hírszerzés igazgatóját is, aki nem avatkozhat bele a felülvizsgálatba ([356]). A panasz felülvizsgálata során az ODNI CLPO-nak „pártatlanul" kell alkalmaznia a jogot, figyelembe véve mind a jelfelderítési tevékenységekhez fűződő nemzetbiztonsági érdekeket, mind a magánélet védelmét ([357]).

(181) A felülvizsgálata részeként az ODNI CLPO megállapítja, hogy sor került-e az alkalmazandó egyesült államokbeli jog megsértésére, és ha igen, dönt a megfelelő kárenyhítésről ([358]). Ez utóbbi olyan intézkedésekre utal, amelyek teljes mértékben orvosolják az azonosított jogsértést, mint például a jogellenes adatszerzés megszüntetése, a jogellenesen gyűjtött adatok törlése, az egyébként jogszerűen gyűjtött adatok helytelen lekérdezése eredményeinek törlése, a jogszerűen gyűjtött adatokhoz való hozzáférés megfelelő képesítéssel rendelkező személyzet számára történő korlátozása, vagy a jogszerű engedély nélkül megszerzett vagy jogellenesen terjesztett adatokat tartalmazó hírszerzési jelentések visszahívása ([359]). Az ODNI CLPO egyedi panaszokról (többek között a kárenyhítésről) szóló határozatai kötelező érvényűek az érintett hírszerző ügynökségekre nézve ([360]).

(182) Az ODNI CLPO-nak nyilvántartást kell vezetnie a felülvizsgálatáról, és titkosított határozatot kell készítenie, amely ismerteti ténybeli megállapításainak alapját, annak megállapítását, hogy az érintett jogsértés megtörtént-e, valamint a megfelelő kárenyhítés meghatározását ([361]). Amennyiben az ODNI CLPO felülvizsgálata a FISC felügyelete alá tartozó bármely hatóság általi szabálysértést tárja fel, a CLPO titkosított jelentést nyújt be a nemzetbiztonsági főügyész-helyettesnek is, aki köteles bejelenteni a meg nem felelést a FISC-nek, amely további végrehajtási intézkedéseket tehet (a (173)–(174) preambulumbekezdésben leírt eljárásnak megfelelően) ([362]).

(183) A felülvizsgálat befejezését követően az ODNI CLPO a nemzeti hatóságon keresztül tájékoztatja a panaszost, hogy „a felülvizsgálat vagy nem tárta fel az érintett jogsértéseket, vagy az ODNI CLPO megfelelő kárenyhítést előíró határozatot hozott" ([363]). Ez lehetővé teszi a nemzetbiztonság védelme érdekében végzett tevékenységek titkosságának védelmét, ugyanakkor olyan határozatot bocsát az egyének rendelkezésére, amely megerősíti, hogy panaszukat megfelelően kivizsgálták és elbírálták. Ezt a határozatot az egyén is megtámadhatja. E célból tájékoztatást kap arról a lehetőségről, hogy a DPRC-nél fellebbezhetnek a CLPO megállapításainak felülvizsgálata iránt (lásd a (184) és azt követő preambulumbekezdéseket), valamint arról, hogy amennyiben a Bírósághoz fordulna, a panaszos érdekének védelme érdekében különleges főtanácsnokot választanak ki ([364]).

([352]) 14086. elnöki rendelet 3. szakasza (c) pontjának (iv) alpontja. Lásd még: az 1947. évi nemzetbiztonsági törvény, 50 U.S.C. §403–3d, 103D. szakasz a CLPO-nak az ODNI-n belüli szerepéről.
([353]) 50 U.S.C § 3029 (b).
([354]) 14086. elnöki rendelet 3. szakasza (c) pontjának (iv) alpontja.
([355]) 14086. elnöki rendelet 3. szakasza (c) pontjának (iii) alpontja.
([356]) 14086. elnöki rendelet 3. szakasza (c) pontjának (iv) alpontja.
([357]) 14086. elnöki rendelet 3. szakasza (c) pontja (i) alpontja (B) szakaszának (i) és (iii) alszakaszai.
([358]) 14086. elnöki rendelet 3. szakasza (c) pontjának (i) alpontja.
([359]) 14086. elnöki rendelet 4. szakaszának (a) pontja.
([360]) 14086. elnöki rendelet 3. szakasza (c) pontjának (d) alpontja.
([361]) 14086. elnöki rendelet 3. szakasza (c) pontja (i) alpontjának (F)–(G) szakasza.
([362]) Lásd még: 14086. elnöki rendelet 3. szakasza (c) pontja (i) alpontjának (D) szakasza.
([363]) 14086. elnöki rendelet 3. szakasza (c) pontja (i) alpontja (E) szakaszának (1) alszakasza.
([364]) 14086. elnöki rendelet 3. szakasza (c) pontjának (i) alpontja (E) szakaszának (2)–(3) alszakasza.

(184) Bármely panaszos, valamint a Hírszerző Közösség minden egyes eleme kérheti az ODNI CLPO határozatának felülvizsgálatát az adatvédelmi fellebbviteli bíróságon (DPRC). Az ilyen felülvizsgálati kérelmeket az ODNI CLPO azon értesítésének kézhezvételétől számított 60 napon belül kell benyújtani, amely szerint a felülvizsgálat teljes, és tartalmaznia kell az egyén által a DPRC-nek átadni kívánt információkat (pl. jogkérdésekre vagy az ügy tényállására való jogalkalmazásra vonatkozó érveket) ([365]). Az uniós érintettek ismét benyújthatják kérelmüket az illetékes adatvédelmi hatósághoz (lásd a (177) preambulumbekezdést).

(185) A DPRC a legfőbb ügyész által a 14086. elnöki rendelet alapján létrehozott független bíróság ([366]). Legalább hat bíróból áll, akiket a legfőbb ügyész nevez ki a PCLOB-val, a kereskedelmi miniszterrel és a nemzeti hírszerzés igazgatójával konzultálva, négyéves megújítható időtartamra ([367]). A bíráknak a legfőbb ügyész általi kinevezése a végrehajtó hatalmi ág által a szövetségi bírói kar jelöltjeinek értékelése során alkalmazott kritériumokon alapul, figyelembe véve a korábbi bírói tapasztalatokat ([368]). Emellett a bíráknak jogi szakembereknek (azaz az ügyvédi kamara aktív tagjainak, akik megfelelő engedéllyel rendelkeznek a jog gyakorlására) kell lenniük, és megfelelő tapasztalattal kell rendelkezniük a magánélet védelmére és a nemzetbiztonságra vonatkozó jog terén. A legfőbb ügyésznek törekednie kell annak biztosítására, hogy adott időpontban a bírák legalább fele előzetes bírói tapasztalattal rendelkezzen, és valamennyi bírónak rendelkeznie kell a minősített nemzetbiztonsági információkhoz való hozzáféréshez szükséges biztonsági tanúsítvánnyal ([369]).

(186) Csak azok az egyének nevezhetők ki a DPRC-be, akik megfelelnek a (185) preambulumbekezdésben említett képesítéseknek, és kinevezésük időpontjában vagy az azt megelőző két évben nem a végrehajtó hatalmi ág alkalmazottai voltak. Hasonlóképpen, a DPRC-ben betöltött hivatali idejük alatt a bírák (a DPRC bíráin kívül) nem tölthetnek be hivatalos feladatokat vagy munkát az Egyesült Államok kormányán belül ([370]).

(187) Az ítélethozatali folyamat függetlensége számos garancia révén valósul meg. Különösen a végrehajtó ág (a legfőbb ügyész és a hírszerző ügynökségek) nem avatkozhat be a DPRC felülvizsgálatába, és nem befolyásolhatja azt nem megfelelően ([371]). Magának a DPRC-nek kell pártatlanul döntenie az ügyekről ([372]), és saját (többséggel elfogadott) eljárási szabályzatával összhangban kell eljárnia. Ezen túlmenően a DPRC bíráit csak a legfőbb ügyész mentheti fel és csak megfelelő indokkal (pl. kötelességszegés, hivatali visszaélés, biztonság megsértése, hivatali mulasztás vagy cselekvőképtelenség miatt), miután kellően figyelembe vette a bírákra alkalmazandó, a bírósági eljárásra és a bírósági fegyelmi eljárásra vonatkozó szabályokat ([373]).

([365]) A főügyészi rendelet 201.6(a)–(b) szakasza.

([366]) A 3. szakasz (d) pontjának (i) alpontja és a főügyészi rendelet. Az Egyesült Államok Legfelsőbb Bírósága elismerte annak lehetőségét, hogy a főügyész döntéshozatali jogkörrel rendelkező független szerveket hozzon létre, beleértve az egyedi ügyek elbírálását, lásd különösen az Egyesült Államok ex rel. Accardi kontra Shaughnessy, ügyben (347 U.S. 260, 1954) és az Egyesült Államok kontra Nixon ügyben (418 U.S. 683, 695, 1974). A 14086. elnöki rendelet különböző követelményeinek – például a DPRC bíráinak kinevezésére és felmentésére vonatkozó kritériumoknak és eljárásoknak – való megfelelés nevezetesen az Igazságügyi Minisztérium főellenőrének felügyelete alá tartozik (lásd még a (109) preambulumbekezdést a főellenőrök törvényes hatásköréről).

([367]) 14086. elnöki rendelet, 3. szakasza (d) pontja (i) alpontjának (A) szakasza, valamint a főügyészi rendelet 201.3(a) szakasza.

([368]) A főügyészi rendelet 201.3(b) szakasza.

([369]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (B) szakasza.

([370]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (A) szakasza, valamint a főügyészi rendelet 201.3(a) és (c) szakasza. A DPRC-be kinevezett személyek részt vehetnek bíróságon kívüli tevékenységekben, beleértve az üzleti, pénzügyi, nonprofit adománygyűjtési és vagyonkezelői tevékenységeket, valamint a jogi gyakorlatot, amennyiben az ilyen tevékenységek nem akadályozzák feladataik pártatlan ellátását vagy a DPRC hatékonyságát vagy függetlenségét (a főügyészi rendelet 201.7. szakaszának (c) pontja).

([371]) 14086. elnöki rendelet 3. szakasza (d) pontjának (iii)–(iv) alpontja, valamint a főügyészi rendelet 201.7(d) szakasza.

([372]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (D) szakasza, valamint a főügyészi rendelet 201.9. szakasza.

([373]) 14086. elnöki rendelet 3. szakasza (d) pontjának (iv) alpontja, valamint a főügyészi rendelet 201.7(d) szakasza. Lásd még: Bumap kontra Egyesült Államok, 252 U.S. 512, 515 (1920), amely megerősítette az Egyesült Államok jogában régóta fennálló elvet, miszerint a kiutasítási hatáskör a kinevezési jogkörrel áll összefüggésben (amint arra az Igazságügyi Minisztérium jogi tanácsadói hivatala is emlékeztetett a „The Constitutional Separation of Powers Between the President and Congress" c. dokumentumban, 20 Op. O.L.C. 124, 166 (1996)).

(188) A DPRC-hez benyújtott kérelmeket három bíróból – köztük egy elnökből álló bíróból – álló tanácsok vizsgálják felül, akiknek az egyesült államokbeli bírák magatartási kódexével összhangban kell eljárniuk ([374]). Minden ítélkező testület munkáját egy különleges főtanácsnok ([375]) segíti, aki hozzáféréssel rendelkezik az üggyel kapcsolatos valamennyi információhoz, beleértve a minősített információkat is ([376]). A különleges főtanácsnok feladata annak biztosítása, hogy a panaszos érdekei képviselve legyenek, és hogy a DPRC testülete megfelelő tájékoztatást kapjon minden releváns jogi és ténybeli kérdésről ([377]). Annak érdekében, hogy megalapozza az álláspontját egy magánszemély által a DPRC-hez benyújtott felülvizsgálati kérelemmel kapcsolatban, a különleges főtanácsnok írásbeli kérdések útján tájékoztatást kérhet a panaszostól ([378]).

(189) A DPRC felülvizsgálja az ODNI CLPO által tett megállapításokat (mind azt, hogy sor került-e az alkalmazandó egyesült államokbeli jog megsértésére, másrészt a megfelelő kárenyhítést), legalább az ODNI CLPO által végzett vizsgálat eredményei alapján, valamint a panaszos, a különleges főtanácsnok vagy egy hírszerző ügynökség által szolgáltatott információkat és beadványokat ([379]). A DPRC tanács hozzáfér minden olyan információhoz, amely a felülvizsgálat elvégzéséhez szükséges, és amelyet az ODNI CLPO-n keresztül szerezhet be (a tanács például felkérheti a CLPO-t, hogy a nyilvántartását egészítsék ki további információkkal vagy ténymegállapításokkal, ha ez a felülvizsgálat elvégzéséhez szükséges) ([380]).

(190) A felülvizsgálat lezárásakor a DPRC 1. dönthet úgy, hogy nincs arra utaló bizonyíték, hogy a panaszos személyes adatait érintő jelfelderítési tevékenységekre került sor, 2. határozhat úgy, hogy az ODNI CLPO megállapításai jogilag helyesek voltak, és azokat érdemi bizonyítékokkal támasztották alá, vagy 3. ha a DPRC nem ért egyet az ODNI CLPO megállapításával (függetlenül attól, hogy sor került-e az alkalmazandó amerikai jog megsértésére vagy a megfelelő kárenyhítésre), kibocsáthatja saját megállapításait ([381]).

([374]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (B) szakasza, valamint a főügyészi rendelet 201.7(a)–(c) szakasza. Az Igazságügyi Minisztérium adatvédelmi és polgári szabadságjogi hivatala (OPCL) – amely a DPRC és a különleges főtanácsnokok adminisztratív támogatásáért felelős (lásd a főügyészi rendelet 201.5. szakaszát) – rotációs alapon kiválaszt egy háromfős testületet, amelynek célja annak biztosítása, hogy minden ítélkező testületben legalább egy olyan bíró legyen, aki rendelkezik bírói tapasztalattal (ha az ítélkező testület egyik bírája sem rendelkezik ilyen tapasztalattal, az elnöklő bíró az OPCL által elsőként kiválasztott bíró).

([375]) A főügyészi rendelet 201.4. szakasza. A legfőbb ügyész a kereskedelmi miniszterrel, a nemzeti hírszerzési igazgatóval és a PCLOB-val konzultálva legalább két különleges főtanácsnokot nevez ki kétszer megújítható időszakra. A különleges főtanácsnokoknak megfelelő tapasztalattal kell rendelkezniük a magánélet védelme és a nemzetbiztonsági jog területén, tapasztalt jogászoknak kell lenniük, az ügyvédi kamara aktív tagjainak kell lenniük, és megfelelő engedéllyel kell rendelkezniük a jog gyakorlására. Ezenkívül az első kinevezésük időpontját megelőző két évben nem lehettek a végrehajtói ág alkalmazottai. Az elnöklő bíró a kérelem minden felülvizsgálatához különleges főtanácsnokot választ ki a tanács támogatására, lásd a főügyészi rendelet 201.8. szakaszának (a) pontját.

([376]) A főügyészi rendelet 201.8(c) és 201.11. szakasza.

([377]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (C) szakasza, valamint a főügyészi rendelet 201.8(e) szakasza. A különleges főtanácsnok nem a panaszos képviselőjeként jár el, és nem áll ügyvéd–ügyfél viszonyban a panaszossal.

([378]) Lásd a főügyészi rendelet 201.8. szakaszának (d) és (e) pontját. Ezeket a kérdéseket először az OPCL vizsgálja felül a Hírszerző Közösség érintett elemével konzultálva azzal a céllal, hogy azonosítsa és kizárja a minősített, privilegizált vagy védett információkat, mielőtt továbbítja azokat a panaszosnak. A különleges főtanácsnok által az ilyen kérdésekre adott válaszban kapott további információk megtalálhatók a különleges főtanácsnok által a DPRC-nek benyújtott beadványokban.

([379]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (D) szakasza.

([380]) 14086. elnöki rendelet 3. szakasza (d) pontjának (iii) alpontja, valamint a főügyészi rendelet 201.9(b) szakasza.

([381]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (E) szakasza, valamint a főügyészi rendelet 201.9(c)–(e) szakasza. A „megfelelő kárenyhítésnek” a 14086. elnöki rendelet 4. szakaszának a) pontjában foglalt fogalommeghatározása szerint a DPRC-nek figyelembe kell vennie „az azonosított típusú jogsértés szokásos kezelési módjait”, amikor a jogsértés teljes körű kezelését célzó korrekciós intézkedésről határoz, azaz a DPRC egyéb tényezők mellett mérlegeli, hogy a múltban hogyan orvosolták a hasonló megfelelési problémákat annak biztosítása érdekében, hogy a jogorvoslat hatékony és megfelelő legyen.

(191) A DPRC minden esetben többségi szavazással írásbeli határozatot fogad el. Amennyiben a felülvizsgálat a hatályos szabályok megsértését tárja fel, a határozat meghatározza a megfelelő kárenyhítést, mint például a jogellenes adatszerzés megszüntetése, a jogellenesen gyűjtött adatok törlése, az egyébként jogszerűen gyűjtött adatok helytelen lekérdezése eredményeinek törlése, a jogszerűen gyűjtött adatokhoz való hozzáférés megfelelő képesítéssel rendelkező személyzet számára történő korlátozása, vagy a jogszerű engedély nélkül megszerzett vagy jogellenesen terjesztett adatokat tartalmazó hírszerzési jelentések visszahívása ([382]). A DPRC határozata kötelező és végleges érvényű az elé terjesztett panasz tekintetében ([383]). Ezenfelül amennyiben a felülvizsgálat a FISC felügyelete alá tartozó bármely hatóság általi szabálysértést tárja fel, a CLPO titkosított jelentést nyújt be a nemzetbiztonsági főügyész-helyettesnek is, aki köteles bejelenteni a meg nem felelést a FISC-nek, amely további végrehajtási intézkedéseket tehet (a (173)–(174) preambulumbekezdésben leírt eljárásnak megfelelően) ([384]).

(192) A DPRC-tanács minden határozatát továbbítják az ODNI CLPO-nak ([385]). Azokban az esetekben, amikor a DPRC felülvizsgálatát a panaszos kérelme indította el, a panaszost a nemzeti hatóságon keresztül értesítik arról, hogy a DPRC befejezte a felülvizsgálatot, és hogy „a felülvizsgálat vagy nem tárt fel érintett jogsértéseket, vagy a DPRC megfelelő kárenyhítést előíró határozatot hozott" ([386]). Az Igazságügyi Minisztérium adatvédelmi és polgári szabadságjogi hivatala nyilvántartást vezet a DPRC által felülvizsgált valamennyi információról és a meghozott határozatokról, amelyeket vizsgálat céljából a DPRC jövőbeli tanácsai számára nem kötelező erejű precedensként bocsátanak rendelkezésre ([387]).

(193) A Kereskedelmi Minisztériumnak nyilvántartást kell vezetnie minden olyan panaszosról, aki panaszt nyújtott be ([388]). Az átláthatóság fokozása érdekében a Kereskedelmi Minisztériumnak legalább ötévente fel kell vennie a kapcsolatot az érintett hírszerző ügynökségekkel annak ellenőrzése érdekében, hogy a DPRC által végzett felülvizsgálattal kapcsolatos információk minősítését megszüntették-e ([389]). Ebben az esetben az egyént értesítik arról, hogy az ilyen információ az alkalmazandó jog alapján rendelkezésre állhat (azaz az információszabadságról szóló törvény alapján kérelmezheti a hozzáférést, lásd a (199) preambulumbekezdést).

(194) Végezetül e jogorvoslati mechanizmus megfelelő működését rendszeres és független értékelésnek vetik alá. Konkrétabban, a 14086. elnöki rendelet szerint a jogorvoslati mechanizmus működését a PCLOB, egy független szerv évente felülvizsgálja (lásd a (110) preambulumbekezdést) ([390]). E felülvizsgálat részeként a PCLOB többek közt értékelni fogja, hogy az ODNI CLPO és a DPRC időben kezelte-e a panaszokat; teljes körű hozzáférést kapott-e a szükséges információkhoz; a felülvizsgálati eljárás során megfelelően figyelembe vette-e a 14086. elnöki rendelet alapvető biztosítékait; és hogy a Hírszerző Közösség teljes mértékben eleget tett-e az ODNI CLPO és a DPRC által tett megállapításoknak. A PCLOB jelentést készít a felülvizsgálat eredményéről az elnöknek, a főügyésznek, a nemzeti hírszerzés igazgatójának, a hírszerző ügynökségek vezetőjének, az ODNI CLPO-nak és a kongresszusi hírszerzési bizottságoknak, amelyet szintén nem titkosított változatban tesznek közzé, és amelyet ezt követően beépítenek e határozat működésének a Bizottság által elvégzendő időszakos felülvizsgálatába. A főügyésznek, a nemzeti hírszerzés igazgatójának, az ODNI CLPO-nak és a hírszerző ügynökségek vezetőinek végre kell hajtaniuk vagy más módon kell kezelniük az ilyen jelentésekben foglalt valamennyi ajánlást. Emellett a PCLOB évente nyilvános tanúsítványt állít ki arról, hogy a jogorvoslati mechanizmus a 14086. elnöki rendelet követelményeinek megfelelően kezeli-e a panaszokat.

([382]) 14086. elnöki rendelet 4. szakaszának (a) pontja.

([383]) 14086. elnöki rendelet 3. szakasza (d) pontjának (ii) alpontja, valamint a főügyészi rendelet 201.9(g) szakasza. Tekintettel arra, hogy a DPRC határozata végleges és kötelező erejű, semmilyen más végrehajtó vagy közigazgatási intézmény/szerv (beleértve az Egyesült Államok elnökét is) nem helyezheti hatályon kívül a DPRC határozatát. Ezt a Legfelsőbb Bíróság ítélkezési gyakorlata is megerősítette, amely egyértelművé tette, hogy azáltal, hogy a legfőbb ügyésznek a végrehajtó hatalmi ágon belül egy független szervre ruházta át a kötelező erejű határozatok kibocsátására vonatkozó kizárólagos hatáskörét, a legfőbb ügyész tagadja, hogy bármilyen módon irányíthatná e szerv döntését (lásd az Egyesült Államok ex rel. Accardi kontra Shaughnessy ügyet, 347 U.S. 260, 1954).

([384]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (F) szakasza, valamint a főügyészi rendelet 201.9(i) szakasza.

([385]) A főügyészi rendelet 201.9(h) szakasza.

([386]) 14086. elnöki rendelet 3. szakasza (d) pontja (i) alpontjának (H) szakasza, valamint a főügyészi rendelet 201.9(h) szakasza. A bejelentés jellegét illetően lásd a főügyészi rendelet 201.9. szakasza h) pontjának 3. alpontját.

([387]) A főügyészi rendelet 201.9(j) szakasza.

([388]) 14086. elnöki rendelet 3. szakasza (d) pontja (v) alpontjának (A) szakasza.

([389]) 14086. elnöki rendelet 3. szakasza (d) pontjának (v) alpontja.

([390]) 14086. elnöki rendelet 3. szakaszának (e) pontja. Lásd továbbá: https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

(195) A 14086. elnöki rendelet alapján létrehozott egyedi jogorvoslati mechanizmus mellett jogorvoslati lehetőségek is rendelkezésre állnak minden természetes személy számára (az állampolgárságuktól vagy tartózkodási helyüktől függetlenül) az Egyesült Államok rendes bíróságai előtt ([391]).

(196) Különösen a FISA és egy kapcsolódó statútum kiterjed az egyének azon lehetőségére, hogy pénzbeli kártérítés iránti polgári jogi keresetet indítsanak az Egyesült Államok ellen, amennyiben jogellenesen és szándékosan használták vagy hozták nyilvánosságra a velük kapcsolatos információkat ([392]); hogy magánszemélyi minőségükben pénzbeli kártérítés iránti keresetet indítsanak az Egyesült Államok kormányzati tisztviselőivel szemben ([393]); továbbá hogy vitassák a megfigyelés jogszerűségét (és az információk törlését követeljék) abban az esetben, ha az Egyesült Államok kormánya az elektronikus megfigyelés során megszerzett vagy abból származó bármely információt szándékozik felhasználni vagy nyilvánosságra hozni az adott személlyel szemben, az Egyesült Államokban zajló bírósági vagy közigazgatási eljárások során ([394]). Általánosabban fogalmazva, ha a kormány bűnüldözési operatív műveletek során szerzett információkat kíván felhasználni a gyanúsított ellen büntetőeljárásban, az alkotmányos és jogszabályi követelmények ([395]) bizonyos információk közlésére vonatkozó kötelezettségeket írnak elő, hogy az alperes vitathassa a bizonyítékok kormány általi gyűjtésének és felhasználásának jogszerűségét.

(197) Másrészt számos további jogorvoslati lehetőség létezik, amelyeket fel lehet használni ahhoz, hogy jogorvoslatot igényeljenek a kormányzati tisztviselőkkel szemben a személyes adatokhoz való jogellenes kormányzati hozzáférés vagy azok jogellenes felhasználása miatt, ideértve az elérni kívánt nemzetbiztonsági célokat (vagyis a számítógépes csalásról és visszaélésről szóló törvény ([396]); az elektronikus kommunikáció adatvédelméről szóló törvény ([397]); valamint a pénzügyi adatok védelméről szóló törvény ([398])). E keresetek minden említett jogcíme konkrét adatokra, célszemélyekre és/vagy hozzáférési típusokra (pl. egy számítógéphez való távoli hozzáférés az interneten keresztül) vonatkozik, és bizonyos feltételek mellett (pl. szándékos cselekmény, hivatalos minőségen kívüli cselekmény, elszenvedett kár) vehető igénybe.

(198) Általánosabb jogorvoslati lehetőséget kínál az államigazgatási eljárásról szóló törvény ([399]), amely szerint „egy hivatal tevékenysége miatt jogellenesen kárt szenvedő vagy egy hivatal tevékenysége révén hátrányos helyzetbe kerülő vagy sérelmet szenvedő személyek" jogosultak bírósági jogorvoslatot igényelni ([400]). Ez többek között azt jelenti, hogy kérhetik a bíróságtól „az önkényesnek, kiszámíthatatlannak, mérlegelési jogkörrel való visszaélésnek vagy egyébként a joggal ellentétesnek talált […] hivatali intézkedés megállapítás és következtetések jogellenességének kimondását és azok hatályon kívül helyezését" ([401]). Például egy szövetségi fellebbviteli bíróság egy 2015-ös APA-keresettel kapcsolatban úgy határozott, hogy a FISA 501. szakasza nem engedélyezte a telefonos metaadatoknak az Egyesült Államok kormánya általi tömeges gyűjtését ([402]).

([391]) Az ezekhez a lehetőségekhez való hozzáférés a „legitimáció" bemutatásától függ. Ez a norma, amely állampolgárságtól függetlenül valamennyi egyénre alkalmazandó, az Egyesült Államok Alkotmányának III. cikkében meghatározott, „ügyek és jogviták" követelményéből ered. A Legfelsőbb Bíróság szerint ehhez az szükséges, hogy 1. az egyén ténylegesen kárt szenvedett (azaz egy jogilag védett érdek olyan sérelme, amely konkrét és különválasztható, valamint tényleges vagy közvetlen), 2. ok-okozati összefüggés áll fenn a sérelem és a bíróság előtt támadott magatartás között, valamint 3. valószínű, és nem csak spekulatív jellegű, hogy a bíróság kedvező döntése megoldja a sérelmet (lásd: Lujan kontra Defenders of Wildlife, 504 U.S. 555, 1992).

([392]) 18 U.S.C. § 2712.

([393]) 50 U.S.C. § 1810.

([394]) 50 U.S.C. § 1806.

([395]) Lásd: Brady kontra Maryland ítélet, 373 U.S. 83 (1963) és Jencks Act, 18 U.S.C., § 3500.

([396]) 18 U.S.C. § 1030.

([397]) 18 U.S.C. §§ 2701–2712.

([398]) 12 U.S.C. § 3417.

([399]) 5 U.S.C. § 702.

([400]) Általában csupán a „végleges" ügynökségi intézkedés – nem pedig az „előzetes" vagy „közbenső" ügynökségi intézkedés – tartozik bírósági felülvizsgálat hatálya alá. Lásd 5 U.S.C. § 704.

([401]) 5 U.S.C. § 706(2)(A).

([402]) ACLU kontra Clapper, 785 F.3d 787 (2d. Cir. 2015), az ezekben az ügyekben megtámadott tömeges telefonos gyűjtési programot az USA FREEDOM-törvény szüntette meg 2015-ben.

(199) Végezetül, a (176)–(198) preambulumbekezdésben említett jogorvoslati lehetőségek mellett minden egyénnek joga van ahhoz, hogy hozzáférést kérjen a FOIA alapján meglévő szövetségi ügynökségi nyilvántartásokhoz, beleértve azokat az eseteket is, amikor azok az egyén személyes adatait tartalmazzák ([403]). Az ilyen hozzáférés a rendes bíróságok előtti keresetindítást is megkönnyítheti, többek között a kereshetőségi jog bizonyításának támogatása céljából. Az ügynökségek visszatarthatják azokat az információkat, amelyek bizonyos felsorolt kivételek hatálya alá tartoznak, ideértve a minősített nemzetbiztonsági információkhoz és a bűnüldözési nyomozásokhoz való hozzáférést is ([404]), de a válasszal elégedetlen panaszosoknak lehetőségük van arra, hogy közigazgatási, majd ezt követően (szövetségi bíróságok előtt) bírósági felülvizsgálatot kérjenek ([405]).

(200) A fentiekből következik, hogy amikor az Egyesült Államok bűnüldözési vagy nemzetbiztonsági hatóságai hozzáférnek az e határozat hatálya alá tartozó személyes adatokhoz, az említett hozzáférést olyan jogszabályi keret szabályozza, amely meghatározza a hozzáférés feltételeit, és biztosítja, hogy az adatokhoz való hozzáférés és a további felhasználás csak az elérni kívánt közérdekű célkitűzésekhez szükséges és azokkal arányos adatokra korlátozódnak. Ezekre a biztosítékokra azok az egyének hivatkozhatnak, akik hatékony jogorvoslati jogokkal rendelkeznek.

4. **KÖVETKEZTETÉS**

(201) A Bizottság úgy véli, hogy az Egyesült Államok – az Egyesült Államok Kereskedelmi Minisztériuma által kiadott elvek révén – olyan szintű védelmet biztosít az Unióból az EU-USA adatvédelmi keret alapján tanúsított, egyesült államokbeli szervezeteknek a továbbított személyes adatok tekintetében, amely lényegében egyenértékű az (EU) 2016/679 rendelet által garantálttal.

(202) A Bizottság ezenfelül úgy ítéli meg, hogy az elvek hatékony alkalmazását az átláthatósági követelmények és az adatvédelmi keret Kereskedelmi Minisztérium általi igazgatása garantálja. Ezenkívül az Egyesült Államok jogában létező felügyeleti mechanizmusok és jogorvoslati megoldások összességében véve lehetővé teszik, hogy a gyakorlatban azonosítsák és szankcionálják, ha a személyes adatokat kezelő bűnüldözési hatóságok jogsértést követnek el, továbbá jogorvoslatot biztosítanak az érintetteknek, hogy betekinthessenek a rájuk vonatkozó személyes adatokba, és adott esetben helyesbíttethessék vagy töröltethessék ezeket az adatokat.

(203) Végül az egyesült államokbeli jogrendről rendelkezésre álló információk alapján – beleértve a VI. és VII. mellékletben szereplő információkat – a Bizottság úgy véli, hogy az egyesült államokbeli hatóságoknak a közérdekbe, különösen azon egyének alapvető jogaiba bűnüldözési és nemzetbiztonsági célokból történő beavatkozása, akiknek személyes adatait az EU-USA adatvédelmi keret alapján az Unióból az Egyesült Államokba továbbítják, a szóban forgó jogszerű cél eléréséhez feltétlenül szükséges mértékre fog korlátozódni, és hogy az említett beavatkozással szemben hatékony jogvédelem áll fenn. Ezért a fenti megállapításokra figyelemmel olyan határozatot kell hozni, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az (EU) 2016/679 rendeletnek az Európai Unió Alapjogi Chartájára figyelemmel értelmezett 45. cikke értelmében az Európai Unióból az EU–USA adatvédelmi keret szerint tanúsított szervezeteknek továbbított személyes adatok tekintetében.

(204) Tekintettel arra, hogy a 14086. elnöki rendelet által létrehozott korlátozások, biztosítékok és jogorvoslati mechanizmusok az Egyesült Államok azon jogi keretének alapvető elemei, amelyen a Bizottság értékelése alapul, e határozat elfogadása azon alapul, hogy valamennyi amerikai hírszerző ügynökség elfogadja a 14086. elnöki rendelet végrehajtására vonatkozó aktualizált szabályzatokat és eljárásokat, valamint hogy az Uniót a 2023. július 3-án (lásd a (126) preambulumbekezdést) és 2023. június 30-án (lásd a (176) preambulumbekezdést) megvalósult jogorvoslati mechanizmus céljából jogosult szervezetnek minősítse.

([403]) 5 U.S.C. § 552. Hasonló törvények vannak hatályban tagállami szinten.

([404]) Ebben az esetben az adott egyén általában csak szabványos választ kap az ügynökségtől, amelyben az ügynökség megtagadja bármely nyilvántartás létezésének megerősítését vagy cáfolatát. Lásd: ACLU kontra CIA ügy, 710 F.3d 422 (D.C. Cir. 2014). A minősítés kritériumait és időtartamát a 13526. elnöki rendelet határozza meg, amely általános szabályként előírja, hogy a minősítés feloldásának konkrét időpontját vagy eseményét az információ nemzetbiztonsági érzékenységének időtartama alapján kell megállapítani, amely időpontban az információ minősítését automatikusan fel kell oldani (lásd a 13526. elnöki rendelet 1.5. szakaszát).

([405]) A bíróság *de novo* határozza meg, hogy a nyilvántartásokat jogszerűen tartják-e vissza, és kötelezheti a kormányt a nyilvántartásokhoz való hozzáférés biztosítására (5 U.S.C. § 552(a)(4)(B)).

5. E HATÁROZAT ÉS AZ ADATVÉDELMI HATÓSÁGOK INTÉZKEDÉSÉNEK JOGHATÁSAI

(205) A tagállamok és szerveik kötelesek megtenni az ahhoz szükséges intézkedéseket, hogy teljesítsék az uniós intézmények jogi aktusait, mivel az utóbbiak vélelmezhetően jogszerűek, és ennélfogva mindaddig joghatásokat váltanak ki, amíg azokat vissza nem vonják, megsemmisítés iránti kereset alapján meg nem semmisítik, illetve előzetes döntéshozatal iránti kérelem vagy jogellenességi kifogás következtében nem nyilvánítják érvénytelennek.

(206) Következésképpen a Bizottságnak az (EU) 2016/679 rendelet 45. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozata kötelező a címzett tagállamok valamennyi szervére, így független felügyeleti hatóságaikra nézve is. E határozat alkalmazásának időtartama alatt különösen az uniós adatkezelőtől vagy adatfeldolgozótól az egyesült államokbeli tanúsított szervezetekhez történő továbbításra további engedély beszerzése nélkül kerülhet sor.

(207) Ugyanakkor emlékeztetni kell arra, hogy az (EU) 2016/679 rendelet 58. cikkének (5) bekezdése alapján, és amint azt a Bíróság a Schrems-ítéletben ([406]) kifejtette, amennyiben egy nemzeti adatvédelmi hatóság megkérdőjelezi – ideértve a panaszra történő eljárást is – a Bizottság megfelelőségi határozatának az egyén magánélethez és adatvédelemhez fűződő alapvető jogaival való összeegyeztethetőségét, a nemzeti jognak biztosítania kell a jogorvoslati lehetőségeket, amelyek lehetővé teszik számára, hogy a nemzeti bíróságok előtt a kifogásokra hivatkozzon annak érdekében, hogy azok esetlegesen előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából ([407]).

6. E HATÁROZAT NYOMON KÖVETÉSE ÉS FEÜLVIZSGÁLATA

(208) A Bíróság ítélkezési gyakorlata alapján ([408]) és az (EU) 2016/679 rendelet 45. cikkének (4) bekezdésében elismerteknek megfelelően a Bizottság folyamatosan figyelemmel kíséri a harmadik országokban egy megfelelőségi határozat elfogadását követő kapcsolódó fejleményeket, hogy értékelje, hogy a harmadik ország továbbra is biztosítja-e a védelem lényegében azonos szintjét. E vizsgálat mindenképpen szükséges azokban az esetekben, amikor a Bizottság által kapott információk alapján indokolt kétségek merülhetnek fel e tekintetben.

(209) A Bizottság ezért folyamatosan nyomon követi az Egyesült Államokban a helyzetet az ebben a határozatban értékelt adatkezelés jogi keretének és mindenkori gyakorlatának vonatkozásában. E folyamat megkönnyítése érdekében az Egyesült Államok hatóságainak haladéktalanul tájékoztatniuk kell a Bizottságot az Egyesült Államok jogrendjének minden olyan lényeges fejleményéről, amely hatást gyakorol az e határozat tárgyát képező jogi keretre, valamint személyes adatok az e határozatban értékelt kezelésével kapcsolatos gyakorlatok minden változásáról, mind a személyes adatok egyesült államokbeli tanúsított szervezetek általi kezelését, mind a személyes adatokhoz a közigazgatási szervek általi hozzáférést illető korlátozásokat és biztosítékokat illetően.

(210) Továbbá annak lehetővé tétele érdekében, hogy a Bizottság hatékonyan lássa el nyomonkövetési feladatát, a tagállamoknak tájékoztatniuk kell a Bizottságot a nemzeti adatvédelmi hatóságok minden vonatkozó lépéséről, különösen az uniós érintetteknek a személyes adatok Európai Unióból az egyesült államokbeli tanúsított szervezetek felé történő továbbításával kapcsolatos kérései vagy panaszai tekintetében. A Bizottságot továbbá tájékoztatni kell minden arra utaló információról, hogy a bűnügyek megelőzéséért, nyomozásáért, felderítéséért vagy a vádemelésért, illetve a nemzetbiztonságért felelős koreai hatóságok – a felügyeleti szerveket is ideértve – intézkedései nem biztosítják a megfelelő szintű védelmet.

([406]) Schrems-ügy, 65. pont.

([407]) Schrems-ügy, 65. pont: „Ezzel összefüggésben a nemzeti jogalkotó feladata, hogy előírja azon jogorvoslati lehetőségeket, amelyek lehetővé teszik az érintett nemzeti felügyelő hatóság számára, hogy a nemzeti bíróságok előtt az általa megalapozottnak talált kifogásokra hivatkozzon annak érdekében, hogy amennyiben az utóbbiak osztják e hatóságnak a bizottsági határozat érvényessége tekintetében fennálló kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából.”

([408]) Schrems-ügy, 76. pont.

(211) Az (EU) 2016/679 rendelet 45. cikke (3) bekezdésének ([409]) alkalmazásában a Bizottságnak e határozat elfogadását követően rendszeresen felül kell vizsgálnia, hogy az Egyesült Államok által az EU–USA adatvédelmi keret szerint biztosított védelmi szint megfelelőségére vonatkozó megállapítások továbbra is tényszerűen és jogilag indokoltak-e. Mivel különösen a 14086. elnöki rendelet és a főügyészi rendelet új mechanizmusok létrehozását és új biztosítékok végrehajtását írja elő, ezt a határozatot a hatálybalépését követő egy éven belül első alkalommal felül kell vizsgálni annak ellenőrzése érdekében, hogy az összes releváns elemet teljes mértékben végrehajtották-e, és azok a gyakorlatban hatékonyan működnek-e. Az első felülvizsgálatot követően és annak eredményétől függően a Bizottság az (EU) 2016/679 rendelet 93. cikkének (1) bekezdése alapján létrehozott bizottsággal és az Európai Adatvédelmi Testülettel szorosan egyeztetve dönt a jövőbeli felülvizsgálatok gyakoriságáról ([410]).

(212) A felülvizsgálatok elvégzése érdekében a Bizottságnak találkoznia kell a Kereskedelmi Minisztériummal, az FTC-vel és a Közlekedési Minisztériummal, adott esetben az EU–USA adatvédelmi keret végrehajtásában részt vevő más szervezeti egységekkel és ügynökségekkel, valamint az adatokhoz való kormányzati hozzáféréssel kapcsolatos ügyekben az Igazságügyi Minisztérium, az ODNI (beleértve a CLPO-t is), a Hírszerző Közösség egyéb elemei, a DPRC és a különleges főtanácsnokok képviselőivel. E találkozón részt vehetnek az Európai Adatvédelmi Testület tagjainak képviselői.

(213) A felülvizsgálatoknak ki kell terjedniük e határozat működésének valamennyi szempontjára, tekintettel a személyes adatoknak az Egyesült Államokban történő kezelésére, és különösen az elvek alkalmazására és végrehajtására, különös tekintettel az újbóli adattovábbítás esetén nyújtott védelemre; a vonatkozó ítélkezési gyakorlat fejleményeire; az egyéni jogok gyakorlásának hatékonyságára; az elveknek való megfelelés nyomon követésére és érvényesítésére; valamint a kormányzati hozzáférésre vonatkozó korlátozások és biztosítékok, nevezetesen a 14086. elnöki rendelet által bevezetett biztosítékok végrehajtására és alkalmazására, többek között a hírszerző ügynökségek által kidolgozott szabályzatok és eljárások révén; a 14086. elnöki rendelet és a FISA 702. szakasza és a 12333. elnöki rendelet közötti kölcsönhatásra; valamint a felügyeleti mechanizmusok és jogorvoslati lehetőségek hatékonyságára (beleértve a 14086. elnöki rendelet alapján létrehozott új jogorvoslati mechanizmus működését). E felülvizsgálatok keretében figyelmet kell fordítani az adatvédelmi hatóságok és az Egyesült Államok illetékes hatóságai közötti együttműködésre is, beleértve az elvek alkalmazására, valamint a keret működésének egyéb szempontjaira vonatkozó iránymutatások és egyéb értelmező eszközök kidolgozását.

(214) A felülvizsgálat alapján a Bizottság az Európai Parlamentnek és a Tanácsnak benyújtandó nyilvános jelentést készít.

7. E HATÁROZAT FELFÜGGESZTÉSE, VISSZAVONÁSA VAGY MÓDOSÍTÁSA

(215) Amennyiben a rendelkezésre álló információk, különösen az e határozat nyomon követéséből származó, vagy az Egyesült Államok vagy a tagállamok hatóságai által szolgáltatott információk arra utalnak, hogy az Egyesült Államok által biztosított védelem szintje már nem feltétlenül megfelelő, a Bizottságnak erről haladéktalanul tájékoztatnia kell az Egyesült Államok illetékes hatóságait, és kérheti a megfelelő intézkedések meghatározott, észszerű határidőn belüli meghozatalát.

(216) Ha az említett határidő lejártakor az Egyesült Államok illetékes hatóságai nem hozzák meg ezeket az intézkedéseket, vagy más módon nem bizonyítják kielégítően, hogy e határozat továbbra is a megfelelő szintű védelmen alapul, a Bizottság megindítja az (EU) 2016/679 rendelet 93. cikkének (2) bekezdésében említett eljárást e határozat részleges vagy teljes felfüggesztése vagy hatályon kívül helyezése céljából.

(217) Ennek alternatívájaként a Bizottságnak ezt az eljárást e határozat módosítása céljából indítja meg, különösen az adattovábbításra további feltételek előírásával vagy a megfelelőség megállapítása hatályának azokra az adattovábbításokra korlátozásával, amelyek esetében biztosított a megfelelő szintű védelem folyamatossága.

([409]) Az (EU) 2016/679 rendelet 45. cikkének (3) bekezdése szerint „a végrehajtási jogi aktusban rendelkezni kell egy rendszeres […] felülvizsgálatra irányuló mechanizmusról, amely az adott harmadik országban vagy nemzetközi szervezetnél végbement valamennyi releváns fejleményt figyelembe vesz”.

([410]) Az (EU) 2016/679 rendelet 45. cikkének (3) bekezdése előírja, hogy a felülvizsgálat rendszeresen, „legalább négyévente elvégzendő”. Lásd még: Európai Adatvédelmi Testület, Megfelelési referencia, WP 254 rev. 01.

(218) A Bizottság mindenekelőtt az alábbi esetekben indítja el a felfüggesztési vagy hatályon kívül helyezési eljárást:

a) annak jelzése, hogy azok a szervezetek, amelyek e határozat alapján személyes adatokat kaptak az Unióból, nem felelnek meg az elveknek, és hogy az illetékes felügyeleti és végrehajtó szervek nem orvosolják hatékonyan az ilyen meg nem felelést;

b) annak jelzése, hogy az Egyesült Államok hatóságai nem felelnek meg az Egyesült Államok hatóságainak az EU–USA adatvédelmi keret alapján továbbított személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésére vonatkozó feltételeknek és korlátozásoknak; vagy

c) az uniós érintettek, többek között az ODNI CLPO és/vagy a DPRC által benyújtott panaszok hatékony kezelésének elmulasztása.

(219) A Bizottságnak emellett meg kell vizsgálnia az olyan eljárás kezdeményezésének lehetőségét, amely e határozat módosításához, felfüggesztéséhez vagy visszavonásához vezet, ha az illetékes egyesült államokbeli hatóságok nem adják át az Európai Unióból az Egyesült Államokba továbbított személyes adatok védelmének szintje vagy az e határozatnak való megfelelés értékeléséhez szükséges információkat vagy nem adnak erre vonatkozó magyarázatokat. Ebben a tekintetben a Bizottságnak figyelembe kell vennie, hogy milyen mértékben szerezhető be más forrásokból a vonatkozó információ.

(220) Kellően indokolt, rendkívül sürgős esetben, például ha a 14086. elnöki rendelet vagy a főügyészi rendelet oly módon módosulna, hogy az aláássa az e határozatban leírt védelmi szintet, vagy ha az Unió főügyész által minősített szervezetnek való kinevezésének visszavonására kerül sor, a Bizottság élni fog azzal a lehetőséggel, hogy az (EU) 2016/679 rendelet 93. cikkének (3) bekezdésében említett eljárásnak megfelelően azonnal alkalmazandó végrehajtási jogi aktusokat fogadjon el e határozat felfüggesztéséről, hatályon kívül helyezéséről vagy módosításáról.

8. **ZÁRÓ MEGÁLLAPÍTÁSOK**

(221) Az Európai Adatvédelmi Testület közzétette véleményét ([411]), amely e határozat kidolgozásakor figyelembevételre került.

(222) Az Európai Parlament állásfoglalást fogadott el az EU–USA adatvédelmi keret által biztosított védelem megfelelőségéről ([412]).

(223) Az e határozatban előírt intézkedések összhangban vannak az (EU) 2016/679 rendelet 93. cikke (1) bekezdése alapján létrehozott bizottság véleményével.

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Az (EU) 2016/679 rendelet 45. cikke alkalmazásában az Egyesült Államok megfelelő szintű védelmet biztosít az olyan szervezetekhez továbbított személyes adatok számára, amelyek szerepelnek az adatvédelmi keretben részt vevő szervezetek listájában, amelyet az Egyesült Államok Kereskedelmi Minisztériuma vezet és tesz nyilvánosan elérhetővé, az I. melléklet I.3. szakaszával összhangban.

2. cikk

Az érintett tagállam haladéktalanul tájékoztatja a Bizottságot, amikor a személyes adataik kezelése tekintetében az egyének védelme érdekében a tagállam illetékes hatóságai gyakorolják az (EU) 2016/679 rendelet 58. cikke értelmében vett hatáskörüket az e határozat 1. cikkében említett adattovábbítások tekintetében.

([411]) 5/2023. sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló, 2023. február 28-i európai bizottsági végrehajtási határozat tervezetéről.

([412]) Az Európai Parlament állásfoglalása (2023. május 11.) az EU–USA adatvédelmi keret által biztosított védelem megfelelőségéről (2023/2501[RSP]).

3. cikk

(1) A Bizottság folyamatosan figyelemmel kíséri az e határozat tárgyát képező jogi keret alkalmazását – ideértve az újbóli adattovábbítások lebonyolításának, az egyéni jogok gyakorlásának és az egyesült államokbeli hatóságok e határozat alapján továbbított adatokhoz való hozzáférésnek feltételeit – annak értékelése céljából, hogy Egyesült Államok az 1. cikk értelmében továbbra is megfelelő szintű védelmet biztosít-e.

(2) A tagállamok és a Bizottság tájékoztatják egymást az olyan esetekről, amikor úgy látszik, hogy a II. mellékletben ismertetett elvek teljesítésének kikényszerítésére törvényi hatáskörrel rendelkező egyesült államokbeli szervek nem biztosítanak olyan hatékony felderítési és felügyeleti mechanizmusokat, amely a lehetővé tennék az elvek megsértéseinek gyakorlati azonosítását és szankcionálását.

(3) A tagállamok és a Bizottság tájékoztatják egymást bármely arra utaló körülményről, hogy az Egyesült Államok felelős hatóságainak az egyének személyes adataik védelméhez fűződő jogába történő nemzetbiztonsági, bűnüldözési vagy egyéb közérdekű célú beavatkozása túllépi a szükséges és arányos mértéket és/vagy nem létezik hatékony jogvédelem az ilyen beavatkozásokkal szemben.

(4) A Bizottság az e határozatról a tagállamoknak küldött értesítés időpontjától számított egy éven belül és azt követően legalább az (EU) 2016/679 rendelet 93. cikkének (1) bekezdése alapján létrehozott bizottsággal és az Európai Adatvédelmi Testülettel folytatott szoros konzultáció során elfogadandó gyakorisággal értékeli az 1. cikk (1) bekezdésében foglalt megállapítást valamennyi rendelkezésre álló információ alapján, ideértve az Egyesült Államok illetékes hatóságaival együtt végzett felülvizsgálatokon keresztül szerzett információkat.

(5) Ha a Bizottság arra utaló körülményről szerez tudomást, hogy már nem biztosított a védelem megfelelő szintje, a Bizottság tájékoztatja erről az illetékes egyesült államokbeli hatóságokat. Szükség esetén úgy határoz, hogy az (EU) 2016/679 rendelet 45. cikkének (5) bekezdésével összhangban felfüggeszti, módosítja vagy hatályon kívül helyezi ezt a határozatot, vagy korlátozza alkalmazási körét. A Bizottság emellett akkor is elfogadhat ilyen határozatot, ha az Egyesült Államok kormánya együttműködésének hiánya miatt nem tudja megállapítani, hogy az Egyesült Államok továbbra is biztosítja-e a megfelelő védelmi szintet.

4. cikk

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2023. július 10-én.

a Bizottság részéről
Didier REYNDERS
a Bizottság tagja

I. MELLÉKLET

AZ EU–USA ADATVÉDELMI KERET ELVEI KIADTA AZ EGYESÜLT ÁLLAMOK KERESKEDELMI MINISZTÉRIUMA

I. ÁTTEKINTÉS

1. Bár az Egyesült Államok és az Európai Unió (a továbbiakban: az EU) egyaránt elkötelezett a magánélet védelmének erősítése és a jogállamiság iránt, és mindketten elismerik a transzatlanti adatáramlás fontosságát polgáraink, gazdaságaink és társadalmaink számára, az Egyesült Államok a magánélet védelmével kapcsolatban más megközelítést alkalmaz, mint az EU. Az Egyesült Államok ágazati megközelítést használ, amely a jogalkotási eszközök, az előírások és az önszabályozás kombinációján alapszik. Az Egyesült Államok Közlekedési Minisztériuma (a továbbiakban: a Minisztérium) a nemzetközi kereskedelem ösztönzésére, előmozdítására és fejlesztésére irányuló, törvényileg meghatározott hatáskörénél fogva (lásd az USA Szövetségi Törvénykönyvének vonatkozó részét: 15 U.S.C. § 1512) kibocsátja az EU–USA adatvédelmi keret elveit, beleértve azok kiegészítő elveit (a továbbiakban együttesen: az elvek) és az elvek I. mellékletét (a továbbiakban: I. melléklet). Az elveket az Európai Bizottsággal (a továbbiakban: a Bizottság), az ágazattal és más érdekelt felekkel konzultálva az Egyesült Államok és az EU közötti kereskedelem megkönnyítése érdekében dolgozták ki. Az elvek, amelyek az EU–USA adatvédelmi keret kulcsfontosságú elemei, megbízható mechanizmust biztosítanak az egyesült államokbeli szervezetek számára a személyes adatok EU-ból az Egyesült Államokba történő továbbítására, miközben biztosítják, hogy az uniós érintettek továbbra is részesüljenek az európai jogszabályok által előírt hatékony biztosítékokban és védelemben személyes adataik kezelése tekintetében, amennyiben azokat nem uniós országokba továbbították. Az elveket kizárólag az Európai Unióból személyes adatokat fogadó egyesült államokbeli szervezetek használhatják az EU–USA adatvédelmi keretnek való megfelelés, és ezáltal az Európai Bizottság megfelelőségi határozatának elnyerése céljából ([1]). Az elvek nem érintik a tagállamokban a személyes adatok kezelésére alkalmazandó (EU) 2016/679 rendelet (a továbbiakban: általános adatvédelmi rendelet vagy GDPR) ([2]) alkalmazását. Az elvek az Egyesült Államok joga alapján egyébként alkalmazandó adatvédelmi kötelezettségeket sem korlátozzák.

2. Annak érdekében, hogy a szervezetek a személyes adatok Unióból történő továbbítása céljából támaszkodhassanak az EU–USA adatvédelmi keretre, a szervezeteknek maguknak kell tanúsítaniuk az elveknek való megfelelésüket a Minisztérium (vagy annak megbízottja) számára. Míg a szervezetek maguk dönthetik el, hogy belépnek-e az EU–USA adatvédelmi keretbe, a tényleges megfelelés kötelező: azoknak a szervezeteknek, amelyek öntanúsítják a Minisztériumnak a megfelelésüket, és nyilvánosan kinyilvánítják elkötelezettségüket az elvek betartása mellett, teljes mértékben meg kell felelniük az elveknek. Az EU–USA adatvédelmi keretbe való belépéshez a szervezetnek a) a Szövetségi Kereskedelmi Bizottság (a továbbiakban: FTC), az Egyesült Államok Közlekedési Minisztériuma (a továbbiakban: Közlekedési Minisztérium vagy DOT) vagy más olyan hivatalos szerv vizsgálati és végrehajtási hatáskörébe kell tartoznia, amely ténylegesen biztosítani fogja az elveknek való megfelelést *(az EU által elismert egyéb állami szervek a jövőben mellékletben felvehetők)*, b) nyilvánosan kötelezettséget kell vállalnia az elvek betartása mellett, c) nyilvánosságra kell hoznia az ezen elvekkel összhangban lévő adatvédelmi szabályzatát, és d) maradéktalanul végre kell azt hajtania ([3]). Ha a szervezet nem felel meg az elveknek, akkor a Szövetségi Kereskedelmi Bizottságról szóló törvény tisztességtelen és megtévesztő cselekmények tilalmáról szóló 5. szakasza (15 U.S.C. § 45), vagy a DOT által a Szövetségi Törvénykönyv 49. címének – a fuvarozók vagy jegyértékesítők által a légi közlekedés vagy a légi közlekedés értékesítése terén folytatott tisztességtelen vagy megtévesztő gyakorlatok tilalmáról szóló – 41712. §-a, vagy az ilyen tevékenységek tilalmáról szóló más törvény vagy rendelet alapján peresíthető.

([1]) Amennyiben az EU–USA adatvédelmi keret által biztosított védelem megfelelőségére vonatkozó bizottsági határozat Izlandra, Liechtensteinre és Norvégiára is alkalmazandó, az EU–USA adatvédelmi keret egyaránt lefedi majd Európai Uniót és ezt a három országot. Következésképpen az EU-ra és annak tagállamaira való hivatkozások úgy értelmezendők, hogy azok Izlandra, Liechtensteinre és Norvégiára is vonatkoznak.

([2]) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

([3]) Az EU–USA adatvédelmi pajzs keretrendszer elveit „EU-USA adatvédelmi keret elveiként” módosították. (*Lásd* az öntanúsítás kiegészítő elvét).

3. A Minisztérium fenntart és nyilvánosságra hoz egy hiteles listát azokról az egyesült államokbeli szervezetekről, amelyek öntanúsítást végeztek a Minisztérium felé, és kötelezettséget vállaltak az elvek betartására (a továbbiakban: az adatvédelmi keretben részt vevő szervezetek listája). Az EU-USA adatvédelmi keret előnyei attól a naptól fogva biztosítottak a szervezet számára, amikor a Minisztérium felveszi a szervezetet az adatvédelmi keretben részt vevő szervezetek listájára. A Minisztérium törli az adatvédelmi keretben részt vevő szervezetek listájáról azon szervezeteket, amelyek önként kilépnek az EU–USA adatvédelmi keretből, vagy nem teljesítik az éves ismételt öntanúsítást a Minisztérium felé; ezeknek a szervezeteknek vagy továbbra is alkalmazniuk kell az elveket az EU–USA adatvédelmi keret alapján kapott személyes adatokra, és évente meg kell erősíteniük a Minisztérium felé az erre vonatkozó kötelezettségvállalásukat (*azaz* mindaddig, amíg megőrzik ezeket az adatokat), vagy más engedélyezett módon „megfelelő" védelmet kell biztosítaniuk az adatok számára (például olyan szerződés alkalmazásával, amely teljes mértékben tükrözi a Bizottság által elfogadott vonatkozó általános szerződési feltételek követelményeit), vagy vissza kell adniuk vagy törölniük kell az adatokat. A Minisztérium törli az adatvédelmi keretben részt vevő szervezetek listájáról azon szervezeteket is, amelyek folyamatosan nem felelnek meg az elveknek; ezeknek a szervezeteknek vissza kell küldeniük vagy törölniük kell az EU–USA adatvédelmi keret alapján kapott személyes adatokat. A szervezet törlése az adatvédelmi keretben részt vevő szervezetek listájáról azt jelenti, hogy többé nem vonatkozik rá a Bizottság megfelelőségi határozata a személyes adatok EU-ból történő fogadása tekintetében.

4. A Minisztérium fenntart és nyilvánosságra hoz egy hiteles listát azokról az egyesült államokbeli szervezetekről is, amelyek korábban öntanúsítást végeztek a Minisztérium felé, de később törölték őket az adatvédelmi keretben részt vevő szervezetek listájáról. A Minisztérium egyértelmű figyelmeztetést fog adni arra vonatkozóan, hogy ezek a szervezetek nem vesznek részt az EU–USA adatvédelmi keretben; hogy az adatvédelmi keretben részt vevő szervezetek listájáról való törlés azt jelenti, hogy az ilyen szervezetek nem állíthatják, hogy megfelelnek az EU–USA adatvédelmi keretnek, és kerülniük kell minden olyan kijelentést vagy félrevezető gyakorlatot, amely arra utal, hogy részt vesznek az EU–USA adatvédelmi keretben; és hogy az ilyen szervezetek már nem jogosultak arra, hogy a Bizottság megfelelőségi határozata alapján személyes adatokat kapjanak az EU-ból. Az a szervezet, amely továbbra is azt állítja, hogy részt vesz az EU–USA adatvédelmi keretben, vagy az adatvédelmi keretben részt vevő szervezetek listájáról történt törlése után az adatvédelmi kerettel kapcsolatos egyéb megtévesztő nyilatkozatot tesz, azzal szemben a Szövetségi Kereskedelmi Bizottság, a Közlekedési Minisztérium vagy más végrehajtási hatóság végrehajtási intézkedést foganatosíthat.

5. Az elvek betartása az alábbiak szerint korlátozható: a) a bírósági végzésnek való megfeleléshez vagy a közérdeknek, bűnüldözési vagy nemzetbiztonsági követelményeknek való megfeleléshez szükséges mértékben, beleértve azt az esetet is, amikor törvény vagy kormányrendelet ellentétes kötelezettségeket keletkeztet, b) olyan törvény, bírósági végzés vagy kormányrendelet által, amely kifejezett felhatalmazást ad erre, feltéve hogy ezen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nem teljesítése az e felhatalmazás által támogatott jogos érdekek teljesítéséhez szükséges mértékre korlátozódik, vagy c) ha az általános adatvédelmi rendelet joghatása – a benne foglalt feltételeknek megfelelően – kivételeket vagy eltéréseket tesz lehetővé, feltéve, hogy az ilyen kivételeket vagy eltéréseket hasonló esetekben alkalmazzák. Ezzel kapcsolatban az Egyesült Államok jogában a magánélet és a polgári szabadságjogok védelmére vonatkozó biztosítékok közé tartoznak a 14086. sz. elnöki rendeletben ([4]) előírt biztosítékok, az abban meghatározott feltételek mellett (beleértve a szükségességre és arányosságra vonatkozóan az elnöki rendeletben meghatározott követelményeket is). Az adatvédelem erősítésének céljával összhangban a szervezeteknek törekedniük kell az elvek teljes mértékű és átlátható megvalósítására, többek között azáltal, hogy törekednek arra, hogy adatvédelmi szabályzatukban feltüntetik, hogy az elvek alól a fenti b) pontban engedélyezett kivételeket mely esetekben alkalmazzák. Ugyanebből az okból, ahol az elvek és/vagy az Egyesült Államok jogszabályai választási lehetőséget engednek, a szervezetektől elvárják, hogy lehetőség szerint a magasabb szintű védelem mellett döntsenek.

6. A szervezetek az EU–USA adatvédelmi kerethez történő csatlakozásuk után az EU–USA adatvédelmi keret alapján továbbított valamennyi személyes adatra kötelesek alkalmazni az elveket. Az a szervezet, amely az EU–USA adatvédelmi keret előnyeit ki akarja terjeszteni az Európai Unióból továbbított, a munkaviszonnyal összefüggésben felhasználandó, humán erőforrással kapcsolatos személyes adatra, köteles ezt jelezni, amikor öntanúsítást végez a Minisztérium felé, és meg kell felelnie az öntanúsításról szóló kiegészítő elvben meghatározott követelményeknek.

([4]) Az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről szóló, 2022. október 7-i elnöki rendelet.

7. Az értelmezési kérdések és az EU–USA adatvédelmi keretben részt vevő szervezetek általi, az elveknek és a vonatkozó adatvédelmi szabályzatoknak való megfelelés tekintetében az Egyesült Államok jogát kell alkalmazni, kivéve, ha a szervezetek az európai adatvédelmi hatóságokkal („adatvédelmi hatóságok") való együttműködés mellett kötelezték el magukat. Eltérő megállapodás hiányában az elvek minden rendelkezését alkalmazni kell, ha relevánsak.

8. Fogalommeghatározások:

   a. „személyes adatok": olyan azonosított vagy azonosítható egyénre vonatkozó adatok, amelyek a GDPR hatálya alá tartoznak, és amelyeket valamely egyesült államokbeli szervezet az Európai Unióból kapott, és valamilyen formában rögzítette őket;

   b. „személyes adatok kezelése": a személyes adatokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés vagy terjesztés, valamint törlés vagy megsemmisítés;

   c. „adatkezelő": az a személy vagy szervezet, amely önállóan vagy másokkal együtt meghatározza a személyes adatok kezelésének célját és eszközeit.

9. Az elvek és az elvek I. melléklete hatálybalépésének napja az a nap, amikor az Európai Bizottság megfelelőségi határozata hatályba lép.

II. ELVEK

1. TÁJÉKOZTATÁS

a. A szervezetnek tájékoztatnia kell az egyéneket az alábbiakról:

   i. az EU–USA adatvédelmi keretben való részvétele, és egy linket vagy internetcímet kell biztosítania az EU–USA adatvédelmi keretben részt vevő szervezetek listájához;

   ii. a gyűjtött személyes adatok típusa és adott esetben a szervezetnek az elveket szintén teljesítő egyesült államokbeli egységei vagy egyesült államokbeli leányvállalatai;

   iii. a szervezet azon kötelezettségvállalása, hogy alkalmazza az elveket valamennyi személyes adatra, amelyet az Európai Uniótól az EU–USA adatvédelmi keret alapján kapott;

   iv. milyen célokra gyűjt és használ fel rájuk vonatkozó személyes adatokat;

   v. a szervezet elérhetősége érdeklődés és panasz esetén, beleértve az Európai Unión belüli szervezeti egységét, amely válaszolni tud az ilyen érdeklődésre vagy panaszra;

   vi. azon harmadik felek típusa vagy meghatározása, amelyekkel közli a személyes adatokat, és az adatok közlésének célja;

   vii. az egyéneknek a személyes adataikhoz való hozzáféréshez való joga;

   viii. a szervezet által az egyének számára biztosított lehetőségek és eszközök a személyes adataik felhasználásának vagy közlésének korlátozására;

   ix. a panaszok kezelésére és az egyének számára ingyenes jogorvoslat biztosítására kijelölt független vitarendezési szerv, valamint annak meghatározása, hogy az: 1. az adatvédelmi hatóságok által létrehozott testület, 2. az EU-ban székhellyel rendelkező alternatív vitarendezési szolgáltató vagy 3. az Egyesült Államokban székhellyel rendelkező alternatív vitarendezési szolgáltató;

   x. az FTC, a Közlekedési Minisztérium vagy más egyesült államokbeli erre felhatalmazott hatósági szerv vizsgálati és végrehajtási hatáskörébe tartozik;

   xi. lehetőség az egyén számára arra, hogy bizonyos feltételek mellett kötelező erejű választottbírósági határozatért folyamodjon ([5]);

   xii. az az előírás, hogy állami hatóságok jogszerű kérésére át kell adnia a személyes adatokat, többek között nemzetbiztonsági vagy bűnüldözési előírások teljesítése érdekében; és

   xiii. a felelőssége harmadik fél részére történő újbóli továbbítás esetén.

([5]) *Lásd pl.* a jogorvoslat, végrehajtás és felelősség elvének c) szakaszát.

b. Ezt a tájékoztatást világos és érthető megfogalmazásban kell megadni, akkor, amikor az egyént első alkalommal kérik fel arra, hogy a szervezet részére személyes adatokat szolgáltasson, vagy azt követően a lehető legrövidebb kivitelezhető időn belül, de minden esetben azt megelőzően, hogy a szervezet ezen adatokat más célra használná fel, mint amely célból az adatokat átadó szervezet eredetileg gyűjtötte vagy kezelte őket, vagy mielőtt harmadik félnek azokat először átadná.

2. VÁLASZTÁSI LEHETŐSÉG

a. A szervezetnek választási lehetőséget (önkéntes kívülmaradás) kell felkínálnia az egyénnek a tekintetben, hogy a személyes adatait i. átadják-e harmadik félnek; vagy ii. felhasználják-e olyan célra, amely lényegesen különbözik attól (azoktól) a cél(ok)tól, amely(ek)re eredetileg gyűjtötték az adatokat, vagy amelye(ke)t az egyén a későbbiekben engedélyezett. Az egyének számára egyértelmű, szembetűnő és könnyen hozzáférhető mechanizmusokat kell biztosítani a választási lehetőség gyakorlására.

b. Az előző bekezdéstől eltérően nem szükséges választási lehetőséget biztosítani, amikor az adatközlés a szervezet nevében és útmutatásai alapján feladato(ka)t végrehajtó, megbízottként eljáró harmadik fél részére történik. A szervezetnek azonban mindig szerződést kell kötnie a megbízottal.

c. A különleges adatok tekintetében (ilyenek az egyén orvosi vagy egészségi állapotára, faji vagy etnikai hovatartozására, politikai véleményére, vallási vagy filozófiai meggyőződésére, szakszervezeti tagságára vagy szexuális életére vonatkozó személyes adatok) a szervezeteknek megerősítő kifejezett hozzájárulást (önkéntes részvétel) kell kapniuk az egyéntől, hogy az adatot i. harmadik fél számára átadhatják-e, vagy ii. felhasználhatják-e a gyűjtés eredeti céljától, illetve az egyén által a választási lehetőségével élve a későbbiekben engedélyezett céltól eltérő célra. Ezenkívül a szervezetnek különleges adatként kell kezelnie minden olyan, harmadik féltől kapott személyes adatot, amelyet a harmadik fél érzékeny (különleges) adatként határoz meg és kezel.

3. ELSZÁMOLTATHATÓSÁG ÚJBÓLI TOVÁBBÍTÁSÉRT

a. A személyes adatok adatkezelőként eljáró harmadik fél számára történő továbbításához a szervezeteknek alkalmazniuk kell a tájékoztatás és a választási lehetőség elveit. A szervezeteknek szerződést kell kötniük a harmadik fél adatkezelővel, amely rendelkezik arról, hogy az ilyen adatok csak korlátozott és meghatározott célokból kezelhetők, amelyek összhangban vannak az egyén által adott hozzájárulással, valamint arról, hogy a címzett az elvekkel azonos szintű védelmet biztosít és értesíti a szervezetet, ha megállapítja, hogy már nem tud megfelelni ennek a kötelezettségnek. A szerződés úgy rendelkezik, hogy ilyen megállapítás esetén a harmadik fél adatkezelő megszünteti az adatkezelést vagy egyéb észszerű és megfelelő lépéseket tesz a védelem helyreállítására.

b. A személyes adatok megbízottként eljáró harmadik fél részére történő továbbítása esetén a szervezeteknek: i. az ilyen adatokat csak korlátozott és meghatározott célokra szabad továbbítaniuk, ii. meg kell bizonyosodniuk arról, hogy a megbízott köteles legalább olyan szintű adatvédelmet biztosítani, mint amit az elvek előírnak, iii. indokolt és megfelelő lépéseket kell tenniük annak biztosítására, hogy a megbízott valóban a szervezet elvek szerinti kötelezettségeivel összhangban kezeli a továbbított személyes adatokat, iv. kötelezniük kell a megbízottat, hogy értesítse a szervezetet, ha megállapítja, hogy már nem tud megfelelni azon kötelezettségének, hogy az elvekben előírttal azonos szintű védelmet biztosítson, v. kérésre – többek között a iv. alpont szerinti esetben – indokolt és megfelelő lépéseket kell tenniük a jogosulatlan adatkezelés megszüntetése és az eredeti állapot helyreállítása érdekében, és vi. az adott megbízottal kötött szerződésük megfelelő adatvédelmi rendelkezéseinek összefoglalását vagy egy reprezentatív példányát kérésre át kell adniuk a Minisztériumnak.

4. BIZTONSÁG

a. A személyes adatokat létrehozó, fenntartó, felhasználó vagy terjesztő szervezeteknek indokolt és megfelelő intézkedéseket kell tenniük, hogy megóvják az adatokat az elvesztéstől, a visszaéléstől, valamint a jogosulatlan hozzáféréstől, közléstől, megváltoztatástól és megsemmisítéstől, megfelelően figyelembe véve a kezeléssel járó kockázatokat és a személyes adatok természetét.

5. AZ ADATOK SÉRTETLENSÉGE ÉS A CÉLHOZ KÖTÖTTSÉG

a. Az elvekkel összhangban a személyes adatoknak olyan információkra kell korlátozódniuk, amelyek a kezelés célja szempontjából relevánsak ([6]). A szervezet nem dolgozhat fel személyes adatot a gyűjtés céljaival vagy az egyén által a későbbiekben engedélyezett célokkal összeegyeztethetetlen módon. A szervezetnek az ilyen célokhoz szükséges mértékben megfelelő lépéseket kell tennie annak biztosítására, hogy a személyes adatok a tervezett felhasználás szempontjából megbízhatók, pontosak, teljesek és naprakészek legyenek. A szervezetnek az adatok megőrzésének teljes időtartama alatt meg kell felelnie az elveknek.

b. Az adatok kizárólag addig őrizhetők meg az egyént azonosító vagy annak azonosítására alkalmas ([7]) formában, amíg ez az 5. pont a. alpontja értelmében az adatkezelés célját szolgálja. Ez a kötelezettség nem akadályozza meg, hogy a szervezet hosszabb időszakokon keresztül kezeljen személyes adatokat, amennyiben a szóban forgó adatkezelés észszerűen szolgálja a közérdekű archiválás, az újságírás, az irodalom és a művészet, a tudományos és történeti kutatás és a statisztikai elemzés céljait. Ilyen esetekben az érintett adatkezelés az EU–USA adatvédelmi keret egyéb elveinek és rendelkezéseinek hatálya alá tartozik. A szervezeteknek észszerű és megfelelő intézkedéseket kell hozniuk annak érdekében, hogy e rendelkezésnek megfeleljenek.

6. HOZZÁFÉRÉS

a. Az egyéneknek hozzáféréssel kell rendelkezniük a valamely szervezet birtokában lévő, rájuk vonatkozó személyes adatokhoz, és lehetőségük kell, hogy legyen a pontatlan vagy az elvek megsértésével kezelt adatok javítására, módosítására vagy törlésére, kivéve, ha az adott esetben a hozzáférés biztosításának terhe vagy költsége nem állna arányban az egyén adatvédelmi jogához fűződő kockázatokkal, vagy ha ezzel más személy jogait érné sérelem.

7. JOGORVOSLAT, VÉGREHAJTÁS ÉS FELELŐSSÉG

a. A hatékony adatvédelemnek magában kell foglalnia az elveknek való megfelelést biztosító erős mechanizmusokat, jogorvoslati jogot az elvek nemteljesítése által érintett egyének számára, valamint azt, hogy az elvek be nem tartása a szervezetre nézve jogkövetkezményekkel jár. Az ilyen mechanizmusoknak minimumkövetelményként tartalmazniuk kell:

   i. könnyen hozzáférhető független jogorvoslati mechanizmusokat, amelyekkel minden egyes személy panaszait és vitáit az egyén számára ingyenesen és az elvekre hivatkozva meg lehet vizsgálni és gyorsan rendezni lehet, és kártérítést lehet megítélni, ha az alkalmazandó jog vagy magánszektorbeli kezdeményezések ezt előírják;

   ii. nyomonkövetési eljárásokat annak ellenőrzésére, hogy a szervezetek által az adatvédelmi gyakorlataikról készített tanúsítványok és állítások helytállóak-e, és hogy az adatvédelmi gyakorlatokat úgy valósították-e meg, ahogyan azokat benyújtották, különös tekintettel a dokumentumokban foglaltak be nem tartásának eseteire; valamint

   iii. az elvek elfogadását kijelentő szervezetek részéről kötelezettséget az elvek be nem tartásából adódó problémák jogorvoslatára, valamint az ilyen szervezetekre vonatkozó következményeket. A szervezetek általi megfelelés biztosítása érdekében a szankcióknak kellőképpen szigorúaknak kell lenniük.

b. A szervezetek és a kiválasztott független jogorvoslati mechanizmusok azonnal válaszolnak a Minisztériumnak az EU–USA adatvédelmi kerettel kapcsolatos megkereséseire és információkéréseire. Valamennyi szervezetnek gyorsan kell válaszolnia az uniós tagállamok hatóságai által a Minisztériumon keresztül az elvek betartására vonatkozóan benyújtott panaszokra. Azoknak a szervezeteknek, amelyek úgy döntöttek, hogy együttműködnek az adatvédelmi hatóságokkal, beleértve a humánerőforrás-adatokat kezelő szervezeteket, közvetlenül ezeknek a hatóságoknak kell válaszolniuk a panaszok kivizsgálása és megoldása során.

([6]) A körülményektől függően az összeegyeztethető kezelési célok közé tartozhatnak azok, amelyek észszerűen szolgálják az ügyfélkapcsolatokat, a megfelelőséget és a jogi szempontokat, az ellenőrzést, a biztonságot, a csalás megelőzését, a szervezet törvényes jogainak megőrzését, illetve védelmét, vagy olyan egyéb célokat, amelyek az adatgyűjtés összefüggésében megfelelnek egy észszerűen gondolkodó személy elvárásainak.

([7]) E tekintetben egy egyén akkor „azonosítható”, ha – tekintettel azokra az azonosítási eszközökre, amelyeknek az alkalmazása észszerűen valószínűsíthető (figyelemmel többek között az azonosítás költségére és időigényére, valamint az adatkezelés idején rendelkezésre álló technológiára, továbbá az adatok megőrzésének formájára) – a szervezet vagy egy harmadik személy észszerűen azonosítani tudná az adott egyént, ha hozzáférne az adatokhoz.

c. A szervezetek kötelesek a panaszok választottbírósági rendezésére és az I. mellékletben meghatározott feltételek követésére, amennyiben egy egyén kötelező erejű választottbírósági határozatot kért az érintett szervezetnek küldött értesítéssel, követve az I. mellékletben meghatározott eljárásokat, és betartva az ott meghatározott feltételeket.

d. Újbóli továbbítás esetén az EU–USA adatvédelmi keretben részt vevő szervezet felelős az általa az adatvédelmi keret alapján kapott és ezt követően a nevében tevékenykedő harmadik fél megbízottnak átadott személyes adatok kezeléséért. Az EU–USA adatvédelmi keretben részt vevő szervezet marad a felelős az elvek alapján, amennyiben a megbízottja ezen személyes adatokat nem az elveknek megfelelően kezeli, kivéve, ha a szervezet bizonyítja, hogy nem felelős a károkozást előidéző eseményért.

e. Ha valamely szervezettel szemben nemteljesítés miatt bírósági végzést adnak ki vagy az elvekben vagy az elvek valamely jövőbeli mellékletében felsorolt, egyesült államokbeli hatóság (pl. az FTC vagy a Közlekedési Minisztérium) ad ki ellene végzést nemteljesítés miatt, a szervezetnek közzé kell tennie a bíróság vagy az egyesült államokbeli hatóság számára benyújtott megfelelési vagy értékelési jelentés EU–USA adatvédelmi keretre vonatkozó minden részét, amennyiben az nem ellentétes a titoktartási előírásokkal. A Minisztérium egy kijelölt kapcsolattartó pontot létesített az adatvédelmi hatóságok számára az adatvédelmi keretben részt vevő szervezetek megfelelőségi problémáinak kezelésére. Az FTC és a Közlekedési Minisztérium elsőbbséggel vizsgálja a Minisztérium és az uniós tagállamok hatóságainak az elvek be nem tartása miatti megkereséseit, és a megkeresésekkel kapcsolatban megfelelő időben információt cserél a megkereső állami hatósággal, amennyiben az nem ellentétes a titoktartási korlátozásokkal.

III. KIEGÉSZÍTŐ ELVEK

1. Különleges adatok

a. A szervezet nem köteles kifejezett megerősítő hozzájárulást (opt-in) beszerezni a különleges adatokra vonatkozóan, ha az adatkezelés:

i. az érintett vagy más személy létfontosságú érdekében áll;

ii. jogi igények előterjesztéséhez vagy védelméhez szükséges;

iii. egészségügyi ellátás vagy diagnózis nyújtásához szükséges;

iv. politikai, filozófiai, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármilyen más nonprofit szerv törvényes tevékenysége során történik, és azzal a feltétellel, hogy a kezelés kizárólag a szerv tagjaira vagy olyan személyekre vonatkozik, akik a céljaival összefüggésben rendszeres kapcsolatban állnak az adott szervvel, és az adatokat az érintettek beleegyezése nélkül nem adják át harmadik félnek;

v. a szervezetnek a foglalkoztatási jog területén fennálló kötelezettségeinek a végrehajtása céljából szükséges; vagy

vi. olyan adatokra vonatkozik, amelyeket az egyén kifejezetten nyilvánosságra hozott.

2. Újságírói kivételek

a. Tekintve a sajtószabadságnak az Egyesült Államok alkotmányában biztosított védelmét, amennyiben az Egyesült Államok alkotmányának első kiegészítésében szereplő, sajtószabadságra vonatkozó jog ütközik az adatvédelem érdekeivel, az első alkotmánykiegészítésnek kell szabályoznia ezen érdekek egyeztetését, tekintettel az egyesült államokbeli személyek vagy szervezetek tevékenységére.

b. A közzétételre, rádió- vagy televíziós műsorhoz vagy újságírói anyag nyilvános közlésének más formájához összegyűjtött személyes adatokra – akár felhasználják azokat, akár nem –, valamint a korábban közzétett anyagban talált, médiaarchívumból terjesztett információkra nem vonatkoznak az elvek követelményei.

3. Mögöttes felelősség

a. Az internetszolgáltatók, a távközlési szolgáltatók és más szervezetek nem felelősek az elvek alapján, amikor más szervezet nevében csupán közlik, továbbítják, átirányítják vagy tárolják az információt. Az EU–USA adatvédelmi keret nem keletkeztet mögöttes felelősséget. Amennyiben a szervezet a harmadik fél által továbbított adatok tekintetében csupán egyszerű továbbítást végez, és nem határozza meg e személyes adatok kezelésének céljait és eszközeit, nem felelős.

4. **Átvilágítás és auditálás végzése**

a. A könyvvizsgálók és befektetési bankárok tevékenységei magukban foglalhatják a személyes adatok feldolgozását az egyén beleegyezése vagy tudta nélkül. Ezt lehetővé teszik a tájékoztatásra, a választási lehetőségre és a hozzáférésre vonatkozó elvek az alább leírt körülmények között.

b. A nyilvánosan működő részvénytársaságok és a zártkörű részvénytársaságok – az adatvédelmi keretben részt vevő szervezeteket is beleértve – rendszeres auditáláson esnek át. Az ilyen auditálásokat – különösen az esetleges törvénysértést vizsgálókat – veszélyezteti, ha idő előtt közlik őket. Ugyanígy átvilágítást kell végez (tet)niük a lehetséges összeolvadásban vagy felvásárlásban érintett, az adatvédelmi keretben részt vevő szervezeteknek is. Ez gyakran személyes adatok – pl. felső vezetők vagy más fontos beosztású személyek adatai – gyűjtésével és kezelésével jár. A túl korai közlés akadályozhatná a tranzakciót, vagy akár az értékpapírokra vonatkozó előírásokat is sérthetné. A befektetési bankárok és az átvilágításban részt vevő ügyvédek, vagy az auditálást végző könyvvizsgálók az egyén tudta nélkül csak a törvényes vagy közérdekű követelményeknek való megfeleléshez szükséges mértékben és időtartamban kezelhetnek információt, és olyan más körülmények között, amelyek esetén ezen elvek alkalmazása sértené a szervezet jogos érdekeit. Ezek a jogos érdekek magukban foglalják a szervezetek jogi kötelezettségei és törvényes számviteli tevékenységei teljesítésének folyamatos ellenőrzését, és a lehetséges akvizíciókkal, összeolvadásokkal, közös vállalkozásokkal vagy a befektetési bankárok vagy könyvvizsgálók által végrehajtott más hasonló ügyletekkel kapcsolatos titoktartás szükségességét.

5. **Az adatvédelmi hatóságok szerepe**

a. A szervezetek az adatvédelmi hatóságokkal folytatott együttműködésre vonatkozó kötelezettségvállalásukat az alábbiakban leírt módon valósítják meg. Az EU–USA adatvédelmi keret alapján az EU-ból személyes adatokat fogadó egyesült államokbeli szervezeteknek kötelezettséget kell vállalniuk az elvek teljesítését biztosító hatékony mechanizmusok alkalmazására. Konkrétabban, a jogorvoslat, jogérvényesítés és felelősség elvének megfelelően a részt vevő szervezeteknek gondoskodniuk kell a következőkről: a) i. jogorvoslati lehetőség azon egyének számára, akikre az adatok vonatkoznak, a) ii. eljárások annak ellenőrzésére, hogy az üzleti vállalkozások által az adatvédelmi gyakorlataikról készített tanúsítványok és állítások helytállóak-e, valamint a) iii. az elvek nem teljesítéséből eredő problémák orvoslására vonatkozó kötelezettségek, és a következmények az ilyen szervezetekre nézve. A szervezet eleget tehet a jogorvoslati, jogérvényesítési és felelősségi elv a) pontja i. és iii. alpontjának, ha elfogadja az adatvédelmi hatóságokkal történő együttműködésre vonatkozóan itt meghatározott előírásokat.

b. A szervezet kötelezi magát az adatvédelmi hatóságokkal történő együttműködésre azáltal, hogy az EU–USA adatvédelmi keret öntanúsítási beadványában bejelenti a Minisztériumnak (*lásd*: öntanúsításról szóló kiegészítő elv), hogy a szervezet:

i. elhatározza, hogy az adatvédelmi hatóságokkal történő együttműködés révén eleget tesz a jogorvoslati, jogérvényesítési és felelősségi elv a) pontja i. és iii. alpontjában meghatározott követelménynek;

ii. együttműködik az adatvédelmi hatóságokkal az elvek hatálya alá tartozó panaszok kivizsgálásában és megoldásában; valamint

iii. betartja az adatvédelmi hatóságoktól kapott valamennyi ajánlást, amennyiben az adatvédelmi hatóságok úgy látják, hogy a szervezetnek különleges intézkedést kell hoznia az elveknek való megfeleléshez, beleértve a jogorvoslati vagy kártérítési intézkedéseket az elvek nemteljesítése által érintett egyének javára, és írásban erősíti meg az adatvédelmi hatóságok felé az ilyen intézkedés megtörténtét.

c. Adatvédelmi hatósági testületek működése

i. Az adatvédelmi hatóságok együttműködése tájékoztatás és tanácsadás formájában, a következőképpen valósul meg:

1. Az adatvédelmi hatóságok tanácsadását az adatvédelmi hatóságok európai uniós szinten létrehozott nem hivatalos testülete biztosítja, amely többek között segíti az összehangolt és koherens megközelítés biztosítását.

2. A testület ajánlást ad ki az érintett egyesült államokbeli szervezeteknek az EU-ból az EU–USA adatvédelmi keret alapján továbbított személyes adatok kezelésével kapcsolatos, magánszemélyektől származó megoldatlan panaszokkal kapcsolatban. Ez az ajánlás az elvek helyes alkalmazását hivatott biztosítani, és magában foglal bármilyen, az érintett egyén(ek)re vonatkozó jogorvoslatot, amelyet az adatvédelmi hatóságok megfelelőnek tartanak.

3. A testület ilyen ajánlást az érintett szervezetek megkeresésére és/vagy a közvetlenül az egyénektől érkező, olyan szervezetek elleni panaszokra válaszul ad ki, amelyek az EU–USA adatvédelmi keret céljainak megfelelően elkötelezték magukat az adatvédelmi hatóságokkal történő együttműködés mellett, miközben ösztönzi ezen egyéneket és szükség esetén segíti őket abban, hogy először a szervezet belső panaszkezelési eljárásait vegyék igénybe, ha vannak ilyenek.

4. Az ajánlást csak azután adják ki, hogy a jogvitában érdekelt mindkét fél megfelelő lehetőséget kapott észrevételeinek előterjesztésére és a bemutatni kívánt bizonyítékok benyújtására. A testület törekszik arra, hogy a jogszerű eljárásra vonatkozó követelményhez mérten a lehető leggyorsabban kiadja az ajánlást. Általános szabályként a testület arra törekszik, hogy a panasz vagy megkeresés kézhezvételét követő 60 napon belül – illetve, ha lehetséges, ennél gyorsabban – kiadja az ajánlást.

5. A testület közzéteszi a hozzá benyújtott panaszok vizsgálatának eredményeit, ha azt helyénvalónak találja.

6. Az ajánlás testület általi kiadása semmilyen kötelezettséget nem ró a testületre vagy az egyes adatvédelmi hatóságokra.

ii. A fentiek szerint a vitarendezésre ezt a lehetőséget választó szervezeteknek vállalniuk kell, hogy betartják az adatvédelmi hatóságok ajánlását. Ha a szervezet az ajánlás kiadásától számított 25 napon belül nem tesz eleget az ajánlásban foglaltaknak, és a késedelmet nem indokolja megfelelően, a testület értesítést küld azon szándékáról, hogy az ügyet az FTC, a Közlekedési Minisztérium vagy az Egyesült Államok más szövetségi vagy állami testülete elé vigye, amely végrehajtási hatáskörrel rendelkezik csalás vagy megtévesztés esetén, vagy hogy megállapítsa, hogy az együttműködési megállapodást súlyosan megszegték, és ezért azt semmisnek kell tekinteni. Az utóbbi esetben a testület tájékoztatja a Minisztériumot annak érdekében, hogy az EU–USA adatvédelmi keretben részt vevő szervezetek listáját megfelelően módosíthassák. Az adatvédelmi hatóságokkal történő együttműködésre vonatkozó kötelezettségvállalás bármilyen nemteljesítése, valamint az elvek be nem tartása a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza (15 U.S.C. § 45), a 49 U.S.C. § 41712 vagy más hasonló törvény alapján megtévesztő gyakorlatként perelhető.

d) Ha a szervezet azt kívánja, hogy az EU–USA adatvédelmi keret előnyei kiterjedjenek a munkaviszony keretében az EU-ból továbbított humánerőforrás-adatokra is, akkor kötelezettséget kell vállalnia, hogy együttműködik az adatvédelmi hatóságokkal az ilyen adatokkal kapcsolatban (lásd a humánerőforrás-adatokra vonatkozó kiegészítő elvet).

e) Az ezt a lehetőséget választó szervezeteknek éves díjat kell fizetniük, amely a testület működési költségeinek fedezésére szolgál. Ezenkívül felkérhetik őket arra, hogy fedezzék a velük kapcsolatos megkeresések vagy panaszok vizsgálóbizottság általi elbírálásából eredő összes fordítási költséget. A díj összegét a Minisztérium határozza meg a Bizottsággal folytatott konzultációt követően. A díj beszedését a Minisztérium által az e célból beszedett pénzeszközök kezelőjeként kiválasztott harmadik személy végezheti. A Minisztérium szorosan együttműködik a Bizottsággal és az adatvédelmi hatóságokkal a díj formájában beszedett pénzeszközök elosztására vonatkozó megfelelő eljárások kialakításában, valamint a testület egyéb eljárási és adminisztratív kérdéseiben. A Minisztérium és a Bizottság megállapodhat a díj beszedési gyakoriságának megváltoztatásáról.

6. **Öntanúsítás**

a. Az EU–USA adatvédelmi keret előnyei attól a naptól fogva biztosítottak a szervezet számára, amikor a Minisztérium felveszi a szervezetet az adatvédelmi keretben részt vevő szervezetek listájára. A Minisztérium csak azt követően veszi fel a szervezetet az adatvédelmi keretben részt vevő szervezetek listájára, hogy megállapította, hogy a szervezet eredeti öntanúsítási beadványa hiánytalan, és törli a szervezetet a listáról, ha az önkéntesen kilép az adatvédelmi keretből, elmulasztja éves újratanúsítását, vagy ismétlődően nem tartja be az elveket (*lásd* a vitarendezésre és a végrehajtásra vonatkozó kiegészítő elvet).

b. Az EU–USA adatvédelmi keretben való részvételhez szükséges kezdeti öntanúsításhoz vagy az újratanúsításhoz a szervezetnek minden alkalommal be kell nyújtania a Minisztériumnak egy beadványt ([8]) az elveknek való megfelelést öntanúsító vagy (adott esetben) újratanúsító szervezet nevében eljáró vállalati tisztviselő által, amely legalább a következő információkat tartalmazza:

([8]) A beadványt a Minisztérium adatvédelmi keretre vonatkozó honlapján keresztül kell benyújtania egy olyan, a szervezeten belüli személynek, aki jogosult a szervezet és annak bármely érintett szervezete nevében eljárni az elvek betartásával kapcsolatban.

i. az öntanúsító vagy újratanúsító egyesült államokbeli szervezet neve, valamint azon egyesült államokbeli szervezeteinek vagy leányvállalatainak neve, amelyek szintén betartják az elveket, és amelyekre a szervezet ki kívánja terjeszteni a részvételt;

ii. a szervezet által az EU-ból az EU–USA adatvédelmi keret alapján kapott személyes adatok tekintetében végzett tevékenységek leírása;

iii. a szervezet ezen személyes adatokra vonatkozó adatvédelmi szabályzatának leírása, beleértve a következőket:

1. ha a szervezetnek van nyilvános honlapja, akkor a honlap címe, ahol az adatvédelmi szabályzat elérhető, vagy ha a szervezet nem rendelkezik nyilvános honlappal, akkor a hely, ahol megtekinthető az adatvédelmi szabályzat a nyilvánosság számára; valamint

2. az adatvédelmi szabályzat bevezetésének tényleges időpontja;

iv. a panaszokat, hozzáférési kérelmeket és az elvekkel kapcsolatban felmerülő bármilyen kérdést kezelő kapcsolattartó iroda ([9]), beleértve a következőket:

1. a szervezeten belüli érintett személy(ek) vagy kapcsolattartó iroda (irodák) neve(i), beosztása(i), (adott esetben), e-mail-címe(i) és telefonszáma(i); valamint

2. a szervezet megfelelő egyesült államokbeli levelezési címe;

v. az az állami szerv, amelynek hatásköre van a szervezet ellen esetleges tisztességtelen vagy megtévesztő gyakorlat, valamint az adatvédelmet szabályozó törvények és rendeletek megsértése ügyében benyújtott panaszok kivizsgálására (és amely szerv az elvekben vagy az elvek jövőbeli mellékletében fel van sorolva);

vi. bármely olyan adatvédelmi program neve, amelynek a szervezet tagja;

vii. az ellenőrzés módja (azaz önértékelés; vagy külső megfelelőségi felülvizsgálatok, beleértve az ilyen vizsgálatokat végző harmadik felet is) ([10]); valamint

viii. az elvekkel kapcsolatos megoldatlan panaszok kivizsgálására rendelkezésre álló független jogorvoslati mechanizmus(ok) ([11]).

c. Amennyiben a szervezet az EU–USA adatvédelmi keret előnyeit ki akarja terjeszteni az Európai Unióból átadott, a munkaviszonnyal összefüggésben felhasználásra kerülő humánerőforrás-adatokra, ezt akkor teheti meg, ha van olyan, az elvekben vagy az elvek jövőbeli mellékletében felsorolt hatósági szerv, amely joghatósággal bír a szervezet ellen humánerőforrás-adatok kezelésével kapcsolatban felmerülő panaszok kivizsgálására. Ezen túlmenően a szervezetnek ezt jeleznie kell az első öntanúsítási beadványában és minden újratanúsítási beadványában, és ki kell jelentenie az EU érintett hatóságával vagy hatóságaival való együttműködésre vonatkozó kötelezettségvállalását a humánerőforrás-adatokra és az adatvédelmi hatóságok szerepére vonatkozó kiegészítő elvnek megfelelően (amelyik alkalmazandó), valamint azt, hogy követi a szóban forgó hatóságok ajánlását. A szervezetnek át kell adnia a Minisztérium számára a humán erőforrásra vonatkozó adatvédelmi szabályzatának egy példányát, és tájékoztatást kell adnia arról, hol tekinthető meg az adatvédelmi szabályzat az érintett alkalmazottai számára.

([9]) Az elsődleges „szervezeti kapcsolattartó” vagy a „szervezeti tisztviselő” nem lehet a szervezeten kívül (*pl.* külső jogtanácsos vagy tanácsadó).

([10]) *Lásd* az ellenőrzésre vonatkozó kiegészítő elvet.

([11]) *Lásd* a vitarendezésre és a végrehajtásra vonatkozó kiegészítő elvet.

d. A Minisztérium fenntartja és nyilvánosan hozzáférhetővé teszi azon, az adatvédelmi keretben részt vevő szervezetek listáját, amelyek hiánytalanul benyújtották első öntanúsítási beadványukat, és ezt a listát a hiánytalanul kitöltött, éves újratanúsítási beadványok, valamint a vitarendezésre és jogérvényesítésre vonatkozó kiegészítő elv alapján kapott értesítések alapján frissíti. Az ilyen újratanúsítási beadványokat legalább évente be kell nyújtani; ellenkező esetben a szervezetet törlik az adatvédelmi keretben részt vevő szervezetek listájáról, és nem részesülhet az EU–USA adatvédelmi keret előnyeiből. A Minisztérium által az adatvédelmi keretben részt vevő szervezetek listájára felvett valamennyi szervezetnek megfelelő adatvédelmi szabályzattal kell rendelkeznie, amely megfelel a tájékoztatás elvének, és ebben az adatvédelmi szabályzatban ki kell jelentenie, hogy betartja az elveket ([12]). Ha a szervezet adatvédelmi szabályzata online elérhető, tartalmaznia kell a Minisztériumnak az adatvédelmi keretre vonatkozó honlapjára mutató hiperhivatkozást, valamint az elvekkel kapcsolatos megoldatlan panaszoknak – az egyén számára térítésmentes – kivizsgálására rendelkezésre álló független jogorvoslati mechanizmus honlapjára vagy panaszbenyújtási formanyomtatványára mutató hiperhivatkozást.

e. Az elvek az öntanúsítást követően azonnal alkalmazandók. Azoknak a részt vevő szervezeteknek, amelyek korábban az EU–USA adatvédelmi pajzs keretrendszer elveinek való megfelelésüket öntanúsították, naprakésszé kell tenniük adatvédelmi szabályzatukat, hogy az ezentúl az „EU–USA adatvédelmi keret elveire" hivatkozzon. Az ilyen szervezetek ezt a hivatkozást a lehető leghamarabb, de legkésőbb az EU–USA adatvédelmi keret elvei hatálybalépésének időpontjától számított három hónapon belül feltüntetik.

f. A szervezetnek alkalmaznia kell az elveket valamennyi személyes adatra, amelyet az Európai Uniótól az EU–USA adatvédelmi keretben kapott. Az elvek betartására vonatkozó kötelezettségvállalást nem kötik időkorláthoz az azon idő alatt fogadott személyes adatok tekintetében, amíg a szervezet élvezi az EU–USA adatvédelmi keret előnyeit; a szervezet kötelezettségvállalása azt jelenti, hogy továbbra is alkalmazza az elveket az ilyen adatok esetében mindaddig, amíg tárolja, felhasználja vagy nyilvánosságra hozza azokat, még akkor is, ha a későbbiekben bármilyen okból kilép az EU–USA adatvédelmi keretből. Annak a szervezetnek, amely ki kíván lépni az EU–USA adatvédelmi keretből, erről előzetesen értesítenie kell a Minisztériumot. Az értesítésnek tartalmaznia kell azt is, hogy a szervezet mit fog tenni az EU–USA adatvédelmi keret alapján kapott személyes adatokkal (*azaz* megőrzi, visszaszolgáltatja vagy törli-e az adatokat, és ha megőrzi őket, akkor fel kell tüntetni azokat az engedélyezett eszközöket, amelyekkel az adatok védelmét biztosítja). Annak a szervezetnek, amely kilép az EU–USA adatvédelmi keretből, de meg akarja őrizni ezeket az adatokat, évente meg kell erősítenie a Minisztérium számára a kötelezettségvállalását, hogy továbbra is alkalmazza az elveket vagy más engedélyezett módon „megfelelő" védelmet nyújt az adatok számára (például olyan szerződés alkalmazásával, amely teljeskörűen tükrözi a megfelelő általános szerződési feltételeket, amelyeket a Bizottság elfogadott); ellenkező esetben a szervezetnek vissza kell küldenie vagy törölnie kell az adatokat ([13]). Annak a szervezetnek, amely kilép az EU–USA adatvédelmi keretből, törölnie kell a vonatkozó adatvédelmi szabályzatából az EU–USA adatvédelmi keretre való bármely hivatkozást, amely arra utal, hogy a szervezet továbbra is aktívan részt vesz az EU–USA adatvédelmi keretben, és jogosult annak előnyeire.

([12]) Az első alkalommal öntanúsító szervezet mindaddig nem tüntetheti fel a végleges adatvédelmi szabályzatában az EU–USA adatvédelmi keretben való részvételét, amíg a Minisztérium nem értesíti a szervezetet arról, hogy ezt megteheti. A szervezetnek az első öntanúsítási beadványa benyújtásakor be kell nyújtania a Minisztériumnak az adatvédelmi szabályzata tervezetét, amelynek meg kell felelnie az elveknek. Miután a Minisztérium megállapította, hogy a szervezet első öntanúsítási beadványa egyébként hiánytalan, értesíti a szervezetet, hogy véglegesítenie kell (pl. adott esetben közzé kell tennie) az EU–USA adatvédelmi keretnek megfelelő adatvédelmi szabályzatát. A szervezetnek haladéktalanul értesítenie kell a Minisztériumot a vonatkozó adatvédelmi szabályzat véglegesítéséről, amely időpontban a Minisztérium felveszi a szervezetet az adatvédelmi keretben részt vevő szervezetek listájára.

([13]) Ha egy szervezet a kilépése időpontjában úgy dönt, hogy megőrzi az EU–USA adatvédelmi keret alapján kapott személyes adatokat, és évente megerősíti a Minisztérium felé, hogy továbbra is alkalmazza az elveket ezekre az adatokra, a szervezetnek a kilépését követően évente egyszer igazolnia kell a Minisztériumnak (azaz, ha és amíg a szervezet más engedélyezett módon „megfelelő" védelmet nem biztosít az ilyen adatok számára, vagy vissza nem küldi vagy törli az összes ilyen adatot, és erről értesíti a Minisztériumot), hogy mit tett ezekkel a személyes adatokkal, mit fog tenni a továbbra is megőrzött személyes adatokkal, és ki szolgál majd folyamatos kapcsolattartási pontként az elvekkel kapcsolatos kérdésekben.

g. Annak a szervezetnek, amely a társasági jogállásának megváltozása, például összeolvadás, felvásárlás, csőd vagy megszűnés eredményeként megszűnik önálló jogi személyként létezni, előzetesen értesítenie kell a Minisztériumot erről. Az értesítésben azt is jelezni kell, hogy a társasági jogállás megváltozása után létrejövő szervezet i. meglévő öntanúsítás révén továbbra is részt vesz-e az EU–USA adatvédelmi keretben, ii. az EU–USA adatvédelmi keret új résztvevőjeként öntanúsítást végez (pl. ha az új jogalany vagy a túlélő jogalany még nem rendelkezik olyan meglévő öntanúsítással, amely révén részt vehetne az EU–USA adatvédelmi keretben), vagy iii. egyéb biztosítékokat, például írásbeli megállapodást vezet be, amely biztosítja az elvek folyamatos alkalmazását a szervezet által az EU–USA adatvédelmi keretben kapott és megőrzött személyes adatokra. Amennyiben sem az i., sem a ii. és sem a iii. alpont nem alkalmazandó, az EU–USA adatvédelmi keretben megszerzett valamennyi személyes adatot haladéktalanul vissza kell szolgáltatni vagy törölni kell.

h. Annak a szervezetnek, amely bármely okból kilép az EU–USA adatvédelmi keretből, törölnie kell minden olyan állítást, amely arra utal, hogy a szervezet továbbra is részt vesz az EU–USA adatvédelmi keretben, vagy jogosult annak előnyeire. Az EU–USA adatvédelmi keret tanúsító védjegyét, amennyiben használták, szintén törölni kell. Ha a szervezet hamisan tájékoztatja a közvéleményt az elvek betartásával kapcsolatban, a szervezet az FTC, a Kereskedelmi Minisztérium vagy más illetékes kormányzati szerv részéről perelhető. A Minisztériumnak adott megtévesztő közlések a hamis nyilatkozatokról szóló törvény (18 U. S. C. § 1001) alapján perelhetők.

7. **Ellenőrzés**

a. A szervezeteknek gondoskodniuk kell nyomonkövetési eljárásokról annak az ellenőrzésére, hogy azok a tanúsítások és állítások, amelyeket az EU–USA adatvédelmi keret szerinti adatvédelmi gyakorlatukról készítenek, megfelelnek-e a valóságnak, és megvalósításuk a tényállításokkal és az elvekkel összhangban történik-e.

b. Ahhoz, hogy a jogorvoslati, végrehajtási és felelősségi elv ellenőrzési követelményeinek megfeleljen, a szervezetnek az ilyen tanúsításokat és állításokat vagy önértékeléssel, vagy külső megfelelőségi felülvizsgálati eljárásokkal kell ellenőriznie.

c. Amennyiben a szervezet az önértékelést választotta, ennek az ellenőrzésnek bizonyítania kell, hogy az EU-ból kapott személyes adatokra vonatkozó adatvédelmi szabályzata pontos, átfogó, könnyen hozzáférhető, megfelel az elveknek, és azt teljes mértékben végrehajtják (azaz betartják). Azt is jeleznie kell, hogy az egyének tájékoztatást kapnak bármely belső panaszkezelési szabályzatról és a független jogorvoslati mechanizmus(ok)ról, amelyen keresztül panaszt tehetnek; jeleznie kell továbbá, hogy tartalmaz a munkavállalók oktatására vonatkozó eljárást a végrehajtást illetően, valamint fegyelmi eljárásokat az adatvédelmi szabályzat követésének elmulasztása esetére; és tartalmaz belső eljárásokat a fentiek teljesítésének időszakos objektív vizsgálatára. Az önértékelés elvégzését hitelesítő nyilatkozatot a vállalkozás egy tisztségviselőjének vagy a szervezet más meghatalmazottjának kell aláírnia legalább évente egyszer, és az egyének kérelmére, illetve a meg nem felelésre vonatkozó vizsgálattal vagy panasszal összefüggésben hozzáférhetővé kell tennie.

d. Amennyiben a szervezet külső megfelelőségi felülvizsgálatot választotta, ennek az ellenőrzésnek bizonyítania kell, hogy az EU-ból kapott személyes adatokra vonatkozó adatvédelmi szabályzata pontos, átfogó, könnyen hozzáférhető, megfelel az elveknek, és azt teljes mértékben végrehajtják (azaz betartják). Az ellenőrzésnek azt is jeleznie kell, hogy az egyének tájékoztatást kapnak azon mechanizmus(ok)ról, amely(ek)en keresztül panaszt tehetnek. A felülvizsgálat módszerei korlátozás nélkül magukban foglalhatják az ellenőrzést, szúrópróbaszerű felülvizsgálatokat, „csapdák” használatát, vagy adott esetben technikai eszközök használatát. A külső megfelelőségi felülvizsgálat sikeres elvégzését hitelesítő nyilatkozatot vagy a felülvizsgálatot végző személynek, vagy a vállalkozás valamelyik tisztségviselőjének vagy a szervezet más meghatalmazottjának kell aláírnia legalább évente egyszer, és az egyének kérésére, illetve megfeleléssel kapcsolatos vizsgálattal vagy panasszal összefüggésben rendelkezésre kell bocsátani.

e. A szervezeteknek meg kell őrizniük az EU–USA adatvédelmi keret szerinti adatvédelmi gyakorlatuk végrehajtásáról szóló nyilvántartásaikat, és kérésre, a megfelelés elmulasztására vonatkozó vizsgálattal vagy panasszal összefüggésben a panaszok kivizsgálásért felelős független szerv vagy a tisztességtelen és megtévesztő gyakorlatok esetében illetékes hivatal számára hozzáférhetővé kell tenniük. A szervezeteknek azonnal válaszolniuk kell az elvek általuk történő betartására vonatkozó minisztériumi megkeresésekre és más információkérésekre.

8. **Hozzáférés**

a. A hozzáférési elv a gyakorlatban

i. Az elvek alapján a hozzáférési jog az adatvédelem alapvető eleme. Különösen azt teszi lehetővé az egyének számára, hogy ellenőrizzék a velük kapcsolatban tárolt adatok pontosságát. A hozzáférési elv azt jelenti, hogy az egyénnek az alábbi jogai vannak:

1. visszajelzést kapni a szervezettől, hogy a szervezet kezel-e rá vonatkozó személyes adatokat ([14]);

2. közöljék vele az ilyen adatokat annak érdekében, hogy ellenőrizni tudja azok pontosságát és az adatkezelés jogszerűségét; valamint

3. az adatokat javíttathatja, módosíttathatja vagy töröltetheti, amennyiben azok pontatlanok vagy az elvek megsértésével kezelték azokat.

ii. Az egyéneknek azonban nem kell indokolniuk a személyes adataikhoz való hozzáférés iránti kérelmüket. Az egyének hozzáférés iránti kérésére reagálva a szervezeteknek először azt kell megtudniuk, hogy mi vezetett elsősorban a kérelemhez. Ha például a hozzáférési kérelem bizonytalan vagy túl általános területre vonatkozik, a szervezet párbeszédet kezdhet az egyénnel, hogy jobban megértse a kérelem indítékát és behatárolja a válaszinformációt. A szervezet kérdéseket tehet fel arra vonatkozóan, hogy az egyén a szervezet mely részével/részeivel állt kapcsolatban, illetve milyen jellegű az információ (vagy felhasználása), amely a hozzáférés iránti kérelem tárgyát képezi.

iii. A hozzáférés alapvető jellegének megfelelően a szervezeteknek mindig jóhiszeműen törekedniük kell a hozzáférés biztosítására. Ha például bizonyos adat védelemre szorul, és könnyen elkülöníthető más, a hozzáférés iránti kérelem tárgyát képező személyes adattól, a szervezetnek el kell takarnia a védett adatokat, és hozzáférhetővé kell tennie a többi adatot. Ha a szervezet úgy határoz, hogy a hozzáférést egy adott esetben korlátozni kell, a hozzáférést kérő egyén számára magyarázatot kell adnia a döntéséről, és a további megkeresésekhez egy kapcsolattartó pontot kell kijelölnie számára.

b) A hozzáférés biztosításának terhe vagy költsége

i. A személyes adatokhoz való hozzáférés joga csak kivételes körülmények esetén korlátozható, amennyiben ezzel más személy jogait érné sérelem, vagy ha az adott esetben a hozzáférés biztosításának terhe vagy költsége nem állna arányban az egyén adatvédelmi jogát érintő kockázattal. A költség és a teher fontos tényezők, amelyeket figyelembe kell venni, de nem meghatározó tényezők annak megállapításában, hogy a hozzáférés biztosítása indokolt-e.

ii. Ha például a személyes adatot olyan döntésekre használják, amelyek jelentős hatással vannak az egyénre (pl. fontos előnyök megtagadása vagy megadása, mint például biztosítás, jelzáloghitel vagy állás), akkor – e kiegészítő elvek más rendelkezéseivel összhangban – a szervezetnek akkor is közölnie kell az adatot, ha ez viszonylag bonyolult vagy költséges. Ha a kért személyes adat nem különleges adat, vagy azt nem olyan döntésekhez használják, amelyek jelentős hatással vannak az egyénre, ezzel szemben azonnal hozzáférhető, és biztosítása nem költséges, a szervezetnek biztosítania kell a hozzáférést az ilyen adatokhoz.

c) Bizalmas üzleti információk

i. A bizalmas kereskedelmi információ olyan információ, amelynek nyilvánosságra hozataltól való megvédésére a szervezet lépéseket tett, ha annak nyilvánosságra kerülése segítené a piaci versenytársat. A szervezet megtagadhatja vagy korlátozhatja a hozzáférést, amennyiben annak engedélyezése a fent meghatározott saját bizalmas kereskedelmi információját – mint például a szervezet által létrehozott marketingkövetkeztetéseket vagy osztályozásokat, vagy mások bizalmas kereskedelmi információját – feltárná, amennyiben az ilyen információ szerződéses titoktartási kötelezettség alá tartozik.

([14]) A szervezetnek válaszolnia kell az egyén arra vonatkozó kéréseire, hogy mi az adatkezelés célja, melyek az érintett személyesadat-kategóriák, valamint a címzettek vagy a címzettek kategóriái, akikkel az adatokat közlik.

ii. Amennyiben a bizalmas kereskedelmi információ könnyen elkülöníthető más, hozzáférés iránti kérelem tárgyát képező személyes adatoktól, a szervezetnek el kell takarnia a bizalmas kereskedelmi adatokat, és rendelkezésre kell bocsátania a nem bizalmas információt.

d) Adatbázisok létrehozása

i. A szervezet biztosíthat hozzáférést a megfelelő személyes adatoknak az egyén számára történő átadása formájában; nem követelmény az egyén hozzáférése a szervezet adatbázisához.

ii. A hozzáférés biztosítása csak azon a szinten szükséges, ahogyan a szervezet tárolja a személyes információt. Maga a hozzáférési elv nem jelent semmilyen kötelezettséget a személyesadat-állományok megőrzésére, karbantartására, újjászervezésére vagy átszerkesztésére.

e) Mikor korlátozható a hozzáférés

i. A szervezeteknek mindig jóhiszeműen törekedniük kell arra, hogy az egyéneknek hozzáférést biztosítsanak a személyes adataikhoz, a szervezetek csak meghatározott körülmények esetén korlátozhatják a hozzáférést, és a hozzáférés korlátozására vonatkozó indoknak mindig meghatározottnak kell lennie. Csakúgy mint a GDPR szerint, a szervezet korlátozhatja az adathoz való hozzáférést, amennyiben a megismerése valószínűleg fontos közérdekek – például nemzetbiztonság, honvédelem, közbiztonság – védelmével ütközne. Ezen túlmenően, amennyiben a személyes adatot kizárólag kutatási vagy statisztikai célokra dolgozzák fel, a hozzáférés megtagadható. A hozzáférés megtagadásának vagy korlátozásának más indokai:

1. a törvény végrehajtásába vagy érvényesítésébe, illetve magánkereseti jogalapokba való beavatkozás, beleértve a bűncselekmények megelőzését, kivizsgálását vagy felderítését, illetve a tisztességes eljáráshoz való jogot;

2. amennyiben felfedés esetén mások törvényes jogai vagy érdekei sérülnének;

3. törvényes vagy más szakmai kiváltság vagy kötelezettség megsértése;

4. munkavállalói biztonsági vizsgálatok vagy panaszeljárások, vagy a munkavállalói utánpótlás-tervezéssel és vállalkozás-átszervezésekkel kapcsolatos eljárások hátrányos befolyásolása; vagy

5. a megfelelő irányítással összefüggő folyamatos ellenőrzéssel, felülvizsgálattal vagy szabályozó funkciókkal összefüggésben vagy a jövőben vagy jelenleg folyamatban lévő, a szervezet részvételével zajló tárgyalások során szükséges titkosság hátrányos befolyásolása.

ii. A kivételre igényt tartó szervezetnek igazolnia kell annak szükségességét, és az egyének számára meg kell jelölni a hozzáférés korlátozásának indokait és a további megkeresésekhez a kapcsolattartási pontot.

f) Visszaigazoláshoz való jog és díj felszámításának joga a hozzáférés költségének fedezésére

i. Az egyénnek joga van visszaigazolást kérni arról, hogy a szervezetnek birtokában van-e rá vonatkozó személyes adat. Az egyénnek joga van a rá vonatkozó személyes adatokat megismerni. A szervezetek felszámíthatnak díjat, feltéve, hogy az nem túlzott.

ii. A díj felszámítása például akkor lehet indokolt, ha a hozzáférés kérése egyértelműen túlzott, különösen az ismétlődő jellege miatt.

iii. A hozzáférés nem utasítható vissza a költségre hivatkozva, ha az egyén felajánlotta a költségek megfizetését.

g) Ismétlődő vagy zaklató hozzáférési kérelmek

i. A szervezetek észszerű korlátokat határozhatnak meg arra, hogy adott időtartamon belül egy adott személy hozzáférési kérései hányszor teljesíthetők. Az ilyen korlátozások megállapításakor a szervezetnek figyelembe kell vennie az olyan tényezőket, mint az információ frissítésének gyakorisága, az adatok felhasználásának célja, valamint az információ jellege.

h) Hozzáférésre irányuló csalárd kérelem

i. A szervezet nem köteles a hozzáférést megadni addig, amíg nem rendelkezik elegendő információval ahhoz, hogy a kérelmező személyazonosságát megállapítsa.

i) Válaszadási határidő

i. A szervezetnek észszerű időn belül, észszerű módon válaszolnia kell a hozzáférésre irányuló kérelmekre – olyan formában, amely könnyen érthető az egyén számára. Az érintettek számára rendszeresen információt biztosító szervezet teljesítheti az egyén hozzáférésre irányuló kérelmét rendszeres adatszolgáltatással, ha az nem jelent túlzott késedelmet.

9. **Humánerőforrás-adatok**

a. Az EU–USA adatvédelmi keret általi lefedettség

i. Amennyiben az EU-ban letelepedett szervezet (korábbi vagy jelenlegi) munkavállalóiról a munkaviszonnyal kapcsolatban gyűjtött személyes adatokat továbbítja az EU–USA adatvédelmi keretben részt vevő, egyesült államokbeli anya- vagy leányvállalatnak vagy hozzá nem tartozó szolgáltatónak, a továbbítás élvezi az EU–USA adatvédelmi keret előnyeit. Ilyen esetekben az adatok gyűjtése és a továbbítást megelőző kezelése annak az uniós országnak a nemzeti joga alá tartozik, ahol azt összegyűjtötték, és tiszteletben kell tartani azon tagállam nemzeti jogának továbbításra vonatkozó feltételeit és korlátozásait.

ii. Az elvek kizárólag egyedileg azonosított vagy azonosítható adatok továbbítása vagy azokhoz való hozzáférés esetén alkalmazandók. Az összesített foglalkoztatási adatokra és a személyes adatokat nem tartalmazó vagy név nélküli adatok felhasználására támaszkodó statisztikai jelentés adatvédelmi aggályokra nem ad okot.

b. A tájékoztatásra és a választási lehetőségre vonatkozó elvek alkalmazása

i. Bármely egyesült államokbeli szervezet, amely az EU–USA adatvédelmi keret alapján az Európai Unióból munkavállalókra vonatkozó adatokat kapott, azt csak a tájékoztatásra és a választási lehetőségre vonatkozó elvvel összhangban fedheti fel harmadik fél számára vagy használhatja fel különböző célokra. Ha például egy szervezet a munkaviszonyon keresztül összegyűjtött személyes adatokat nem munkaviszonnyal összefüggő célokra – például marketingértesítésekre – szándékozik felhasználni, akkor az egyesült államokbeli szervezetnek ezt megelőzően biztosítania kell az előírt választási lehetőséget az érintett egyének számára, kivéve, ha azok már engedélyezték az adatok ilyen célú felhasználását. E felhasználás nem lehet összeegyeztethetetlen azokkal a célokkal, amelyek érdekében a személyes adatokat gyűjtötték, vagy amelyeket az egyén később engedélyezett. Ezenfelül az ilyen választási lehetőségeket tilos a foglalkoztatási lehetőségek korlátozására vagy az ilyen alkalmazottakkal szemben bármilyen megtorló intézkedés alkalmazására felhasználni.

ii. Meg kell jegyezni, hogy egyes általánosan alkalmazandó feltételek, melyek néhány EU tagállam esetében az onnan történő továbbításra vonatkoznak, kizárhatják az ilyen adatok felhasználását más célokra, még az EU-n kívülre történő továbbítást követően is, és az ilyen feltételeket tiszteletben kell tartani.

iii. Ezen túlmenően, a munkaadóknak észszerű erőfeszítéseket kell tenniük, hogy igazodjanak a munkavállalók adatvédelmi preferenciáihoz. Ez jelentheti például a személyes adatokhoz való hozzáférés korlátozását, bizonyos adatok névtelenítését, vagy kódok vagy álnevek hozzárendelését, ha az adott vállalatirányítási célhoz nincs szükség a valódi nevekre.

iv. Olyan mértékben és arra az időtartamra, amely annak érdekében szükséges, hogy a szervezet lehetőségei ne csorbuljanak az előléptetések, kinevezések vagy más hasonló foglalkoztatási döntések meghozatala során, a szervezet nem köteles felajánlani a tájékoztatást és a választási lehetőséget.

c. A hozzáférési elv alkalmazása

i. A hozzáférésről szóló kiegészítő elv útmutatást ad azokról az indokokról, amelyek igazolhatják a hozzáférés iránti kérelem megtagadását vagy korlátozását a humán erőforrások összefüggésében. Természetesen az Európai Unióban a munkaadóknak a helyi szabályozásnak kell megfelelniük, és biztosítaniuk kell, hogy az európai unióbeli alkalmazottak a saját országaik jogszabályaiban előírtaknak megfelelően hozzáférjenek az ilyen adatokhoz, az adatkezelés és -tárolás helyszínétől függetlenül. Az EU–USA adatvédelmi keret megköveteli, hogy az ilyen adatokat az Egyesült Államokban kezelő szervezet együttműködjön az ilyen hozzáférés biztosításában vagy közvetlenül, vagy az EU-beli munkáltatón keresztül.

d. Végrehajtás

i. Amennyiben a személyes adatokat csak a munkaviszonnyal összefüggésben használják fel, a munkavállalóval szemben az adatokért az elsődleges felelősség az EU-beli szervezeté marad. Ebből következik, hogy, amennyiben az európai munkavállalók adatvédelmi jogaik megsértésére vonatkozó panaszokkal élnek, és nincsenek megelégedve a belső felülvizsgálati, panasz- és fellebbezési eljárások (vagy egy szakszervezettel kötött szerződés alá tartozó bármilyen alkalmazható jogorvoslati eljárás) eredményeivel, akkor a munkavállaló munkahelye szerint illetékes állami vagy nemzeti adatvédelmi vagy munkaügyi hatósághoz kell irányítani őket. Ez magában foglalja azokat az eseteket is, amikor a személyes adat vélelmezett helytelen kezelésének a felelőssége azé az egyesült államokbeli szervezeté, amely az adatot a munkavállalótól kapta, ilyenformán az elvek vélelmezett megsértését jelenti. Ez lesz a leghatékonyabb módja a helyi munkajog és munkaügyi megállapodások, valamint az adatvédelmi jogszabályok által előírt, egymást gyakran átfedő jogok és kötelezettségek kezelésének.

ii. Ezért azon, az EU–USA adatvédelmi keretben részt vevő egyesült államokbeli szervezetnek, amely az Európai Unióból továbbított európai unióbeli humánerőforrás-adatokat használ fel a munkaviszonnyal összefüggésben, és amely az ilyen adattovábbításokat az EU–USA adatvédelmi keret hatálya alá kívánja helyezni, el kell köteleznie magát az EU illetékes hatóságai által elvégzett vizsgálatokban való együttműködésre, valamint azok ajánlásainak követésére az ilyen esetekben.

e. Az újbóli továbbításért való elszámoltathatóság elvének alkalmazása

i. Az EU–USA adatvédelmi keretben részt vevő szervezet foglalkoztatással kapcsolatos, az adatvédelmi keretrendszerben továbbított személyes adatokra vonatkozó alkalmi igényei esetén – pl. repülőút, szállodai szoba foglalása, biztosítás kötése – kisszámú munkavállaló személyes adatai továbbíthatók adatkezelők számára a hozzáférési elv alkalmazása nélkül vagy a harmadik fél adatkezelővel kötött szerződés nélkül (amit egyébként megkövetel az újbóli továbbításért való elszámoltathatóság elve), amennyiben a részt vevő szervezet betartotta a tájékoztatás és a választási lehetőség elvét.

10. **Újbóli továbbításra vonatkozó kötelező szerződések**

a. Adatkezelési szerződések

i. Amikor kizárólag kezelés céljából továbbítanak személyes adatokat az Európai Unióból az Egyesült Államokba, szükség van szerződésre, tekintet nélkül az adatfeldolgozó EU–USA adatvédelmi keretben való részvételére.

ii. Az EU-ban az adatkezelőktől mindig megkövetelik a szerződés megkötését, amikor pusztán adatkezelési célú továbbítás történik, akár az EU-n belül, akár azon kívül végzik el az adatkezelési műveletet, függetlenül attól, hogy az adatfeldolgozó részt vesz-e az EU–USA adatvédelmi keretben. A szerződés célja annak biztosítása, hogy az adatfeldolgozó:

1. kizárólag az adatkezelő utasítása alapján jár el;

2. megfelelő technikai és szervezési intézkedéseket tesz a személyes adatok véletlen vagy jogellenes megsemmisítése, véletlen elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés elleni védelme érdekében, és tudatában van, hogy az újbóli továbbítás engedélyezett-e; valamint

3. figyelembe véve az adatkezelés jellegét, segít az adatkezelőnek az elvek szerinti jogaikat gyakorló egyéneknek történő válaszadásban.

iii. Mivel a részt vevő szervezetek megfelelő védelmet biztosítanak, az ilyen szervezetekkel pusztán adatkezelés céljából kötött szerződésekhez nincs szükség előzetes engedélyre.

b) Adattovábbítás vállalatok vagy jogi személyek ellenőrzött csoportján belül

i. Amikor személyes adatokat továbbítanak vállalatok vagy jogi személyek ellenőrzött csoportján belül, nem mindig szükséges szerződés az újbóli továbbításért való elszámoltathatóság elve alapján. Vállalatok vagy jogi személyek ellenőrzött csoportján belül az adatkezelők az adattovábbítást más eszközök – köztük kötelező erejű uniós vállalati szabályok vagy más csoporton belüli eszközök (pl. megfelelőségi vagy ellenőrzési programok) – alapján is végezhetik, amelyek biztosítják a személyes adatok elvek szerinti védelmének folytonosságát. Ilyen adattovábbítás esetén a részt vevő szervezet marad a felelős az elveknek való megfelelésért.

c) Adatkezelők közötti adattovábbítás

i. Adatkezelők közötti adattovábbítás esetén a címzett adatkezelőnek nem kell az EU–USA adatvédelmi keretben részt vevő szervezetnek lennie, vagy rendelkeznie független jogorvoslati mechanizmussal. A részt vevő szervezetnek szerződést kell kötnie a címzett harmadik fél adatkezelővel, amely ugyanolyan szintű védelemről rendelkezik, mint amilyen az EU–USA adatvédelmi keretben rendelkezésre áll, de nem tartalmazza azt az előírást, hogy a harmadik fél adatkezelő részt vevő szervezet legyen vagy rendelkezzen független jogorvoslati mechanizmussal, feltéve, hogy elérhetővé tesz egy ezzel egyenértékű mechanizmust.

11. **Vitarendezés és végrehajtás**

a. A jogorvoslati, végrehajtási és felelősségi elv megállapítja az EU–USA adatvédelmi keret végrehajtására vonatkozó követelményeket. Az elv a) pontja ii. alpontja szerinti követelményeknek való megfelelést az ellenőrzésről szóló kiegészítő elv határozza meg. Ez a kiegészítő elv az a) pont i. és iii. alpontjával foglalkozik; mindkét esetben független jogorvoslati mechanizmusra van szükség. Ezek a mechanizmusok különböző formákat ölthetnek, de meg kell felelniük a jogorvoslati, végrehajtási és felelősségi elv követelményeinek. A szervezetek a követelményeknek a következőkön keresztül tesznek eleget: i. magánszektor által kifejlesztett olyan adatvédelmi programoknak való megfelelés, amelyek belefoglalják az elveket a szabályaikba, és a jogorvoslati, végrehajtási és felelősségi elvben leírt típusú, hatékony végrehajtási mechanizmusokat tartalmaznak, ii. megfelelés a törvényi vagy szabályozó felügyeleti hatóságoknak, amelyek rendelkeznek az egyedi panaszok kezeléséről és a jogviták megoldásáról, vagy iii. kötelezettségvállalás az EU-beli adatvédelmi hatóságokkal vagy azok meghatalmazott képviselőivel való együttműködésre.

b. E felsorolás példálózó, és nem korlátozó jellegű. A magánszektor a végrehajtás biztosítására további mechanizmusokat is kialakíthat, amennyiben azok megfelelnek a jogorvoslati, végrehajtási és felelősségi elv és a kiegészítő elvek követelményeinek. Meg kell jegyezni, hogy a jogorvoslati, végrehajtási és felelősségi elv követelményei kiegészítik azt a követelményt, hogy az önszabályozási erőfeszítéseknek végrehajthatónak kell lenniük az FTC-törvény (15 U.S.C. § 45.) tisztességtelen vagy megtévesztő cselekmények tilalmáról szóló 5. szakasza, vagy a Szövetségi Törvénykönyvnek a fuvarozók vagy jegyértékesítők által a légi közlekedés vagy a légi közlekedés értékesítése terén folytatott tisztességtelen vagy megtévesztő gyakorlatok tilalmáról szóló 49 U.S.C. 41712. §-a, vagy az ilyen cselekményeket tiltó más törvény vagy rendelet értelmében.

c. Az EU–USA adatvédelmi keret szerinti kötelezettségvállalásaik teljesítésének biztosítása és a program igazgatásának a támogatása érdekében a szervezeteknek, valamint a független jogorvoslati mechanizmusoknak – a Minisztérium kérésére – tájékoztatást kell nyújtaniuk az EU–USA adatvédelmi keretről. Ezenkívül valamennyi szervezetnek gyorsan kell válaszolnia az adatvédelmi hatóságok által a Minisztériumon keresztül az elvek betartására vonatkozóan benyújtott panaszokra. A válaszban szerepelnie kell annak, hogy a panasz érdemi-e, és amennyiben igen, akkor a szervezet hogyan fogja orvosolni a problémát. A Minisztérium az Egyesült Államok joga szerint védi az általa kapott információk titkosságát.

d. Jogorvoslati mechanizmusok

i. Az egyéneket arra kell ösztönözni, hogy szükség esetén az adott szervezettel kapcsolatban azelőtt emeljenek panaszt, hogy a független jogorvoslati mechanizmusokhoz fordulnának. A szervezeteknek a panasz kézhezvételétől számított 45 napon belül válaszolniuk kell az egyénnek. A jogorvoslati mechanizmus függetlensége olyan ténykérdés, amely különösen elfogulatlansággal, átlátható összetétellel és finanszírozással, valamint hitelesített nyomon követő nyilvántartással demonstrálható. A jogorvoslati, végrehajtási és felelősségi elvben megkövetelteknek megfelelően az egyének számára rendelkezésre álló jogorvoslatnak könnyen hozzáférhetőnek és az egyének számára ingyenesnek kell lennie. A független vitarendezési szerveknek az egyénektől átvett minden egyes panaszt ki kell vizsgálniuk, hacsak azok nem nyilvánvalóan alaptalanok vagy komolytalanok. Ez nem zárja ki eleve a jogosultsági követelmények megállapítását a jogorvoslati mechanizmust működtető független vitarendezési szerv részéről, de az ilyen követelményeknek átláthatónak és indokoltnak kell lenniük (például az olyan panaszok kizárása érdekében, amelyek a program hatályán kívül esnek, vagy amelyeket egy másik fórumon mérlegelnek), és nem érinthetik negatívan a jogos panaszok kivizsgálására vonatkozó kötelezettségvállalást. Ezen túlmenően, a jogorvoslati mechanizmusoknak az egyének számára a panasz benyújtásakor teljes és könnyen elérhető tájékoztatást kell nyújtaniuk a vitarendezési eljárás működéséről. E tájékoztatásnak ki kell terjednie a mechanizmus adatvédelmi gyakorlataira, összhangban az elvekkel. Szintén együtt kell működniük az eszközök – például a panasztételi formanyomtatványok – kidolgozásában, a panaszrendezési eljárás megkönnyítése érdekében.

ii. A független jogorvoslati mechanizmusok nyilvános honlapján tájékoztatást kell nyújtani az elvekről és az adott mechanizmus által az EU–USA adatvédelmi keretben nyújtott szolgáltatásokról. E tájékoztatásnak a következőket kell tartalmaznia: 1. az elvek független jogorvoslati mechanizmusokra vonatkozó követelményeire vonatkozó információk vagy az e követelményekre mutató hiperhivatkozás, 2. a Minisztérium adatvédelmi keretre vonatkozó honlapjára mutató hiperhivatkozás, 3. arra vonatkozó információ, hogy az EU–USA adatvédelmi keret szerinti vitarendezési szolgáltatásaik ingyenesek az egyének számára, 4. annak leírása, hogy az elvekkel kapcsolatos panaszok hogyan nyújthatók be, 5. az elvekkel kapcsolatos panaszok feldolgozásának határideje, és 6. a lehetséges jogorvoslatok körének leírása.

iii. A független jogorvoslati mechanizmusoknak éves jelentést kell közzétenniük, amely összesített statisztikákat tartalmaz a vitarendezési szolgáltatásaikra vonatkozóan. Az éves jelentésnek az alábbiakat kell tartalmaznia: 1. a jelentéstételi év folyamán beérkezett, az elvekkel kapcsolatos panaszok teljes száma, 2. a beérkezett panaszok típusa, 3. a vitarendezés minőségével kapcsolatos intézkedések, például a panaszok feldolgozásához igénybe vett idő hossza, valamint 4. a beérkezett panaszok eredménye, nevezetesen az alkalmazott jogorvoslatok és szankciók száma és típusa.

iv. Az I. mellékletben meghatározottak szerint az egyén igénybe vehet választottbíráskodást annak meghatározására – fennmaradó követelés esetén –, hogy az EU–USA adatvédelmi keretben részt vevő szervezet megsértette-e az elvek szerinti kötelezettségeit az adott egyénnel kapcsolatban, és az ilyen jogsértés teljesen vagy részlegesen orvoslás nélkül maradt-e. Ez a lehetőség csak ezekre a célokra áll rendelkezésre. Ez a lehetőség nem áll például rendelkezésre az elvek alóli kivételek esetében ([15]), vagy az EU–USA adatvédelmi keret megfelelőségére vonatkozó állítások tekintetében. E választottbíráskodási lehetőség keretében az EU–USA adatvédelmi kerettel foglalkozó testületnek (amely a felek megállapodása szerint egy–három választottbíróból áll) hatáskörében áll csak az adott egyén tekintetében egyénspecifikus, nem pénzbeli méltányos jogorvoslatot (pl. az egyén kérdéses adataihoz való hozzáférés, azok korrekciója, törlése vagy visszaadása) biztosítani, amely szükséges az elvek megsértésének orvoslásához. Az egyének és az EU–USA adatvédelmi keretben részt vevő szervezetek kérhetik az USA szövetségi választottbíráskodási törvénye alapján a választott bíróság határozatának bírósági felülvizsgálatát és végrehajtását.

e. Jogorvoslatok és szankciók

i. A független vitarendezési szerv által nyújtott bármilyen jogorvoslatnak azt kell eredményeznie, hogy a nemteljesítés hatását a szervezet visszafordítsa vagy kijavítsa, amennyiben ez megvalósítható, és a szervezet által a jövőben végzett adatkezelés összhangba kerüljön az elvekkel, valamint – adott esetben – a panaszt tevő egyén személyes adatainak kezelését szüntessék be. A szankcióknak kellőképpen szigorúaknak kell lenniük ahhoz, hogy biztosítsák az elvek szervezet általi betartását. A változó szigorúságú szankciók skálája a vitarendezési számára lehetővé teszi a nemteljesítés különböző fokozatainak megfelelő választ. A szankcióknak magukban kell foglalniuk a nemteljesítésre vonatkozó megállapítások közzétételét és

([15]) Az elvek, Áttekintés, 5. pont.

bizonyos körülmények között az adatok törlésére vonatkozó követelményt ([16]). Egyéb szankció lehet a jóváhagyás felfüggesztése és visszavonása, az egyének ellentételezése a nemteljesítés következtében felmerült veszteségekért és a felfüggesztő végzés. A magánfelek jogvitáit eldöntő vitarendezési szerveknek és az önszabályozó testületeknek értesíteniük kell a megfelelő joghatósággal rendelkező kormányzati szervet vagy adott esetben a bíróságokat, továbbá a Minisztériumot arról, hogy az EU–USA adatvédelmi keretben részt vevő szervezetek nem teljesítették a vitarendezési szerv határozatában foglaltakat.

f) A Szövetségi Kereskedelmi Bizottság (FTC) fellépése

i. Az FTC kötelezettséget vállalt arra, hogy soron kívül kivizsgálja az alábbi felektől kapott, az elvek állítólagos be nem tartásával kapcsolatos megkereséseket: i. adatvédelmi önszabályozó szervezetek és más független vitarendezési szervek, ii. uniós tagállamok, és iii. a Minisztérium, annak a meghatározására, hogy a Szövetségi Kereskedelmi Bizottságról szóló törvény tisztességtelen vagy megtévesztő kereskedelmi eljárások vagy gyakorlatok tiltásáról szóló 5. szakaszát megszegték-e. Ha az FTC arra a következtetésre jut, hogy okkal feltételezi, hogy az 5. szakaszt megszegték, megoldhatja az ügyet a kifogásolt gyakorlatot megtiltó, abbahagyásra kötelező határozattal, vagy panasz benyújtásával valamelyik szövetségi kerületi bírósághoz, amelynek az eredménye siker esetén az ugyanilyen tartalmú szövetségi bírósági végzés lehet. Ide tartozik az EU–USA adatvédelmi keret elvei teljesítésének vagy az EU–USA adatvédelmi keretben való részvételnek a hamis állítása olyan szervezetek részéről, amelyek vagy már nem szerepelnek az EU–USA adatvédelmi keretbe tartozó szervezetek listáján, vagy soha nem nyújtottak be öntanúsítást a Minisztériumhoz. Az FTC az adott magatartás beszüntetésére kötelező határozat megsértéséért polgári szankciókat eszközölhet ki, míg a szövetségi bírósági végzés megsértéséért polgári vagy bűnvádi engedetlenség címén indíthat pert. Az FTC értesíti a Minisztériumot bármilyen ilyen irányú fellépéséről. A Minisztérium arra ösztönzi az egyéb kormányzati szerveket, hogy értesítsék az ilyen megkeresésekre vonatkozó végleges intézkedésekről vagy az elvekhez való csatlakozást meghatározó más döntésekről.

g) Ismétlődő nemteljesítés

i. Ha egy szervezet ismétlődően nem teljesíti az elveket, tovább már nem jogosult az EU–USA adatvédelmi keret előnyeire. Az elveket ismétlődően nem teljesítő szervezeteket a Minisztérium törli az EU–USA adatvédelmi keretben részt vevő szervezetek listájáról, és vissza kell adniuk vagy törölniük kell azokat a személyes adatokat, amelyeket az EU–USA adatvédelmi keretben kaptak.

ii. Ismétlődő nemteljesítés áll fenn, ha a szervezet, amely önmaga tanúsította megfelelését a Minisztériumnak, megtagadja valamely adatvédelmi önszabályozó, független vitarendezési vagy kormányzati szerv végleges határozatának teljesítését, vagy az ilyen szerv – a Minisztériumot is beleértve – megállapítja, hogy a szervezet gyakran nem teljesíti az elveket, olyan mértékben, hogy a teljesítésre vonatkozó állítása már nem hihető. Abban az esetben, ha ezt a megállapítást a Minisztériumtól eltérő szerv teszi, a szervezetnek haladéktalanul értesítenie kell a Minisztériumot ezen tényekről. Ellenkező esetben a szervezet a hamis nyilatkozatokról szóló törvény (18 U. S. C. § 1001) alapján perelhető. Egy szervezet kilépése egy magánszektorbeli adatvédelmi önszabályozó programból vagy független vitarendezési mechanizmusból nem menti fel azon kötelezettsége alól, hogy megfeleljen az elveknek, és a megfelelés ismétlődő nemteljesítését jelenti.

iii. A Minisztérium törli a szervezetet az EU–USA adatvédelmi keretben részt vevő szervezetek listájáról ismétlődő nemteljesítés miatt, többek között abban az esetben, ha értesítést kap erről magától a szervezettől, egy adatvédelmi önszabályozó szervtől vagy más független vitarendezési szervtől vagy egy kormányzati szervtől, de csak azután, hogy először 30 napos határidővel értesítést küld erre vonatkozóan, és lehetőséget biztosít a nemteljesítő szervezet számára a válaszadásra ([17]). Ennek megfelelően a Minisztérium által fenntartott, az EU–USA adatvédelmi keretben részt vevő szervezetek listája egyértelműen mutatja, mely szervezetek élvezik és mely szervezetek nem élvezik már az EU–USA adatvédelmi keret előnyeit.

iv. Az EU–USA adatvédelmi keretben való részvételhez szükséges újraminősítés céljából egy önszabályozó szervben való részvételért folyamodó szervezetnek az EU–USA adatvédelmi keretben való előző részvételéről teljeskörűen tájékoztatnia kell az adott szervet.

([16]) A független vitarendezési szervek saját belátásuk szerint ítélhetik meg azokat a körülményeket, amelyek esetén ezeket a szankciókat alkalmazzák. Az érintett adatok különleges volta figyelembe veendő tényező annak eldöntésében, hogy elő kell-e írni az adatok törlését, mint ahogyan az is, hogy a szervezet az elvek durva áthágásával gyűjtött-e össze, használt-e fel vagy közölt adatokat.

([17]) A Minisztérium az értesítésben megjelöli azt az időtartamot – amely szükségszerűen kevesebb, mint 30 nap – amelyen belül a szervezetnek válaszolnia kell az értesítésre.

12. **Választási lehetőség – A kívülmaradás időzítése**

a. A választási lehetőség elvének célja alapvetően annak biztosítása, hogy a személyes adatot olyan módon használják, illetve közöljék, amely összhangban van az egyén elvárásaival és választásaival. Ennek megfelelően az egyénnek lehetősége kell hogy legyen bármikor kizárni azt, hogy a személyes adatot közvetlen üzletszerzési célra használják fel, a szervezet által megállapított észszerű határokon belül, azaz például időt adva a szervezetnek a kívülmaradás érvénybe léptetésére. A szervezet ezenkívül megkövetelheti a kívülmaradást kérő egyéntől a személyazonosság megállapításához elegendő információt. Az Egyesült Államokban az egyének ezzel a választási lehetőséggel egy központi „kívülmaradási" program révén élhetnek. Az egyén számára minden esetben könnyen hozzáférhető és megfizethető mechanizmust kell biztosítani e lehetőség gyakorlására.

b. Hasonlóképpen, a szervezet felhasználhatja az adatot bizonyos közvetlen értékesítési célokra, olyankor, amikor a gyakorlatban kivitelezhetetlen az egyén számára a kívülmaradási lehetőség megadása az adat felhasználása előtt, ha a szervezet ugyanakkor (és kérésre bármikor) haladéktalanul megadja az egyén számára azt a lehetőséget, hogy visszautasítsa (anélkül hogy ez számára költséget jelentene) minden további közvetlen marketingcélú kommunikáció fogadását, és a szervezet eleget tesz a személy kívánságának.

13. **Utazással kapcsolatos információk**

a. A légi utasok helyfoglalása és más utazási információi, mint például a törzsutasprogramra vagy a szállodafoglalásra, illetve a különleges kiszolgálási igényekre, mint például a vallási követelményeknek megfelelő ételekre vagy az esetleges fizikai segítségre vonatkozó információ különböző körülmények között továbbítható az EU-n kívül található szervezetek részére. Az általános adatvédelmi rendelet értelmében megfelelőségi határozat hiányában a személyes adatok akkor továbbíthatók harmadik országba, ha az általános adatvédelmi rendelet 46. cikke értelmében megfelelő adatvédelmi garanciákat biztosítanak, vagy konkrét helyzetekben akkor, ha az általános adatvédelmi rendelet 49. cikkében foglalt feltételek valamelyike teljesül (*pl.* ha az érintett kifejezetten hozzájárult az adattovábbításhoz). Az EU–USA adatvédelmi kerethez csatlakozó egyesült államokbeli szervezetek megfelelő védelmet biztosítanak a személyes adatok számára, és ezért az általános adatvédelmi rendelet 45. cikke alapján fogadhatnak az EU-ból továbbított adatokat anélkül, hogy az általános adatvédelmi rendelet 46. cikke szerinti, adattovábbításra vonatkozó jogi eszközt kellene bevezetniük, vagy teljesíteniük kellene az általános adatvédelmi rendelet 49. cikkében foglalt feltételeket. Mivel az EU–USA adatvédelmi keret a különleges adatok tekintetében specifikus szabályokat tartalmaz, az ilyen adatokat (amelyek összegyűjtésére például a vásárlók fizikai segítségre vonatkozó igényeivel összefüggésben lehet szükség) a részt vevő szervezetek számára történő adattovábbítások magukban foglalhatják. Az adatot továbbító szervezetnek azonban minden esetben tiszteletben kell tartania annak az EU-tagállamnak a jogszabályait, amelyben működik, amelyek többek között különleges feltételeket írhatnak elő a különleges adatok kezelésére vonatkozóan.

14. **Gyógyszeripari és gyógyászati termékek**

a. Az uniós tagállamok jogszabályainak, illetve az EU–USA adatvédelmi keret elveinek alkalmazása

i. A személyes adatok összegyűjtésére és bármilyen, az Egyesült Államokba történő továbbítást megelőző kezelésére az uniós/tagállami jogszabályokat kell alkalmazni. Amint az adatokat továbbították az Egyesült Államokba, az EU–USA adatvédelmi keret elvei vonatkoznak rájuk. A gyógyszeripari kutatásra és más célokra használt adatokat adott esetben anonimizálni kell.

b. Jövőbeli tudományos kutatások

i. A különleges orvosi vagy gyógyszeripari kutatások során felhasznált személyes adatok gyakran értékes szerepet játszanak a jövőbeli tudományos kutatásban. Amennyiben egy adott kutatásra összegyűjtött személyes adatokat az Egyesült Államok valamelyik EU–USA adatvédelmi keretben részt vevő szervezetéhez továbbítják, a szervezet felhasználhatja az adatokat egy új tudományos kutatási tevékenységhez, ha az első esetben megfelelő értesítést és választási lehetőséget biztosítottak. Az ilyen értesítésnek tájékoztatást kell adnia az adatok sajátos jövőbeli felhasználásairól: például időszakos nyomon követés, kapcsolódó tanulmányok vagy marketing.

ii. Magától értetődő, hogy az adatok összes jövőbeli felhasználása nem határozható meg pontosan, mivel az eredeti adatokkal kapcsolatos új meglátásokból új kutatási felhasználás, új orvosi felfedezések és előrelépések, illetve közegészségügyi és szabályozói fejlesztések keletkezhetnek. Ahol lehetséges, az értesítésnek ezért tartalmaznia kell egy magyarázatot arról, hogy a személyes adatokat jövőbeli, előre nem látható orvosi és gyógyszeripari kutatási tevékenységekben esetleg felhasználják. Ha a felhasználás nem összeegyeztethető azzal (azokkal) az általános kutatási cél(ok)kal, amelyekre a személyes adatokat eredetileg gyűjtötték, vagy amelyekhez az egyén utóbb hozzájárult, ismét kérni kell a beleegyezését.

c. Klinikai kísérletből való kilépés

i. A résztvevők bármikor dönthetnek a klinikai kísérletből való kilépés mellett, illetve felkérhetők a kilépésre. A kilépést megelőzően gyűjtött személyes adatokat a klinikai kísérlet részeként gyűjtött más adatokkal együtt még lehet kezelni, de csak abban az esetben, ha ezt az értesítésben egyértelműen a résztvevő tudtára adták, amikor beleegyezett a részvételbe.

d. Adattovábbítás szabályozási vagy felügyeleti célokra

i. A gyógyszeripari és orvostechnikai eszközt gyártó vállalkozások számára megengedett, hogy az Egyesült Államok szabályozó hatóságai számára szabályozási és felügyeleti célokból az EU-ban végzett klinikai kísérletekből származó személyes adatokat adjanak át. A szabályozó hatóságokon kívül más felek, mint például a vállalkozás telephelyei és más kutatóhelyek számára engedélyezettek hasonló továbbítások az értesítési és választási lehetőség elvnek megfelelően.

e. „Vak” kísérletek

i. Sok klinikai kísérletnél a tárgyilagosság biztosítása érdekében a résztvevők, és gyakran a vizsgálók számára sem adható hozzáférés az arra vonatkozó információhoz, hogy az egyes résztvevők milyen kezelést kapnak. Ha így tennének, az veszélyeztetné a kutatás és az eredmények érvényességét. Az ilyen (úgynevezett „vak”) klinikai kísérletek résztvevői számára nem kell hozzáférést biztosítani a saját kezelésükre vonatkozó adatokhoz a kísérlet során, ha ezt a korlátozást elmagyarázták, amikor a résztvevő belépett a kísérletbe, és az ilyen információ felfedése veszélyeztetné a kutatás integritását.

ii. A kísérletben e feltételek alapján történő részvételre vonatkozó megállapodás a hozzáférési jogról való indokolt lemondásnak tekintendő. A kísérlet befejezését és az eredmények elemzését követően a résztvevők kérésre hozzáférhetnek adataikhoz. Ezt elsősorban az orvostól vagy más egészségügyi szolgáltatótól kell kérniük, akitől a klinikai kísérleten belül a kezelést kapták, vagy másodsorban a támogató szervezettől.

f. Termékbiztonság és a hatékonyság ellenőrzése

i. A gyógyszeripari vagy orvostechnikai eszközt gyártó vállalatnak nem kell alkalmaznia az elveket a tájékoztatásra, a választási lehetőségre, az újbóli továbbításért való elszámoltathatóságra és a hozzáférésre vonatkozóan a termékbiztonságot és a hatékonyságot ellenőrző tevékenységeiben, beleértve a nemkívánatos események jelentését és a bizonyos gyógyszereket vagy orvostechnikai eszközöket használó betegek/alanyok megfigyelését, amennyiben az elvek betartása akadályozza a szabályozási követelményeknek való megfelelést. Ez egyaránt igaz mind az egészségügyi szolgáltatók jelentéseire a gyógyszeripari és orvostechnikai eszközt gyártó vállalkozások felé, mind pedig a gyógyszeripari és orvostechnikai eszközt gyártó vállalkozások jelentéseire a kormányzati ügynökségek – mint pl. a Szövetségi Élelmiszer- és Gyógyszerügyi Hivatal (FDA) – felé.

g. Egyedülálló módon és megváltoztathatatlanul kódolt adatok

i. A kutatási adatokat a kutatás vezetője egyedi módon és megváltoztathatatlanul kódolja azok keletkezésekor, hogy az egyéni érintettek személyazonosságát ne lehessen megismerni. Az ilyen kutatást támogató gyógyszeripari vállalkozások nem kapják meg a kulcsot. Az egyedülálló kóddal csak a kutató rendelkezik, annak érdekében, hogy különleges körülmények esetén (pl. ha utólagos orvosi ellenőrzésre van szükség) azonosíthassa a kutatási alanyt. Az ilyen módon kódolt adatok EU-ból az Egyesült Államokba történő továbbítása az elvek hatálya alá tartozik, ha uniós jog hatálya alá tartozó uniós személyes adatról van szó.

15. **Nyilvános nyilvántartás és nyilvánosan hozzáférhető információ**

a. A szervezetnek a nyilvánosan hozzáférhető forrásból származó személyes adatokra alkalmaznia kell a biztonságra, az adatok sértetlenségére és a célhoz kötöttségre, valamint a jogorvoslatra, végrehajtásra és felelősségre vonatkozó elveket. Ezeket az elveket kell alkalmazni a nyilvános nyilvántartásokból gyűjtött személyes adatokra is, *azaz* olyan nyilvántartásokból, amelyeket a kormányzati ügynökségek vagy bármilyen szintű jogi személyek tartanak fenn, amelyek általában nyitottak a betekintésre a nyilvánosság számára).

b. A tájékoztatás, a választási lehetőség és az újbóli továbbításért való elszámoltathatóság elvét nem szükséges alkalmazni a nyilvános nyilvántartásban lévő adatra mindaddig, amíg az nem kapcsolódik össze nem nyilvános nyilvántartásban lévő adattal, valamint amennyiben a vonatkozó joghatóság által a betekintésre megállapított feltételeket tiszteletben tartják. Általában nem szükséges a tájékoztatás, a választási lehetőség és az újbóli továbbításért való elszámoltathatóság elvét alkalmazni a nyilvánosan hozzáférhető adatokra, hacsak az európai átadó nem jelzi, hogy az ilyen adatok olyan korlátozások alá tartoznak, amelyek megkövetelik a szervezettől a fenti elvek alkalmazását a tervezett felhasználásokra. A szervezetek nem felelősek azért, hogy az adatokat hogyan használják fel azok, akik azokhoz nyilvánosságra hozott anyagokból jutnak hozzá.

c. Amennyiben egy szervezetről megállapították, hogy az elveket megsértve szándékosan hozott nyilvánosságra személyes adatokat annak érdekében, hogy ő vagy mások e kivételekből részesülhessenek, a továbbiakban nem jogosult az EU–USA adatvédelmi keret előnyeire.

d. A hozzáférés elvét nem szükséges alkalmazni a nyilvános nyilvántartásban lévő adatokra mindaddig, amíg azok nem kapcsolódnak össze más személyes adatokkal (kivéve a nyilvános nyilvántartásban lévő információ indexálásához vagy rendezéséhez használt kis mennyiségben); azonban a vonatkozó joghatóság által a betekintésre megállapított feltételeket tiszteletben kell tartani. Ha azonban a nyilvános adatokhoz (a fent kifejezetten említettektől eltérő) nem nyilvános adatok kapcsolódnak, a szervezetnek biztosítania kell az összes ilyen adathoz való hozzáférést – feltételezve, hogy az nem tartozik más engedélyezett kivételek közé.

e. Ugyanúgy, mint a nyilvános nyilvántartásokban tárolt adatok esetében, nem szükséges a nagyközönség számára már elérhető adatokhoz való hozzáférés biztosítása, amíg azokat nem kapcsolják össze nyilvánosan nem elérhető adatokkal. Azok a szervezetek, amelyek a nyilvánosan hozzáférhető adatok értékesítési üzletágában tevékenykednek, a hozzáférésre vonatkozó kérelmek megválaszolása során a szervezet szokásos díját számíthatják fel. Más megoldásként az egyének az adataikhoz való hozzáférést attól a szervezettől kérhetik, amely eredetileg gyűjtötte az adatokat.

16. **Közigazgatási szervek hozzáférési kérései**

a. A közigazgatási szervek személyes adatokhoz történő hozzáférésre vonatkozó jogszerű kérései átláthatóságának a biztosítása érdekében az EU–USA adatvédelmi keretben részt vevő szervezetek önkéntesen kiadhatnak rendszeres átláthatósági jelentéseket azoknak a személyes adatokhoz történő hozzáférésre vonatkozó kéréseknek a számáról, amelyeket közigazgatási szervektől kaptak bűnüldözési vagy nemzetbiztonsági okokból, amennyiben az ilyen adatközlést a vonatkozó jogszabályok megengedik.

b. A részt vevő szervezet által ezekben a jelentésekben nyújtott információ minden olyan más információval együtt, amelyet a hírszerző közösség adott ki más információkkal együtt, felhasználható az EU–USA adatvédelmi keret működéséről szóló közös időszakos áttekintés céljára az elveknek megfelelően.

c. A tájékoztatás elve a) pontja xii. alpontjának megfelelően a tájékoztatás hiánya nem akadályozza meg a szervezetet abban, valamint nem teszi képtelenné arra, hogy választ adjon a jogszerű kérésekre.

I. MELLÉKLET: VÁLASZTOTTBÍRÓSÁGI MODELL

A jelen I. melléklet meghatározza azokat a feltételeket, amelyek szerint az EU–USA adatvédelmi keretben részt vevő szervezetek kötelesek a követeléseket – a jogorvoslati, végrehajtási és felelősségi elv szerint – választottbíróság elé vinni. Az alább leírt kötelező erejű választottbírósági lehetőség az EU–USA adatvédelmi keret körébe tartozó adatokkal kapcsolatos bizonyos „fennmaradó követelésekre" vonatkozik. Ennek a lehetőségnek a célja azonnali, független és méltányos mechanizmus biztosítása az egyén kérésére az elvek olyan állítólagos megsértésének rendezésére, amelyet az EU–USA adatvédelmi keret többi mechanizmusa nem rendez.

A. **Hatály**

Ez a választottbírósági lehetőség az egyének rendelkezésére áll annak meghatározására fennmaradó követelések esetén, hogy a részt vevő szervezet megsértette-e az elvek szerint az adott egyénre vonatkozóan a kötelezettségeit, és az ilyen jogsértés teljesen vagy részlegesen orvoslás nélkül maradt-e. Ez a lehetőség csak ezekre a célokra áll rendelkezésre. Ez a lehetőség nem áll például rendelkezésre az elvek alóli kivételek esetében ([1]), vagy az EU–USA adatvédelmi keret megfelelőségére vonatkozó állítások tekintetében.

B. **Rendelkezésre álló jogorvoslatok**

E választottbíráskodási lehetőség keretében az EU–USA adatvédelmi keret választottbírói testületnek (választottbírói testület, amely a felek megállapodása szerint egy–három választott bíróból áll) hatáskörében áll csak az adott egyén tekintetében egyénspecifikus, nem pénzbeli méltányos jogorvoslatot (pl. az egyén kérdéses adataihoz való hozzáférés, azok korrekciója, törlése vagy visszaadása) biztosítani, amely szükséges az elvek megsértésének orvoslásához. Ez az EU–USA adatvédelmi kerettel foglalkozó testület egyetlen hatásköre a jogorvoslatok tekintetében. A jogorvoslatok elbírálásakor az EU–USA adatvédelmi kerettel foglalkozó testületnek figyelembe kell vennie az EU–USA adatvédelmi keretben más mechanizmusok által már biztosított jogorvoslatokat. Kártérítés, költségtérítés, díjfizetés vagy más jogorvoslatok nem állnak rendelkezésre. Mindegyik fél maga fizeti a saját ügyvédi költségét.

C. **Választottbíráskodás előtti követelmények**

Az ezzel a választottbírósági lehetőséggel élő egyénnek az alábbi lépéseket kell megtennie a választott bírósági kereset indítása előtt: 1. az állítólagos jogsértést közvetlenül a szervezetnek kell jeleznie, és lehetőséget kell biztosítania a szervezet számára a kérdés rendezésére a vitarendezési és végrehajtási kiegészítő elv d) pontjának i. alpontjában meghatározott határidőn belül, 2. az elvek szerinti független jogorvoslati mechanizmusok igénybevétele, amely az egyén számára ingyenes, és 3. a kérdés jelzése az egyén adatvédelmi hatóságán keresztül a Minisztériumnak, és lehetőség biztosítása a Minisztérium számára, hogy mindent megtegyen a kérdés rendezésére a Minisztérium Nemzetközi Kereskedelmi Igazgatóságának a levelében meghatározott határidőn belül – az egyén számára ingyenesen.

Ez a választottbírósági lehetőség nem vehető igénybe, ha az elveknek az egyén által említett állítólagos megsértése tárgyában 1. korábban már lefolytattak kötelező erejű választottbírósági eljárást, 2. az egyén részvételével folyó bírósági perben jogerős döntést hoztak, vagy 3. a felek azt már korábban rendezték. Ezenkívül ez a lehetőség nem alkalmazható, ha az adatvédelmi hatóság 1. az adatvédelmi hatóságok szerepére vonatkozó kiegészítő elv vagy a humánerőforrás-adatokra vonatkozó kiegészítő elv alapján hatáskörrel rendelkezik, vagy 2. felhatalmazással rendelkezik arra, hogy az állítólagos jogsértést közvetlenül a szervezettel rendezze. Az adatvédelmi hatóság azon hatásköre, hogy ugyanazt a keresetet az uniós adatkezelővel szemben rendezze, önmagában nem zárja ki ennek a választottbírósági lehetőségnek az alkalmazását egy másik jogi személlyel szemben, amelyre nem vonatkozik az adatvédelmi hatóság hatásköre.

D. **Az ítéletek kötelező ereje**

Az egyén azon döntése, hogy ezzel a választottbírósági lehetőséggel éljen, teljesen önkéntes. A választottbírósági ítélet a választottbírósági eljárásban részt vevő valamennyi félre nézve kötelező erejű. Az eljárás megindítása után az egyén lemond arról a lehetőségről, hogy ugyanarra az állítólagos jogsértésre más jóvátételt keressen más fórumon, azzal a kivétellel, hogy amennyiben a nem pénzbeli méltányos jóvátétel nem teljesen orvosolja az állítólagos jogsértést, akkor a választottbírósági eljárás egyén általi kezdeményezése nem zárja ki a kártérítés iránti követelést, amely egyébként bírósági úton elérhető.

([1]) Az elvek, Áttekintés, 5. pont.

E. **Felülvizsgálat és végrehajtás**

Az egyének és az EU–USA adatvédelmi keretben részt vevő szervezetek kérhetik az USA szövetségi választottbíráskodási törvénye alapján a választott bíróság határozatának bírósági felülvizsgálatát és végrehajtását ([2]). Az ilyen ügyeket a szövetségi kerületi bírósághoz kell benyújtani, amelynek területi illetékessége kiterjed a részt vevő szervezet üzleti tevékenységének elsődleges helyére is.

Ennek a választottbírósági lehetőségnek a célja egyéni viták rendezése, és a választottbírósági ítéleteknek nem célja, hogy megerősítő vagy kötelező erejű precedenst szolgáltassanak más felekkel kapcsolatos ügyekben, beleértve jövőbeli választott bírósági eljárásokat vagy uniós vagy egyesült államokbeli bíróságokat vagy FTC eljárásokat.

F. **A választottbírói testület**

A felek a választottbírák alább tárgyalt listájáról választják ki az EU–USA adatvédelmi keret választottbírói testületének választottbíráit.

A vonatkozó jogszabályokkal összhangban a Minisztérium és a Bizottság legalább 10 választottbírát tartalmazó listát állít össze, akiket a függetlenségük, a feddhetetlenségük és a tapasztalatuk alapján választanak ki. Erre a folyamatra az alábbiak vonatkoznak:

Választottbírák:

1. kivételes körülmények vagy indokolt eltávolítás hiányában 3 évig maradnak a listán, amely időszakot a Minisztérium a Bizottság előzetes értesítésével további 3 évre meghosszabbíthatja,

2. nem utasíthatja őket egyik fél vagy az EU–USA adatvédelmi keretben részt vevő szervezet, vagy az USA, az EU vagy bármely uniós tagállam vagy más kormányzati hatóság, közigazgatási szerv vagy végrehajtási hatóság sem, és nem kapcsolódhatnak az említettekhez, valamint

3. engedéllyel kell rendelkezniük az Egyesült Államokban történő jogi praktizálásra, és szakértőnek kell lenniük az Egyesült Államok adatvédelmi törvényét illetően, továbbá szakértelemmel kell rendelkezniük az uniós adatvédelmi jog területén.

([2]) A szövetségi választottbíráskodási törvény (a továbbiakban: FAA) 2. fejezete úgy rendelkezik, hogy „egy akár szerződéses, akár másmilyen jogviszonyból eredő választottbírósági megállapodás vagy választottbírósági ítélet, amely kereskedelmi jellegű, beleértve egy [az FAA 2. pontjában] leírt tranzakciót, szerződést vagy megállapodást, a külföldi választottbírósági ítéletek elismeréséről és érvényesítéséről szóló 1958. június 10-i egyezmény, 21 U.S.T. 2519, T.I.A.S. No. 6997 (»New York-i Egyezmény«) hatálya alá esik". 9 U.S.C.§ 202. Az FAA tovább úgy rendelkezik, hogy „egy ilyen jogviszonyból eredő megállapodás vagy ítélet, amely teljes egészében az Egyesült Államok polgárai között jön létre, nem esik a [New York-i] Egyezmény hatálya alá – kivéve, ha a jogviszony magában foglal külföldön levő ingatlant, célja külföldön történő teljesítés vagy végrehajtás, vagy más módon indokolt kapcsolatban áll egy vagy több más állammal". *Uo.* A 2. fejezetben „a választottbírósági eljárásban részt vevő bármelyik fél az e fejezet szerint hatáskörrel rendelkező bírósághoz fordulhat a választottbírósági eljárásban részt vevő másik féllel szemben hozott ítéletet megerősítő végzés érdekében. A bíróságnak meg kell erősítenie az ítéletet – kivéve, ha az említett [New York-i] Egyezményben az ítélet elismerésének vagy végrehajtásának elutasítására vagy elhalasztására meghatározott okok egyikét állapítja meg". Uo. 207. §. A 2. fejezet továbbá úgy rendelkezik, hogy „az Egyesült Államok kerületi bíróságainak […] van alapvetően hatáskörük […] egy [New York-i Egyezmény] szerinti kereset vagy eljárás esetén, függetlenül a vitatott összegtől". Uo. 203. §.
A 2. fejezet továbbá úgy rendelkezik, hogy „az 1. fejezet vonatkozik az e fejezet szerint indított keresetekre vagy eljárásokra, amennyiben az a fejezet nincs ellentétben ezzel a fejezettel vagy a [New York-i] Egyezménnyel, amelyet az Egyesült Államok ratifikált". Uo. 208. §. Az 1. fejezet viszont úgy rendelkezik, hogy „egy írásos rendelkezés az […] olyan kereskedelmi jellegű tranzakciót bizonyító szerződésben, amely választottbírósági úton rendez egy vitát, amely utólag abból a szerződésből vagy tranzakcióból ered, vagy a teljes vagy részleges végrehajtásának a megtagadását, vagy egy írásos megállapodást, amely szerint választott bírósági eljárást kezdeményeznek egy abból a szerződésből, tranzakcióból vagy megtagadásból eredő meglevő vita esetében, érvényes, visszavonhatatlan és érvényesíthető, kivéve a bármely szerződés hatályon kívül helyezésére jogszabály vagy méltányosság alapján rendelkezésre álló okokból". Uo. 2. §. Az 1. fejezet továbbá úgy rendelkezik, hogy „a választott bírósági eljárás bármelyik fele az így meghatározott bírósághoz fordulhat az ítélet megerősítése érdekében, és ezután a bíróság ilyen végzést adhat ki, kivéve, ha az ítéletet érvénytelenítik, módosítják vagy javítják az [FAA] 10. és 11. pontjában előírtak szerint". Uo. 9. §.

G. **Választottbírósági eljárás**

A Minisztérium és a Bizottság az alkalmazandó joggal összhangban megállapodott az EU–USA adatvédelmi kerettel foglalkozó testület előtti eljárásokra irányadó választottbírósági szabályok elfogadásáról ([3]). Abban az esetben, ha az eljárásra vonatkozó szabályokat meg kell változtatni, a Minisztérium és a Bizottság megállapodik abban, hogy módosítják ezeket a szabályokat, vagy adott esetben egyéb, már meglévő, jól bevált egyesült államokbeli választottbírósági eljárásokat fogadnak el, az alábbi megfontolások mindegyikének figyelembevételével:

1. A szervezetnek küldött értesítéssel az egyének kezdeményezhetnek kötelező erejű választottbírósági eljárást a fenti választottbírósági eljárásra vonatkozó előzetes követelmények teljesítése esetén. Az értesítésnek tartalmaznia kell a C bekezdés alapján a kereset rendezése érdekében tett lépések összefoglalását, az állítólagos jogsértés leírását és az egyén döntése szerint a keresetet alátámasztó dokumentumokat és anyagokat, illetve az állítólagos sérelemmel kapcsolatos jogi elemzést.

2. Eljárásokat fognak kidolgozni annak biztosítása érdekében, hogy az egyén állítása szerinti ugyanazon jogsértés esetén kétszeres jogorvoslatra vagy eljárásra ne kerülhessen sor.

3. Az FTC fellépése a választottbírósági eljárással párhuzamosan történhet.

4. Az USA, az EU vagy bármely uniós tagállam vagy más kormányzati hatóság, közigazgatási szerv vagy végrehajtási hatóság képviselője nem vehet részt az ilyen választottbírósági eljárásban – azzal, hogy egy uniós polgár kérésére az uniós adatvédelmi hatóságok segítséget nyújthatnak kizárólag az értesítés megfogalmazásában, de az uniós adatvédelmi hatóságok nem férhetnek hozzá az ilyen választottbírósági eljárások betekintésre szánt vagy más anyagaihoz.

5. A választottbírósági eljárás helyszíne az Egyesült Államok, és az egyén dönthet úgy, hogy video- vagy telefonkapcsolat útján vesz részt az eljárásban, amelyet az egyén számára ingyenesen biztosítanak. Személyes részvétel nem szükséges.

6. A választottbírósági eljárás nyelve az angol, kivéve, ha a felek másképpen állapodnak meg. Indokolt kérés esetén, és figyelembe véve, hogy az egyént képviseli-e ügyvéd, a választottbírósági tárgyaláson a tolmácsolás és a választottbírósági anyagok fordítása ingyenesen biztosított az egyén számára – kivéve, ha az EU–USA adatvédelmi kerettel foglalkozó testület megállapítja, hogy a választott bíráskodás konkrét körülményei között ez indokolatlan, vagy aránytalan költségekkel járna.

7. A választottbíráknak benyújtott anyagokat bizalmasan kezelik, és csak a választottbírósági eljárással kapcsolatban használják fel.

8. Egyénspecifikus betekintés szükség esetén engedélyezhető; az ilyen betekintést a felek bizalmasan kezelik, és csak a választottbírósági eljárással kapcsolatban használják fel.

9. A felek eltérő megállapodásának hiányában a választottbírósági eljárást az értesítés adott szervezethez történt benyújtását követő 90 napon belül be kell fejezni.

([3]) A Minisztérium a Nemzetközi Vitarendezési Központot (a továbbiakban: ICDR), az Amerikai Választottbírósági Szövetség (a továbbiakban: AAA) nemzetközi divízióját (a továbbiakban együttesen: ICDR-AAA) választotta ki az elvek I. melléklete szerinti választottbírósági eljárások lebonyolítására és az ugyanazon mellékletben meghatározott választottbírósági alap kezelésére. 2017. szeptember 15-én a Minisztérium és a Bizottság megállapodott az elvek I. mellékletében ismertetett kötelező erejű választottbírósági eljárásokra vonatkozó választottbírósági szabályok elfogadásáról, valamint a választottbírák magatartási kódexéről, amely összhangban van a kereskedelmi választottbírákra vonatkozó általánosan elfogadott etikai normákkal és az elvek I. mellékletével. A Minisztérium és a Bizottság megállapodott abban, hogy kiigazítják a választottbírósági szabályokat és a magatartási kódexet, hogy azok tükrözzék az EU–USA adatvédelmi keret szerinti frissítéseket, és a Minisztérium együtt fog működni az ICDR-AAA-vel e frissítések elvégzése érdekében.

H. **Költségek**

A választottbíráknak észszerű lépéseket kell tenniük a választottbírósági eljárás költségeinek minimalizálása érdekében.

A vonatkozó jogszabályokkal összhangban a Minisztérium előmozdítja egy alap fenntartását, amelybe az adatvédelmi keretben részt vevő szervezeteknek – részben a szervezet mérete alapján – éves hozzájárulást kell fizetniük, amely egy maximális összeg („plafon”) erejéig fedezi a választottbírósági költségeket, beleértve a választottbírák díjazását. Az alapot egy harmadik fél kezeli, amely rendszeresen beszámol a Minisztériumnak az alap működéséről. A Minisztérium együttműködik e harmadik féllel az alap működésének felülvizsgálata céljából, beleértve azt is, hogy szükséges-e a hozzájárulások összegének vagy a választottbírósági költségek plafonjának a kiigazítása, és megvizsgálja többek között a választottbírósági eljárások számát, valamint költségeit és időzítését, szem előtt tartva, hogy az adatvédelmi keretben részt vevő szervezetek számára a hozzájárulás ne jelentsen túlzott pénzügyi terhet. A Minisztérium értesíti a Bizottságot a harmadik féllel együtt végzett ezen felülvizsgálatok eredményéről, és előzetesen értesíti a Bizottságot a hozzájárulások összegének esetleges kiigazításáról. Az ügyvédi költségekre ez a rendelkezés nem vonatkozik, és azok az e rendelkezés szerinti alapból nem fedezhetők.

II. MELLÉKLET

AZ EGYESÜLT ÁLLAMOK KERESKEDELMI MINISZTÉRIUMA
Kereskedelmi miniszter
Washington, 20230

2023. július 6.

Didier Reynders
jogérvényesülésért felelős biztos
Európai Bizottság
Rue de la Loi/Wetstraat 200
1049 Brüsszel
Belgium

Tisztelt Reynders biztos úr!

Az Egyesült Államok nevében örömmel továbbítom az EU–USA adatvédelmi kerettel kapcsolatos csomagot, amely az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről szóló 14086. sz. elnöki rendelettel és a Szövetségi Rendeletek Kódexe 28. címének – az Adatvédelmi Felülvizsgálati Bíróság létrehozása céljából egyes igazságügyi minisztériumi rendeleteket módosító – 201. szakaszával (28 CFR part 201) együttesen tükrözi a magánélet és a polgári szabadságjogok védelmének megerősítéséről folytatott fontos és részletes tárgyalásokat. E tárgyalások eredményeként egyrészt új biztosítékok születtek arra vonatkozóan, hogy az Egyesült Államok – meghatározott nemzetbiztonsági célkitűzések elérésére irányuló – jelfelderítési tevékenységei szükségesek és arányosak legyenek, másrészt létrejött egy új mechanizmus, amely lehetővé teszi az európai unióbeli (a továbbiakban: EU) magánszemélyek számára, hogy jogorvoslatot kérjenek, ha úgy vélik, hogy egyes jelfelderítési tevékenységek jogellenesen célozzák őket – és e két tényező együttesen biztosítani fogja az uniós polgárok személyes adatainak védelmét. Az EU–USA adatvédelmi keret támogatni fogja az inkluzív és versenyképes digitális gazdaságot. Mindketten büszkének kell lennünk arra a fejlődésre, amelyet a keret tükröz, és amely világszerte erősíteni fogja a személyes adatok védelmét. Ez a csomag az elnöki rendelettel, a rendeletekkel és a nyilvános forrásokból elérhető más anyagokkal együtt nagyon szilárd alapot biztosít az Európai Bizottság számára a megfelelőség újonnan történő megállapításához ([1]).

E levélhez csatoltuk a következőket:

– az EU–USA adatvédelmi keret elvei, beleértve a kiegészítő elveket (együttesen: az elvek) és az elvek I. mellékletét (*azaz* egy olyan mellékletet, amely meghatározza azokat a feltételeket, amelyek alapján az adatvédelmi keretben részt vevő szervezetek kötelesek választottbírósági döntést kérni bizonyos fennmaradó követelésekről az elvek hatálya alá tartozó személyes adatokkal kapcsolatban),

– a Minisztérium adatvédelmi keretet kezelő Nemzetközi Kereskedelmi Igazgatóságának levele, amely ismerteti a Minisztérium által az EU–USA adatvédelmi keret hatékony működésének biztosítása érdekében tett kötelezettségvállalásokat,

– a Szövetségi Kereskedelmi Bizottság levele, amely leírja az elvek általa történő végrehajtását,

– a Közlekedési Minisztérium levele, amely leírja az elvek általa történő végrehajtását,

– a Nemzeti Hírszerzési Igazgatóság által készített két levél az USA nemzetbiztonsági hatóságaira vonatkozó biztosítékokról és korlátozásokról, valamint

– az Igazságügyi Minisztérium által készített levél az Egyesült Államok kormányának a bűnüldözési és közérdekű célból történő hozzáférésére vonatkozó biztosítékokról és korlátozásokról.

([1]) Amennyiben az EU–USA adatvédelmi keret által biztosított védelem megfelelőségére vonatkozó bizottsági határozat Izlandra, Liechtensteinre és Norvégiára is alkalmazandó, az EU–USA adatvédelmi kerettel kapcsolatos csomag egyaránt lefedi majd az Európai Uniót és ezt a három országot.

Az EU–USA adatvédelmi kerettel kapcsolatos teljes csomagot közzéteszik a Minisztérium adatvédelmi keretre vonatkozó honlapján, az elvek és az elvek I. melléklete pedig az Európai Bizottság megfelelőségi határozata hatálybalépésének napján lép hatályba.

Biztosíthatom arról, hogy az Egyesült Államok komolyan veszi ezeket a kötelezettségvállalásokat. Várakozással tekintünk az Önökkel történő együttműködés elé az EU–USA adatvédelmi keret megvalósítása, valamint e folyamat következő szakaszának megkezdése során.

Üdvözlettel:

Gina M. RAIMONDO

III. MELLÉKLET

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

2022. december 12.

Didier Reynders
jogérvényesülésért felelős biztos
Európai Bizottság
Rue de la Loi/Wetstraat 200
1049 Brüsszel
Belgium

Tisztelt Reynders biztos úr!

A Nemzetközi Kereskedelmi Igazgatóság nevében örömmel mutatom be azokat a kötelezettségvállalásokat, amelyeket a Kereskedelmi Minisztérium (a továbbiakban: a Minisztérium) tett annak érdekében, hogy az adatvédelmi keret igazgatása és felügyelete révén biztosítsa a személyes adatok védelmét. Az EU–USA adatvédelmi keret véglegesítése jelentős eredmény a személyes adatok védelme és a vállalkozások számára az Atlanti-óceán mindkét partján, mivel e keret bizalmat fog kelteni az uniós polgárokban abban a tekintetben, hogy adataik védelemben részesülnek, és hogy rendelkezésükre állnak jogorvoslati lehetőségek az adataikkal kapcsolatos aggályok kezelésére, valamint több ezer vállalkozás számára teszi lehetővé, hogy gazdaságaink és polgáraink javát szolgálva folytassák az Atlanti-óceánon átnyúló kereskedelmet. Az EU–USA adatvédelmi keret az Önnel és az Európai Bizottságban (a továbbiakban: a Bizottság) dolgozó kollégáival folytatott, évek óta tartó szorgos munkát és együttműködést tükrözi. Várakozással tekintünk a Bizottsággal végzett munka folytatása elé annak biztosítása érdekében, hogy e közös rendszer eredményesen működjön.

Az EU–USA adatvédelmi keret az egyének és a vállalkozások számára is jelentős előnyöket nyújt. Először is az uniós polgárok Egyesült Államokba továbbított adatait jelentős adatvédelmi rendelkezésekkel védi. Előírja a részt vevő egyesült államokbeli szervezetek számára, hogy az elveknek megfelelő adatvédelmi szabályzatot dolgozzanak ki; hogy nyilvános kötelezettségvállalást tegyenek az EU–USA adatvédelmi keret elveinek és kiegészítő elveinek (a továbbiakban együttesen: az elvek), valamint az elvek I. mellékletének (az azon feltételeket meghatározó melléklet, amely alapján az EU–USA adatvédelmi keretben részt vevő szervezetek kötelesek bizonyos, az elvek hatálya alá tartozó személyes adatokkal kapcsolatos fennmaradó követeléseket választottbírósági úton rendezni) való megfelelés tekintetében azért, hogy a kötelezettségvállalás az amerikai jog alapján érvényesíthető legyen ([1]); hogy évente ismételten tanúsítsák megfelelésüket a Minisztériumnak; biztosítsanak ingyenes és független vitarendezési lehetőséget az uniós polgárok számára; és az elvekben felsorolt valamely egyesült államokbeli hatósági szerv (*pl.* a Szövetségi Kereskedelmi Bizottság (a továbbiakban: FTC) és a Közlekedési Minisztérium, a továbbiakban: DOT) vagy az elvek jövőbeli mellékletében felsorolt egyesült államokbeli szerv vizsgálati és végrehajtási hatáskörébe kell tartozniuk. Míg egy szervezet öntanúsításra vonatkozó döntése önkéntes, ha egy szervezet nyilvánosan elkötelezi magát az EU–USA adatvédelmi keret mellett, kötelezettségvállalását az Egyesült Államok joga szerint az FTC, a DOT vagy az Egyesült Államok más hivatalos szerve kikényszerítheti attól függően, hogy melyik

([1]) Azoknak a szervezeteknek, amelyek öntanúsították az EU–USA adatvédelmi pajzs elveinek való megfelelés iránti kötelezettségvállalásukat, és élni kívánnak az EU–USA adatvédelmi keretben való részvétel előnyeivel, meg kell felelniük az EU–USA adatvédelmi keret elveinek. Az EU–USA adatvédelmi keret elveinek való megfelelésre vonatkozó kötelezettségvállalásnak a lehető leghamarabb, de legkésőbb az elvek hatálybalépésének időpontjától számított három hónapon belül tükröződnie kell a részt vevő szervezetek adatvédelmi szabályzatában. (*Lásd* az öntanúsítás kiegészítő elvének e) pontját).

szerv rendelkezik joghatósággal a részt vevő szervezet felett. Másodszor, az EU–USA adatvédelmi keret lehetővé teszi az Egyesült Államokban működő vállalatok – többek között az európai vállalatok egyesült államokbeli leányvállalatai – számára, hogy személyes adatokat kapjanak az Európai Unióból a transzatlanti kereskedelmet támogató adatáramlás elősegítése érdekében. Az Egyesült Államok és az Európai Unió közötti adatáramlás a világon a legnagyobb, és alapját képezi az Egyesült Államok és az EU közötti 7,1 billió USD-s gazdasági kapcsolatnak, amely munkahelyek millióit hozta létre az Atlanti-óceán mindkét partján. A transzatlanti adatáramlásra támaszkodó vállalkozások valamennyi ipari ágazatot képviselik, köztük vannak a legnagyobb Fortune 500 listán szereplő cégek, valamint sok kis- és középvállalkozás. A transzatlanti adatáramlás lehetővé teszi az egyesült államokbeli szervezetek számára az áruk, szolgáltatások és munkalehetőségek európai polgárok számára történő nyújtásához szükséges adatok kezelését.

A Minisztérium elkötelezett amellett, hogy szorosan és produktívan együttműködjön uniós partnereinkkel az adatvédelmi keret hatékony igazgatása és felügyelete érdekében. Ez a kötelezettségvállalás tükröződik a Minisztérium által kifejlesztett és folyamatosan tökéletesített különféle erőforrásokban, amelyek segítik a szervezeteket az öntanúsítási folyamat során, továbbá tükröződik az érdekelt felek számára célzott tájékoztatást biztosító honlap létrehozásában, a Bizottsággal és az európai adatvédelmi hatóságokkal az EU–USA adatvédelmi keret fontos elemeit tisztázó iránymutatás kidolgozása céljából folytatott együttműködésben, a szervezetek adatvédelmi kötelezettségeinek jobb megértését elősegítő tájékoztatási tevékenységben, valamint annak felügyeletében és nyomon követésében, hogy a szervezetek megfelelnek-e a keret követelményeinek.

A nagyra becsült uniós partnerekkel való folyamatos együttműködésünk lehetővé teszi a Minisztérium számára, hogy biztosítsa az EU–USA adatvédelmi keret hatékony működését. Az Egyesült Államok kormánya régóta együttműködik a Bizottsággal a közös adatvédelmi elvek előmozdítása érdekében, áthidalva a jogi megközelítéseink közötti különbségeket, valamint előmozdítva a kereskedelmet és a gazdasági növekedést az Európai Unióban és az Egyesült Államokban. Úgy véljük, hogy az EU–USA adatvédelmi keret, amely ennek az együttműködésnek az egyik példája, lehetővé teszi a Bizottság számára, hogy új megfelelőségi határozatot adjon ki, amely lehetővé teszi a szervezetek számára, hogy az EU–USA adatvédelmi keretet használják a személyes adatok Európai Unióból az Egyesült Államokba történő, az uniós joggal összhangban lévő továbbítására.

Az adatvédelmi keret Kereskedelmi Minisztérium általi igazgatása és felügyelete

A Minisztérium szilárdan elkötelezett az adatvédelmi keret hatékony igazgatása és felügyelete mellett, és megfelelő erőfeszítéseket tesz, valamint megfelelő forrásokat különít el ezen eredmény biztosítása érdekében. A Minisztérium fenntartja és nyilvánosságra hozza azon egyesült államokbeli szervezetek hiteles listáját, amelyek elvégezték az öntanúsítást a Minisztérium felé, és elkötelezték magukat az elvek betartása mellett (a továbbiakban: adatvédelmi keretben részt vevő szervezetek listája); e listát egyrészt a részt vevő szervezetek által benyújtott éves újratanúsítási beadványok alapján, másrészt a szervezetek önkéntes kilépése, a minisztérium eljárásainak megfelelő éves újratanúsítás elmulasztása, vagy a tartós nem megfelelés esetén a szervezetek törlése révén frissít. A Minisztérium vezeti továbbá az adatvédelmi keretben részt vevő szervezetek listájáról törölt szervezetek nyilvános és hiteles nyilvántartását, és minden esetben meghatározza a törlés okát. A fent említett hiteles lista és nyilvántartás továbbra is elérhető lesz a Minisztérium adatvédelmi keretre vonatkozó honlapján. Az adatvédelmi keret honlapján jól látható módon ismertetőt helyeznek majd el arra vonatkozóan, hogy az adatvédelmi keretben részt vevő szervezetek listájáról törölt szervezet nem állíthatja többé, hogy részt vesz az EU–USA adatvédelmi keretben, vagy megfelel annak, és hogy az EU–USA adatvédelmi keret alapján személyes adatokat kaphat. Az ilyen szervezetnek mindazonáltal továbbra is alkalmaznia kell az elveket az EU–USA adatvédelmi keretben való részvétele során kapott személyes adatokra mindaddig, amíg azokat megőrzi. A Minisztérium – az adatvédelmi keret hatékony igazgatása és felügyelete iránti átfogó és folyamatos elkötelezettségének előmozdítása érdekében – különösen a következőket vállalja:

Öntanúsításra vonatkozó követelmények ellenőrzése

– A Minisztérium a szervezet első öntanúsításának vagy éves újratanúsításának (együttesen: öntanúsítás) véglegesítése, valamint a szervezetnek az adatvédelmi keretben részt vevő szervezetek listájára való felvétele vagy a listán tartása előtt ellenőrzi, hogy a szervezet teljesítette-e legalább az öntanúsításra vonatkozó kiegészítő elvben meghatározott követelményeket arra vonatkozóan, hogy a szervezetnek milyen információkat kell megadnia a Minisztériumnak benyújtott öntanúsítási beadványában, és kellő időben biztosította-e a megfelelő adatvédelmi szabályzatot, amely tájékoztatja az egyéneket a tájékoztatás elvében felsorolt 13 elem mindegyikéről. A Minisztérium ellenőrzi, hogy a szervezet:

– azonosította-e az öntanúsítást benyújtó szervezetet, valamint az öntanúsító szervezet azon egyesült államokbeli szervezeteit vagy egyesült államokbeli leányvállalatait, amelyek szintén betartják az elveket, és amelyekre a szervezet az öntanúsítást ki kívánja terjeszteni,

– megadta-e a szervezet előírt kapcsolattartási adatait (pl. az öntanúsító szervezeten belül a panaszok, a hozzáférési kérelmek és az EU–USA adatvédelmi kerettel kapcsolatban felmerülő bármely egyéb kérdés kezeléséért felelős személy(ek) és/vagy egység(ek) elérhetőségi adatai),

– ismertette-e az(oka)t a cél(oka)t, amely(ek)re a szervezet összegyűjti és felhasználja az Európai Unióból kapott személyes adatokat,

– jelezte-e, hogy milyen személyes adatokat kapna az Európai Uniótól az EU–USA adatvédelmi keret alapján, amelyek ezért az öntanúsítás hatálya alá tartoznának,

– ha a szervezet nyilvános honlappal rendelkezik, megadta-e azt a webcímet, ahol a vonatkozó adatvédelmi szabályzat könnyen elérhető az adott honlapon, vagy ha a szervezet nem rendelkezik nyilvános honlappal, átadta-e a Minisztériumnak a vonatkozó adatvédelmi szabályzat egy példányát, és hogy ezt az adatvédelmi szabályzatot az érintett egyének meg tudják-e tekinteni (azaz az érintett munkavállalók, ha a vonatkozó adatvédelmi szabályzat az emberi erőforrásokra vonatkozó adatvédelmi szabályzat, vagy a nagyközönség, ha a vonatkozó adatvédelmi szabályzat nem az emberi erőforrásokra vonatkozó adatvédelmi szabályzat),

– a vonatkozó adatvédelmi szabályzatába kellő időpontban (azaz először csak a beadvánnyal együtt benyújtott adatvédelmi szabályzat tervezetébe, ha az első öntanúsításról van szó; egyéb esetekben a végleges, és adott esetben közzétett adatvédelmi szabályzatba) belefoglalt-e egy arra vonatkozó nyilatkozatot, hogy megfelel az elveknek, valamint a Minisztérium adatvédelmi keretre vonatkozó honlapjának címét (pl. a honlapot vagy az adatvédelmi keretben részt vevő szervezetek listáját tartalmazó weboldalt) vagy az arra mutató linket,

– megfelelő időpontban belefoglalta-e a vonatkozó adatvédelmi szabályzatába a tájékoztatási elvben meghatározott mind a 12 további felsorolt elemet (pl. annak lehetősége, hogy az érintett uniós polgár bizonyos feltételek mellett kötelező erejű választottbírósági eljárást kezdeményezzen; az a követelmény, hogy állami hatóságok jogszerű kérésére – nemzetbiztonsági vagy bűnüldözési követelmények teljesítése céljából – át kell adni személyes adatokat; valamint a felelőssége harmadik fél részére történő újbóli továbbítás esetén),

– meghatározta-e azt az állami szervet, amelynek hatásköre van a szervezet ellen esetleges tisztességtelen vagy megtévesztő gyakorlatok, valamint törvénysértések vagy adatvédelmi előírások megsértése miatt benyújtott panaszok kivizsgálására (amelyek felsorolása az elvekben vagy az elvek jövőbeli mellékletében található),

– megadta-e azokat az adatvédelmi programokat, amelyekben a szervezet részt vesz,

– meghatározta-e, hogy az elveknek való megfelelése ellenőrzésére szolgáló módszer (azaz az általa előírandó nyomonkövetési eljárások) „önértékelés” (azaz szervezeten belüli ellenőrzés) vagy „külső megfelelőségi felülvizsgálat” (azaz harmadik fél általi ellenőrzés), és ha a külső megfelelőségi felülvizsgálatot választotta, azt a harmadik felet is megnevezte-e, amely a felülvizsgálatot elvégezte,

– megjelölte-e azt a megfelelő független jogorvoslati mechanizmust, amely rendelkezésre áll az elvek alapján benyújtott panaszok kezelésére, és megfelelő és ingyenes jogorvoslatot biztosít-e az érintett személy számára.

  – Ha a szervezet egy magánszektorbeli alternatív vitarendezési szerv által biztosított független jogorvoslati mechanizmust választott ki, vonatkozó adatvédelmi szabályzatába beillesztette-e az elvek alapján benyújtott megoldatlan panaszok kivizsgálására rendelkezésre álló mechanizmus megfelelő weboldalára vagy panaszbenyújtási űrlapjára mutató hiperlinket vagy internetcímet.

  – Amennyiben a szervezetnek vagy kötelessége (az Európai Unióból munkaviszony keretében továbbított emberierőforrás-adatok tekintetében), hogy együttműködjön a megfelelő adatvédelmi hatóságokkal az elvek alapján benyújtott panaszok kivizsgálása és megoldása során, vagy úgy döntött, hogy együttműködik, azzal kinyilvánította elkötelezettségét az adatvédelmi hatóságokkal való ezen együttműködés és az általuk ehhez kapcsolódóan kiadott ajánlásoknak való megfelelés mellett, melyek az elveknek való megfelelés érdekében konkrét lépéseket javasolnak.

– A Minisztérium azt is ellenőrzi, hogy a szervezet öntanúsítási beadványa összhangban van-e a vonatkozó adatvédelmi szabályzatával/szabályzataival. Amennyiben egy öntanúsító szervezet ki kívánja terjeszteni a részvételt bármely olyan egyesült államokbeli szervezetére vagy leányvállalatára, amely önálló, releváns adatvédelmi szabályzattal rendelkezik, a Minisztérium felülvizsgálja az érintett szervezetek vagy leányvállalatok vonatkozó adatvédelmi szabályzatait is annak biztosítása érdekében, hogy azok tartalmazzák a tájékoztatási elvben meghatározott valamennyi szükséges elemet.

– A Minisztérium együttműködik az állami szervekkel (*pl.* FTC és DOT) annak ellenőrzése érdekében, hogy a szervezetek az öntanúsítási beadványaikban megjelölt megfelelő hatósági szerv joghatósága alá tartoznak-e, amennyiben a Minisztériumnak oka van kételkedni abban, hogy az említett joghatóság alá tartoznak.

– A Minisztérium együttműködik a magánszektor alternatív vitarendezési szerveivel annak ellenőrzése érdekében, hogy a szervezetek aktív regisztrációval rendelkeznek-e az öntanúsítási beadványaikban meghatározott független jogorvoslati mechanizmus tekintetében; és együttműködik ezekkel a szervekkel annak ellenőrzése érdekében, hogy a szervezetek aktív regisztrációval rendelkeznek-e az öntanúsítási beadványaikban azonosított külső megfelelőségi felülvizsgálat tekintetében, amennyiben ezek a testületek mindkét típusú szolgáltatást kínálhatják.

– A Minisztérium együttműködik az általa kiválasztott azon harmadik féllel, amely az adatvédelmi hatóságok testületének díjából (*azaz* az adatvédelmi hatóságok testülete működési költségeinek fedezésére szolgáló éves díj) begyűjtött pénzeszközök letétkezelőjeként jár el annak ellenőrzése érdekében, hogy a szervezetek az adott évre megfizették-e ezt a díjat, amennyiben a szervezetek az adatvédelmi hatóságokat jelölték meg megfelelő független jogorvoslati mechanizmusként.

– A Minisztérium együttműködik az általa kiválasztott harmadik féllel, amely az elvek I. mellékletében meghatározott választottbírósági eljárásokat lebonyolítja és az ott meghatározott választottbírósági alapot kezeli, annak ellenőrzése érdekében, hogy a szervezetek hozzájárultak-e az említett választottbírósági alaphoz.

– Amennyiben a Minisztérium a szervezetek öntanúsítási beadványainak felülvizsgálata során problémákat tár fel, tájékoztatja őket arról, hogy minden ilyen kérdést a Minisztérium által meghatározott megfelelő határidőn belül kezelniük kell ([2]). A Minisztérium arról is tájékoztatni fogja őket, hogy a Minisztérium által meghatározott határidőn belüli reagálás elmulasztása, illetve a Minisztérium eljárásai szerinti öntanúsítás teljesítésének egyéb módon történő elmulasztása ahhoz vezet, hogy az öntanúsítási beadványokat visszavontnak fogják tekinteni, valamint hogy a szervezetnek az EU–USA adatvédelmi keretben való részvételére vagy az annak való megfelelésére vonatkozó hamis nyilatkozattétel az FTC, a DOT vagy más illetékes kormányzati szerv végrehajtási intézkedésének tárgyát képezheti. A Minisztérium a szervezeti egységek által a Minisztériumnak megadott kapcsolattartási módon tájékoztatja a szervezeteket.

Az elvekhez kapcsolódó szolgáltatásokat nyújtó alternatív vitarendezési szervekkel való együttműködés elősegítése

– A Minisztérium együttműködik a független jogorvoslati mechanizmusokat biztosító, magánszektorbeli alternatív vitarendezési szervekkel – amelyeket igénybe lehet venni az elvek alapján benyújtott megoldatlan panaszok kivizsgálására –, annak ellenőrzése céljából, hogy azok megfelelnek-e legalább a vitarendezésről és a végrehajtásról szóló kiegészítő elvben meghatározott követelményeknek. A Minisztérium ellenőrzi, hogy a testületek:

  – tájékoztatást nyújtanak az elvekről és az adott mechanizmus által az EU–USA adatvédelmi keretben nyújtott szolgáltatásokról, amely tájékoztatásnak magában kell foglalnia az alábbiakat: 1. az elvek független jogorvoslati mechanizmusokra vonatkozó követelményeire vonatkozó információk vagy az e követelményekre mutató hiperlink, 2. a Minisztérium adatvédelmi keretre vonatkozó honlapjára mutató hiperlink, 3. arra vonatkozó információ, hogy az EU–USA adatvédelmi keret szerinti vitarendezési szolgáltatásaik ingyenesek az egyének számára, 4. annak leírása, hogy az elvekkel kapcsolatos panaszok hogyan nyújthatók be, 5. az elvekkel kapcsolatos panaszok feldolgozásának határideje, és 6. a lehetséges jogorvoslatok körének leírása. A Minisztérium időben értesíti a szerveket az adatvédelmi keret Minisztérium általi felügyeletében és igazgatásában bekövetkezett lényeges változásokról, amennyiben ilyen változások küszöbön állnak vagy már megtörténtek, és ezek a változások relevánsak a testületek által az EU–USA adatvédelmi keretben betöltött szerep szempontjából,

([2]) *Pl.* ami az újratanúsítást illeti, az az elvárás, hogy a szervezetek 45 napon belül foglalkozzanak az összes ilyen kérdéssel, kivéve, ha a Minisztérium egyéb megfelelő időkeretet határoz meg.

– éves jelentést tesznek közzé, amely összesített statisztikákat tartalmaz vitarendezési szolgáltatásaikról, amelyek a következőket tartalmazzák: 1. a jelentéstételi év folyamán beérkezett, az elvekkel kapcsolatos panaszok teljes száma, 2. a beérkezett panaszok típusa, 3. a vitarendezés minőségével kapcsolatos intézkedések, például a panaszok feldolgozásához igénybe vett idő hossza, valamint 4. a beérkezett panaszok eredménye, nevezetesen az alkalmazott jogorvoslatok és szankciók száma és típusa. A Minisztérium konkrét, kiegészítő iránymutatást nyújt a szerveknek arra vonatkozóan, hogy milyen információkat kell szolgáltatniuk az említett éves jelentésekben, részletezve a követelményeket (*pl.* azon konkrét kritériumok felsorolása, amelyeknek a panasznak meg kell felelnie ahhoz, hogy az éves jelentésben az elvekhez kapcsolódó panaszként lehessen feltüntetni), valamint meghatározza a szervek által szolgáltatandó egyéb információtípusokat (*pl.* ha a szerv az elvekkel kapcsolatos ellenőrzési szolgáltatást is nyújt, annak leírása, hogy a szerv hogyan kerüli el a tényleges vagy potenciális összeférhetetlenséget olyan helyzetekben, amikor ugyanazon szervezetnek ellenőrzési szolgáltatásokat és vitarendezési szolgáltatásokat is nyújt). A Minisztérium által nyújtott kiegészítő iránymutatás azt az időpontot is meghatározza, ameddig a szervek éves jelentéseit az adott jelentéstételi időszakra vonatkozóan közzé kell tenni.

Azon szervezetek nyomon követése, amelyek töröltetni kívánják magukat vagy amelyeket töröltek az adatvédelmi keretben részt vevő szervezetek listájáról

– Ha egy szervezet ki kíván lépni az EU–USA adatvédelmi keretből, a Minisztérium megköveteli, hogy a szervezet minden vonatkozó adatvédelmi szabályzatból töröljön minden olyan, az EU–USA adatvédelmi keretre való hivatkozást, amely arra utal, hogy továbbra is részt vesz az EU–USA adatvédelmi keretben, és hogy az EU–USA adatvédelmi keret alapján személyes adatokat kaphat (*lásd* a Minisztérium azon kötelezettségvállalásának leírását, hogy feltárja a részvételre vonatkozó hamis állításokat). A Minisztérium azt is előírja, hogy a szervezet töltsön ki és nyújtson be megfelelő kérdőívet a Minisztériumnak a következők igazolása céljából:

  – a kilépési szándéka,

  – az alább felsoroltak közül melyiket fogja tenni az EU–USA adatvédelmi keret alapján, a keretben való részvétele során kapott személyes adatokkal: a) megőrzi ezeket az adatokat, továbbra is alkalmazza az elveket ezekre az adatokra, és évente megerősíti a Minisztérium felé az elvek ezen adatokra való alkalmazására vonatkozó kötelezettségvállalását, b) megőrzi ezeket az adatokat, és „megfelelő” védelmet biztosít ezek számára más engedélyezett módon, vagy c) az összes ilyen adatot egy meghatározott időpontig visszaküldi vagy törli, valamint

  – a szervezeten belül ki szolgál majd állandó kapcsolattartó pontként az elvekkel kapcsolatos kérdésekben.

– Ha a szervezet a fenti a) pontban leírtakat választotta, a Minisztérium azt is elő fogja írni számára, hogy a kilépését követően évente (*azaz* a kilépés első évfordulójáig, valamint minden ezt követő évfordulóig mindaddig, amíg a szervezet más engedélyezett módon „megfelelő” védelmet biztosít a szóban forgó adatoknak, vagy amíg vissza nem küldi vagy törli az összes ilyen adatot, és erről értesíti a Minisztériumot) töltsön ki és nyújtson be a Minisztériumnak a megfelelő kérdőívet annak ellenőrzésére, hogy mit tett ezekkel a személyes adatokkal, mit fog tenni azokkal a személyes adatokkal, amelyeket továbbra is megőriz, és a szervezeten belül ki szolgál majd állandó kapcsolattartó pontként az elvekkel kapcsolatos kérdésekben.

– Ha egy szervezet hagyta, hogy lejárjon az öntanúsítása (*azaz* nem végezte el az elvek betartására vonatkozó éves újratanúsítását, és nem törölték az adatvédelmi keretben részt vevő szervezetek listájáról más okból, például kilépés miatt), a Minisztérium utasítja, hogy töltsön ki és nyújtson be egy megfelelő kérdőívet a Minisztériumnak annak igazolása érdekében, hogy ki akar-e lépni a keretből vagy az újratanúsítást választja:

  – és ha ki kíván lépni, igazolnia kell továbbá, hogy mit fog tenni azokkal a személyes adatokkal, amelyeket az EU–USA adatvédelmi keretben való részvétele során kapott az EU–USA adatvédelmi keret alapján (*lásd* az előző leírást arról, hogy a szervezetnek mit kell igazolnia, ha ki kíván lépni),

  – és amennyiben az újratanúsítást választja, igazolnia kell továbbá, hogy tanúsítási státuszának lejártát követően alkalmazta-e az elveket az EU–USA adatvédelmi keret alapján kapott személyes adatokra, és tisztáznia kell, hogy milyen lépéseket fog tenni az újratanúsítását késleltető lezáratlan kérdések kezelése érdekében.

– Ha egy szervezetet az alábbi okok bármelyike miatt törölnek az adatvédelmi keretben részt vevő szervezetek listájáról: a) az EU–USA adatvédelmi keretből való kilépés, b) az elveknek való megfelelés éves újratanúsításának elmulasztása (azaz az éves újratanúsítási folyamatot elkezdte, de nem végezte el időben, vagy meg sem indította), vagy c) „tartós meg nem felelés" miatt, a Minisztérium értesítést küld a szervezet öntanúsítási beadványában megjelölt kapcsolattartó(k)nak, amelyben megjelöli a törlés okát és kifejti, hogy a szervezet a továbbiakban nem tehet arra vonatkozó kifejezett vagy hallgatólagos állításokat, hogy részt vesz az EU–USA adatvédelmi keretben vagy megfelel a keret elveinek, és hogy a keret alapján személyes adatokat kaphat. Az értesítés – amelynek a törlés okának megfelelően a fentieken túl mást is tartalmazhat – arra is kitér, hogy azon szervezetekkel szemben, amelyek megtévesztő módon nyilatkoznak az EU–USA adatvédelmi keretben való részvételükről vagy az annak való megfelelésről, ideértve azt is, ha az adatvédelmi keretben részt vevő szervezetek listájáról való törlésüket követően kijelentik, hogy részt vesznek az EU–USA adatvédelmi keretben, az FTC, a Közlekedési Minisztérium vagy más illetékes kormányzati szerv végrehajtási intézkedést foganatosíthat.

Hamis részvételi nyilatkozatok keresése és kezelése

– Ha egy szervezet: a) kilép az EU–USA adatvédelmi keretből, b) elmulasztja az elveknek való megfelelés éves újratanúsítását (azaz az éves újratanúsítási folyamatot elkezdte, de nem végezte el időben, vagy meg sem indította), vagy c) pl. „tartós meg nem felelés" miatt törölték a részt vevő szervezetek listájáról, vagy d) nem nyújtja be az elveknek való megfelelésére vonatkozó első öntanúsítást (azaz elkezdte, de nem végezte el időben az első öntanúsítási folyamatot), a Minisztérium folyamatosan hivatalból ellenőrzi, hogy a szervezet releváns közzétett adatvédelmi szabályzatai közül egy sem tartalmaz arra vonatkozó hivatkozásokat, hogy a szervezet részt vesz az EU–USA adatvédelmi keretben, és hogy az EU–USA adatvédelmi keret alapján személyes adatokat kaphat. Amennyiben a Minisztérium megállapítja, hogy az ilyen hivatkozásokat nem törölték, a Minisztérium figyelmezteti a szervezetet, hogy a Minisztérium adott esetben a megfelelő hatóságnak továbbítja az ügyet esetleges végrehajtási intézkedés céljából, amennyiben a szervezet továbbra is megtévesztő módon azt állítja, hogy részt vesz az EU–USA adatvédelmi keretben. A Minisztérium a szervezet által a Minisztérium számára megjelölt kapcsolattartási módon, vagy szükség esetén más megfelelő módon tájékoztatja a szervezetet. Ha a szervezet nem távolítja el a hivatkozásokat, és nem igazolja önként az EU–USA adatvédelmi keretnek való megfelelését a Minisztérium eljárásaival összhangban, a Minisztérium hivatalból az FTC, a DOT vagy más megfelelő végrehajtási hatóság elé utalja az ügyet, vagy más megfelelő intézkedést tesz az EU–USA adatvédelmi keret tanúsító védjegye megfelelő használatának biztosítása érdekében;

– A Minisztérium további erőfeszítéseket tesz annak érdekében, hogy azonosítsa az EU–USA adatvédelmi keretben való részvételre vonatkozó hamis állításokat és az EU–USA adatvédelmi keret tanúsító védjegyének helytelen használatát, többek között olyan szervezetek esetében, amelyek a fentebb leírt szervezetekkel ellentétben még egyszer sem kezdték meg az öntanúsítási eljárást (ilyen erőfeszítés lehet *pl.* az arra irányuló megfelelő internetes keresés, hogy a szervezetek adatvédelmi szabályzatában szerepelnek-e az EU–USA adatvédelmi keretre való hivatkozások). Amennyiben ezen erőfeszítéseknek köszönhetően a Minisztérium megállapítja, hogy az EU–USA adatvédelmi keretben való részvételre vonatkozóan hamis állításokat tüntettek fel, és jogtalanul használták a keret tanúsító védjegyét, a Minisztérium figyelmezteti a szervezetet, hogy a Minisztérium adott esetben a megfelelő hatóságnak továbbítja az ügyet esetleges végrehajtási intézkedés céljából, amennyiben a szervezet továbbra is megtévesztő módon azt állítja, hogy részt vesz az EU–USA adatvédelmi keretben. A Minisztérium a szervezet által a Minisztérium számára megjelölt kapcsolattartási módon (ha van ilyen), vagy szükség esetén más megfelelő módon tájékoztatja a szervezetet. Ha a szervezet nem távolítja el a hivatkozásokat, és nem igazolja önként az EU–USA adatvédelmi keretnek való megfelelését a Minisztérium eljárásaival összhangban, a Minisztérium hivatalból az FTC, a DOT vagy más megfelelő végrehajtó szerv elé utalja az ügyet, vagy más megfelelő intézkedést tesz az EU–USA adatvédelmi keret tanúsító védjegye megfelelő használatának biztosítása érdekében;

– a Minisztérium haladéktalanul felülvizsgálja és kezeli az EU–USA adatvédelmi keretben való részvételre vonatkozó hamis állításokkal kapcsolatos, a Minisztériumhoz beérkező – specifikus és nem komolytalan – panaszokat (*mint pl.* az adatvédelmi hatóságoktól, a magánszektorbeli alternatív vitarendezési szervek által biztosított független jogorvoslati mechanizmusoktól, az érintettektől, az uniós és egyesült államokbeli vállalkozásoktól, valamint más típusú harmadik felektől kapott panaszok), valamint

– a Minisztérium egyéb megfelelő korrekciós intézkedéseket is megtehet. A Minisztériumnak adott megtévesztő közlések a hamis nyilatkozatokról szóló törvény (18 U. S. C. § 1001) alapján perelhetők.

Az adatvédelmi keret rendszeres, hivatalból történő megfelelőségifelülvizsgálata és értékelése

– a Minisztérium folyamatos erőfeszítéseket tesz annak érdekében, hogy nyomon kövesse az EU–USA adatvédelmi keretben részt vevő szervezetek tényleges megfelelését, és ezáltal azonosítsa azokat a problémákat, amelyek további intézkedést igényelhetnek. A Minisztérium hivatalból rutinszerű helyszíni ellenőrzéseket végez véletlenszerűen kiválasztott, az EU–USA adatvédelmi keretben részt vevő szervezeteknél, valamint eseti helyszíni ellenőrzéseket végez az EU–USA adatvédelmi keretben részt vevő egyes konkrétan meghatározott szervezeteknél, amennyiben azoknál potenciális megfelelési hiányosságokat azonosítanak (pl. harmadik felek által a Minisztérium tudomására hozott esetleges megfelelési hiányosságok) a következők ellenőrzése céljából: a) az EU–USA adatvédelmi kerettel összefüggésben felmerülő panaszok, hozzáférési kérelmek és egyéb kérdések kezeléséért felelős kapcsolattartó pont(ok) rendelkezésre állnak-e, b) adott esetben az, hogy a szervezet nyilvános adatvédelmi szabályzata a nyilvánosság számára könnyen hozzáférhető legyen mind a szervezet nyilvános honlapján, mind az adatvédelmi keretbe tartozó szervezetek listáján található hiperlinken keresztül, c) a szervezet adatvédelmi szabályzata továbbra is megfelel az elvekben leírt öntanúsítási követelményeknek, és d) a szervezet által azonosított független jogorvoslati mechanizmus rendelkezésre áll az EU–USA adatvédelmi keret alapján benyújtott panaszok kezelésére. A Minisztérium emellett aktívan nyomon fogja követni az olyan beszámolókról szóló híreket, amelyek hiteles bizonyítékot szolgáltatnak arra vonatkozóan, hogy az EU–USA adatvédelmi keretben részt vevő egyes szervezetek nem felelnek meg a követelményeknek,

– a megfelelőségi felülvizsgálat részeként a Minisztérium előírja, hogy az EU–USA adatvédelmi keretben részt vevő szervezet töltsön ki és nyújtson be részletes kérdőívet a minisztériumnak, amennyiben: a) a Minisztérium konkrét lényegi panaszt kap az elvek szervezet általi teljesítésével kapcsolatban, b) a szervezet nem reagál megfelelő módon a Minisztérium EU–USA adatvédelmi keretre vonatkozó információkkal kapcsolatos megkeresésére, vagy c) hitelt érdemlő bizonyíték van arra, hogy a szervezet nem teljesíti az EU–USA adatvédelmi kerettel összefüggésben tett kötelezettségvállalásait. Amennyiben a Minisztérium ilyen részletes kérdőívet küldött egy szervezetnek, és a szervezet nem ad kielégítő választ a kérdőívre, a Minisztérium tájékoztatja a szervezetet arról, hogy adott esetben az ügyet az illetékes hivatalhoz utalja esetleges végrehajtási intézkedés céljából, ha a Minisztérium nem kap kellő időben kielégítő választ a szervezettől. A Minisztérium a szervezet által a Minisztérium számára megjelölt kapcsolattartási módon, vagy szükség esetén más megfelelő módon tájékoztatja a szervezetet. Ha a szervezet nem ad kellő időben kielégítő választ, a Minisztérium hivatalból az FTC, a DOT vagy más megfelelő végrehajtási szerv elé utalja az ügyet, vagy más megfelelő intézkedést tesz a megfelelés biztosítása érdekében. A Minisztérium adott esetben tanácskozik az illetékes adatvédelmi hatóságokkal az ilyen megfelelőség-felülvizsgálatokról, valamint

– a Minisztérium rendszeres időközönként értékelni fogja az adatvédelmi keret igazgatását és felügyeletét annak biztosítása érdekében, hogy a nyomonkövetési erőfeszítései – beleértve a keresőeszközök használatával tett ilyen erőfeszítéseket is (*pl.* az EU–USA adatvédelmi keretben részt vevő szervezetek adatvédelmi szabályzataira mutató, meghibásodott linkek ellenőrzése) – alkalmasak legyenek a meglévő problémák és az újonnan felmerülő problémák kezelésére.

Az adatvédelmi keret honlapjának célközönségre szabása

A Minisztérium az adatvédelmi keret honlapját az alábbi célközönségre szabja: uniós polgárok, uniós vállalkozások, egyesült államokbeli vállalkozások és adatvédelmi hatóságok. A közvetlenül uniós polgárokat és uniós vállalkozásokat célzó anyagok szerepeltetése számos módon megkönnyíti az átláthatóságot. Az uniós polgárok számára a honlap egyértelműen ismertetni fogja a következőket: 1. az EU–USA adatvédelmi keret által az uniós polgárok számára biztosított jogok, 2. az uniós polgárok rendelkezésére álló jogorvoslati mechanizmusok, amennyiben úgy vélik, hogy egy szervezet megszegte az elvek betartására vonatkozó kötelezettségvállalását, és 3. hogyan lehet információkat találni egy szervezet EU–USA adatvédelmi keret szerinti öntanúsításával kapcsolatban. Az uniós vállalkozások számára meg fogja könnyíteni a következők ellenőrzését: 1. egy szervezet részt vesz-e az EU–USA adatvédelmi keretben, 2. a szervezet EU–USA adatvédelmi keret szerinti öntanúsítása által lefedett információk típusa, 3. az érintett információkra vonatkozó adatvédelmi szabályzat, valamint 4. a szervezet által az elvek betartásának ellenőrzésére alkalmazott módszer. Az egyesült államokbeli vállalkozások számára a honlap egyértelműen ismertetni fogja a következőket: 1. az EU–USA adatvédelmi keretben való részvétel előnyei, 2. hogyan lehet csatlakozni az EU–USA adatvédelmi kerethez, valamint hogyan lehet megújítani a tanúsítást az EU–USA adatvédelmi keretben és hogyan lehet kilépni onnan, valamint 3. hogyan kezeli és juttatja érvényre az Egyesült Államok az EU–USA adatvédelmi keretet. A közvetlenül az adatvédelmi hatóságoknak szánt anyagok (*pl.* a Minisztérium adatvédelmi hatóságok számára kijelölt kapcsolattartó pontjára vonatkozó információk, valamint az FTC honlapján az elvekkel kapcsolatos tartalomra mutató hiperhivatkozás) beillesztése elősegíti majd az együttműködést és az átláthatóságot. A Minisztérium továbbá eseti alapon együttműködik a Bizottsággal és az Európai Adatvédelmi Testülettel (EDPB) annak érdekében is, hogy további aktuális anyagokat (*pl.* a gyakran feltett kérdésekre adott válaszokat) dolgozzon ki az adatvédelmi keret weboldalán való felhasználásra, ahol az ilyen információk megkönnyítenék az adatvédelmi keret hatékony igazgatását és felügyeletét.

Az adatvédelmi hatóságokkal folytatott együttműködés előmozdítása

Az adatvédelmi hatóságokkal folytatott együttműködés lehetőségeinek bővítése érdekében a Minisztérium kijelölt kapcsolattartó pontot tart fenn a Minisztériumban, aki kapcsolattartóként jár el az adatvédelmi hatóságok felé. Azokban az esetekben, amikor egy adatvédelmi hatóság úgy gondolja, hogy egy, az EU–USA adatvédelmi keretben részt vevő szervezet nem teljesíti az elveket, beleértve azt az esetet, amikor egy uniós polgár panaszt nyújtott be, az adatvédelmi hatóság kapcsolatba léphet majd a Minisztérium kijelölt kapcsolattartó pontjával a szervezet további felülvizsgálatra történő bejelentése érdekében. A Minisztérium megtesz minden tőle telhetőt az EU–USA adatvédelmi keretben részt vevő szervezettel kapcsolatos panasz megoldásának elősegítése érdekében. A panasz kézhezvételétől számított 90 napon belül a Minisztérium tájékoztatást ad az adatvédelmi hatóságnak az aktuális helyzetről. Az erre a célra kijelölt kapcsolattartó pont olyan szervezetekkel kapcsolatos bejelentéseket is kap, amelyek hamisan nyilatkoznak arról, hogy részt vesznek az EU–USA adatvédelmi keretben. A kijelölt kapcsolattartó nyomon követi az adatvédelmi hatóságoknak a Minisztériumhoz küldött bejelentéseit, és a Minisztérium az alább leírt közös felülvizsgálat során jelentést ad ki az adott évben általa kapott panaszok összegzéséről. A kijelölt kapcsolattartó pont segít az adatvédelmi hatóságoknak az adott szervezet öntanúsítására vagy az EU–USA adatvédelmi keretben való korábbi részvételére vonatkozó információk keresésében, és válaszol az adatvédelmi hatóságoknak az EU–USA adatvédelmi keret adott követelményeinek megvalósításával kapcsolatos megkereséseire. A Minisztérium együtt fog működni a Bizottsággal és az Európai Adatvédelmi Testülettel az adatvédelmi hatóságok testületét érintő eljárási és igazgatási kérdésekben is, ideértve többek között az adatvédelmi hatóságok testületének díjából beszedett pénzeszközök elosztására vonatkozó megfelelő eljárások kialakítását. Tudomásul vesszük, hogy a Bizottság együtt fog működni a Minisztériummal az ezen eljárásokkal kapcsolatban esetlegesen felmerülő kérdések megoldásának megkönnyítése érdekében. Továbbá a Minisztérium anyagokat biztosít az adatvédelmi hatóságoknak az EU–USA adatvédelmi keretre vonatkozóan, hogy azokat megjelenítsék a saját honlapjukon az uniós polgárok és uniós vállalkozások számára az átláthatóság növelése érdekében. Az EU–USA adatvédelmi keret és az általa keletkeztetett jogok és felelősségek jobb ismerete elősegíti a felmerülő problémák azonosítását azok megfelelő kezelése érdekében.

Az elvek I. melléklete szerinti kötelezettségvállalásainak teljesítése

A Minisztérium teljesíti az elvek I. melléklete szerinti kötelezettségvállalásait, beleértve a Bizottság által a függetlenség, feddhetetlenség és szakértelem alapján kiválasztott választottbírák jegyzékének vezetését; valamint adott esetben annak a harmadik félnek a támogatását, amelyet a Minisztérium az elvek I. melléklete szerinti választottbírósági eljárások lebonyolítására és az ugyanezen mellékletben meghatározott választottbírósági alap kezelésére kiválaszt ([3]). A Minisztérium együttműködik a harmadik féllel többek között annak ellenőrzése érdekében, hogy a harmadik fél fenntart-e a választottbírósági eljárásra vonatkozó iránymutatást tartalmazó honlapot, amely iránymutatás többek között a következőkre terjed ki: 1. az eljárás megindításának és a dokumentumok benyújtásának módja, 2. a Minisztérium által vezetett választottbírói névjegyzék, valamint a választottbírák e jegyzékből való kiválasztásának módja, 3. a Minisztérium és a Bizottság által elfogadott irányadó választottbírósági eljárások és választottbírói magatartási kódex ([4]), valamint 4. a választottbírák díjainak beszedése és kifizetése. Továbbá a Minisztérium együttműködik e harmadik féllel a választottbírósági alap működésének felülvizsgálata céljából, beleértve azt is, hogy szükséges-e a hozzájárulások összegének vagy a választottbírósági költségek plafonjának (vagyis maximális összegének) a kiigazítása, és megvizsgálja többek között a választottbírósági eljárások számát, valamint költségeit és időzítését, szem előtt tartva, hogy az adatvédelmi keretben részt vevő szervezetek számára a hozzájárulás ne jelentsen túlzott pénzügyi terhet. A Minisztérium értesíti a Bizottságot a harmadik féllel együtt végzett ezen felülvizsgálatok eredményéről, és előzetesen értesíti a Bizottságot a hozzájárulások összegének esetleges kiigazításáról.

Az EU–USA adatvédelmi keret működésére irányuló közös felülvizsgálatok lefolytatása

A Minisztérium és adott esetben más hatóságok rendszeres időközönként találkozókat tartanak a Bizottsággal, az érdekelt adatvédelmi hatóságokkal és az Európai Adatvédelmi Testület megfelelő képviselőivel, ahol a Minisztérium naprakész tájékoztatást nyújt az EU–USA adatvédelmi keretről. Az ülések keretében megvitatják az adatvédelmi keret működésével, végrehajtásával, felügyeletével és érvényre juttatásával kapcsolatos aktuális kérdéseket. Az üléseken adott esetben megvitathatnak kapcsolódó témákat is, például az EU–USA adatvédelmi keret szerinti biztosítékok hatálya alá tartozó egyéb adattovábbítási mechanizmusokat.

([3]) A Minisztérium a Nemzetközi Vitarendezési Központot (a továbbiakban: ICDR), az Amerikai Választottbírósági Szövetség (a továbbiakban: AAA) nemzetközi divízióját (a továbbiakban együttesen: ICDR-AAA) választotta ki az elvek I. melléklete szerinti választottbírósági eljárások lebonyolítására és az ugyanazon mellékletben meghatározott választottbírósági alap kezelésére.

([4]) 2017. szeptember 15-én a Minisztérium és a Bizottság megállapodott az elvek I. mellékletében ismertetett kötelező erejű választottbírósági eljárásokra vonatkozó választottbírósági szabályok elfogadásáról, valamint a választottbírák magatartási kódexéről, amely összhangban van a kereskedelmi választottbírákra vonatkozó általánosan elfogadott etikai normákkal és az elvek I. mellékletével. A Minisztérium és a Bizottság megállapodott abban, hogy kiigazítják a választottbírósági szabályokat és a magatartási kódexet, hogy azok tükrözzék az EU–USA adatvédelmi keret szerinti frissítéseket, és a Minisztérium együtt fog működni az ICDR-AAA-vel e frissítések elvégzése érdekében.

Tájékoztatás a jogszabályi fejleményekről

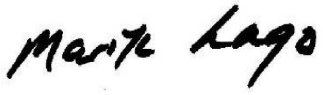
A Minisztérium észszerű erőfeszítéseket tesz arra, hogy tájékoztassa a Bizottságot az Egyesült Államok jogában bekövetkező lényeges fejleményekről, amennyiben azok relevánsak az EU–USA adatvédelmi keret szempontjából az adatvédelem, valamint az Egyesült Államok hatóságainak a személyes adatokhoz való hozzáférésére és azt követő használatára vonatkozó korlátozások és biztosítékok terén.

Az Egyesült Államok kormányának hozzáférése a személyes adatokhoz

Az Egyesült Államok kiadta a 14086. sz. elnöki rendeletet (az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről) és a Szövetségi Rendeletek Kódexe 28. címének – az Adatvédelmi Felülvizsgálati Bíróság (DPRC) létrehozása céljából egyes igazságügyi minisztériumi rendeleteket módosító – 201. szakaszát (28 CFR part 201), amelyek erős védelmet biztosítanak a személyes adatok számára az adatokhoz való nemzetbiztonsági célú kormányzati hozzáférés tekintetében. Ez a védelem a következőket foglalja magában: a személyes adatok védelmére és a polgári szabadságjogokra vonatkozó biztosítékok megerősítése annak biztosítása érdekében, hogy az USA meghatározott nemzetbiztonsági célok elérésére irányuló jelfelderítési tevékenységei szükségesek és arányosak legyenek; új jogorvoslati mechanizmus létrehozása független és kötelező erejű hatáskörrel; valamint az Egyesült Államok jelfelderítési tevékenységeire irányuló jelenlegi szigorú és többszintű felügyelet megerősítése. E védelem révén az uniós magánszemélyek egy új, többszintű jogorvoslati mechanizmus keretében kérhetnek jogorvoslatot, amely magában foglal egy független DPRC-t, amely az Egyesült Államok kormányától független kiválasztott személyekből állna, akik teljesen önállóan járhatnának el a keresetek elbírálása és szükség esetén a korrekciós intézkedések irányítása tekintetében. A Minisztérium nyilvántartást fog vezetni azokról az uniós állampolgárokról, akik a 14086. sz. elnöki rendelet és a CFR 28. címének 201. szakasza szerinti megfelelőnek minősülő panaszt nyújtanak be. E levél kelte után öt évvel, majd azt követően ötévente a Minisztérium felveszi a kapcsolatot az érintett szervekkel a tekintetben, hogy a megfelelőnek minősülő panaszok vagy a DPRC-hez benyújtott felülvizsgálati kérelmek felülvizsgálatára vonatkozó információk minősítését megszüntették-e. Amennyiben az ilyen információk minősítését megszüntették, a Minisztérium együttműködik az illetékes adatvédelmi hatósággal az uniós polgár tájékoztatása céljából. Ezek a fejlesztések megerősítik, hogy az Egyesült Államokba továbbított uniós személyes adatokat az adatokhoz való kormányzati hozzáférésre vonatkozó uniós jogi követelményekkel összhangban fogják kezelni.

Az elvek, a 14086. sz. elnöki rendelet, a CFR 28. címének 201. szakasza, valamint a kísérőlevelek és anyagok – köztük a Minisztériumnak az adatvédelmi keret igazgatására és felügyeletére vonatkozó kötelezettségvállalásai – alapján azt várjuk, hogy a Bizottság úgy dönt, hogy az EU–USA adatvédelmi keret megfelelő védelmet biztosít az uniós jogszabályok értelmében, és az Európai Unióból jövő adattovábbítás folytatódik azon szervezetek felé, amelyek részt vesznek az EU–USA adatvédelmi keretben. Arra is számítunk, hogy az uniós általános szerződési feltételek vagy az uniós kötelező erejű vállalati szabályok alapján az egyesült államokbeli szervezetek részére történő adattovábbítást e feltételek és szabályok tovább könnyítik.

Üdvözlettel:



Marisa LAGO

IV. MELLÉKLET

AMERIKAI EGYESÜLT ÁLLAMOK
Szövetségi Kereskedelmi Bizottság
Washington, 20580

Elnöki hivatal

2023. június 9.

Didier REYNDERS
jogérvényesülésért felelős biztos
Európai Bizottság
Rue de la Loi / Wetstraat 200
1049 Brüsszel
Belgium

Tisztelt Reynders biztos úr!

Az Egyesült Államok Szövetségi Kereskedelmi Bizottsága (a továbbiakban: FTC) nagyra értékeli azt a lehetőséget, hogy az EU–USA adatvédelmi keret elveivel összefüggésben éljen jogérvényesítési szerepével. Az FTC régóta elkötelezett a fogyasztók és a személyes adatok határokon átnyúló védelme mellett, és elkötelezettek vagyunk az adatvédelmi keret kereskedelmi ágazati vonatkozásainak érvényre juttatása mellett. Az FTC 2000 óta tölti be ezt a szerepet az Egyesült Államok és az EU közötti védett adatkikötőre vonatkozó keretrendszerrel, 2016 óta pedig az EU–USA adatvédelmi pajzs keretrendszerrel kapcsolatban ([1]). 2020. július 16-án az Európai Unió Bírósága (a továbbiakban: EUB) érvénytelenítette az Európai Bizottságnak EU–USA adatvédelmi pajzs keretrendszer alapjául szolgáló megfelelőségi határozatát az FTC által érvényre juttatott kereskedelmi elvektől eltérő kérdések alapján. Az Egyesült Államok és az Európai Bizottság azóta tárgyalásokat folytatott az EU–USA adatvédelmi keretről az EUB ítéletét követően kialakult helyzet kezelése érdekében.

Ezúton megerősítem, hogy az FTC elkötelezett az EU–USA adatvédelmi keret elveinek szigorú érvényesítése mellett. Ezen belül is megerősítjük elkötelezettségünket három kulcsfontosságú területen: 1. megkeresések soron kívüli kezelése és vizsgálatok, 2. végzések kibocsátása és nyomon követése, valamint 3. az uniós adatvédelmi hatóságokkal folytatott végrehajtási együttműködés.

I. **Bevezetés**

a. **Az FTC-nek az adatvédelem végrehajtásával és az adatvédelmi szabályzattal kapcsolatos munkája**

Az FTC széles körű polgári jogi végrehajtási jogkörrel rendelkezik a fogyasztóvédelem és a kereskedelem területén a verseny elősegítése érdekében. A fogyasztóvédelmi jogkörének részeként az FTC a jogszabályok széles körét hajtja végre a fogyasztók és adataik védelme és biztonsága érdekében. Az FTC által végrehajtott elsődleges törvény, az FTC-törvény tiltja

([1]) Edith Ramirez elnök levele Věra Jourovának, az Európai Bizottság jogérvényesülésért, fogyasztópolitikáért és nemek közötti esélyegyenlőségért felelős biztosának az új EU–USA adatvédelmi pajzs keretrendszerének a Szövetségi Kereskedelmi Bizottság általi érvényesítéséről (2016. február 29.), *elérhető a következő internetcímen:* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. Az FTC korábban kötelezettséget vállalt az USA–EU védett adatkikötő program érvényre juttatására is. Robert Pitofsky, az FTC elnökének levele John Mogg, az Európai Bizottság Belső Piaci Főigazgatóságának igazgatója részére (2000. július 14.), *elérhető a következő címen:* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission Jelen levél a korábbi kötelezettségvállalások helyébe lép.

a kereskedelemben végrehajtott vagy arra kiható „tisztességtelen” vagy „megtévesztő” cselekedeteket vagy gyakorlatokat ([2]). Az FTC olyan ágazati törvényeket is végrehajt, amelyek védik az egészségügyi, hitellel és más pénzügyi kérdésekkel kapcsolatos, valamint a gyermekekkel kapcsolatos online információkat, és ezen törvények mindegyikéhez végrehajtási rendeleteket bocsátott ki ([3]).

Az FTC a közelmúltban számos kezdeményezést indított a személyes adatok védelmével kapcsolatos munkánk megerősítésére. 2022 augusztusában az FTC bejelentette, hogy a káros kereskedelmi felügyelet és a nem eléggé szigorú adatbiztonság elleni fellépést célzó szabályok elfogadását mérlegeli ([4]). A projekt célja, hogy megbízható nyilvános nyilvántartást hozzon létre, amely információt ad arról, hogy az FTC-nek ki kell-e dolgoznia a kereskedelmi felügyeleti és adatbiztonsági gyakorlatokkal kapcsolatos szabályokat, és hogy e szabályoknak milyennek kellene lenniük. Üdvözöltük az uniós érdekelt felek ezzel és más kezdeményezésekkel kapcsolatos észrevételeit.

Az adatvédelmi kongresszusainkon továbbra is vezető kutatók gyűlnek össze, hogy megvitassák a fogyasztók adatainak védelmével és az adatbiztonsággal kapcsolatos legújabb kutatásokat és tendenciákat. Javítottuk hatóságunk azon képességét is, hogy lépést tartson a technológiai fejlődéssel, amely az adatvédelmi munkánk nagy részének központi elemét képezi, és egyre több technológiai szakértőből és interdiszciplináris kutatóból álló csapatot építünk ki. Amint azt Ön is tudja, bejelentettük, hogy közös párbeszédre kerül sor Önnel és az Európai Bizottságnál dolgozó kollégáival, amely olyan, a személyes adatok védelmével kapcsolatos témákat foglal magában, mint például a sötét megoldások és a széles körű adatgyűjtés által jellemzett üzleti modellek ([5]). A közelmúltban egy jelentést is benyújtottunk a Kongresszus számára, amelyben figyelmeztettünk a Kongresszus által azonosított online veszélyek mesterséges intelligencia (MI) révén történő kezelésének veszélyeire. Ebben a jelentésben aggályokat fogalmaztunk meg a pontatlansággal, a torzítással, a hátrányos megkülönböztetéssel és a kereskedelmi célú leplezett megfigyeléssel kapcsolatban ([6]).

b. **Az Egyesült Államok által az uniós fogyasztóknak nyújtott jogi védelem**

Az EU–USA adatvédelmi keret az Egyesült Államok tágabb adatvédelmi környezetében fog működni, amely többféle módon is védi az uniós fogyasztókat. Az FTC-törvényben szereplő, a tisztességtelen vagy megtévesztő cselekményekre és gyakorlatokra vonatkozó tilalom nem korlátozódik az egyesült államokbeli fogyasztók egyesült államokbeli vállalatokkal szembeni védelmére, mivel kiterjed azokra a gyakorlatokra is, amelyek 1. észszerűen előrelátható kárt okoznak vagy okozhatnak az Egyesült Államokon belül, illetve 2. az Egyesült Államokban történő érdemi cselekményt foglalnak magukban. Ezenkívül a külföldi fogyasztók védelme során az FTC igénybe vehet minden olyan jogorvoslatot, amely rendelkezésre áll a belföldi fogyasztók védelmére ([7]).

Az FTC más célzott jogszabályokat is végrehajt, amelyek a nem egyesült államokbeli fogyasztókat is védik, ideértve például a gyermekek személyes adatainak az online térben való védelméről szóló törvényt (a továbbiakban: COPPA). Többek között a COPPA előírja, hogy a gyermekeket célzó honlapok és online szolgáltatások, vagy az általános közönségnek szánt oldalak, amelyek tudatosan gyűjtenek személyes adatokat 13 évnél fiatalabb gyermekektől, biztosítsanak szülői figyelmeztetést, és

([2]) 15 U.S.C. § 45(a). Az FTC nem rendelkezik hatáskörrel a bűnüldözéssel vagy a nemzetbiztonsággal kapcsolatos ügyekben. Az FTC a legtöbb egyéb kormányzati intézkedést sem tudja befolyásolni. Ezenkívül az FTC kereskedelmi tevékenységekre vonatkozó hatáskörére is vonatkoznak kivételek, többek között a bankok, légitársaságok és a biztosítási üzletág, továbbá a távközlési szolgáltatók közszolgáltatási tevékenysége tekintetében. Az FTC nem rendelkezik hatáskörrel a legtöbb nonprofit szervezet esetében sem, de van hatásköre olyan hamis jótékonysági szervezetek vagy egyéb nonprofit szervezetek felett, amelyek ténylegesen üzleti alapon működnek. Az FTC hatáskörrel rendelkezik olyan nonprofit szervezetek felett is, amelyek működése a saját üzleti alapon működő tagjaik nyereségét eredményezi, többek között azáltal, hogy jelentős gazdasági előnyöket nyújtanak ezeknek a tagoknak. Néhány esetben az FTC hatásköre egybeesik egyéb bűnüldözési hivatalok hatáskörével. Szoros munkakapcsolatot alakítottunk ki a szövetségi és állami hatóságokkal, és szorosan együttműködünk velük a nyomozások koordinálásában és szükség esetén megkeresések benyújtásában.

([3]) *Lásd*: FTC, Privacy and Security (Adatvédelem és biztonság), https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Lásd*: Sajtóközlemény, Szövetségi Kereskedelmi bizottság, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices [Az FTC fontolóra veszi a kereskedelmi felügyelet és a nem megfelelő adatbiztonsági gyakorlatok javítását célzó szabályok bevezetését], (2022. augusztus 11.), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *Lásd*: Didier Reynders, az Európai Bizottság jogérvényesülésért felelős biztosa és Lina Khan, az Egyesült Államok Szövetségi Kereskedelmi Bizottsága elnöke együttes sajtónyilatkozatát (2022. március 30.), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *Lásd:* Sajtóközlemény, Szövetségi Kereskedelmi Bizottság, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems [FTC-jelentés: az online veszélyek mesterséges intelligencia révén történő leküzdése kockázatokkal jár] (2022. június 16.), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) 15 U.S.C. § 45(a)(4)(B). Továbbá a „tisztességtelen vagy megtévesztő cselekmények és gyakorlatok” magukban foglalnak minden olyan külkereskedelmet érintő cselekményt vagy gyakorlatot, amely i. észszerűen előrelátható kárt okoz vagy okozhat az Egyesült Államokon belül, vagy ii. az Egyesült Államokban történő érdemi cselekményt foglal magában. 15 U.S.C. § 45(a)(4)(A).

kérjenek ellenőrizhető szülői hozzájárulást. A COPPA hatálya alá eső egyesült államokbeli honlapoknak és szolgáltatásoknak, amelyek személyes adatokat gyűjtenek külföldi gyermekektől, meg kell felelniük a COPPA rendelkezéseinek. A külföldön levő honlapoknak és online szolgáltatásoknak is meg kell felelniük a COPPA rendelkezéseinek, ha az Egyesült Államokban levő gyermekeket célozzák, vagy ha tudatosan gyűjtenek személyes adatokat az Egyesült Államokban levő gyermekektől. Továbbá az FTC által végrehajtott egyesült államokbeli szövetségi jogszabályok mellett más szövetségi vagy állami fogyasztóvédelmi és adatvédelmi jogszabályok is biztosíthatnak további előnyöket az uniós fogyasztóknak.

c. **Az FTC jogérvényesítési tevékenysége**

Az FTC mind az USA–EU védett adatkikötő, mind az EU–USA adatvédelmi pajzs keretében indított eljárásokat, és folytatta az EU–USA adatvédelmi pajzs érvényre juttatását, még azt követően is, hogy az EUB érvénytelenítette az EU–USA adatvédelmi pajzs keretrendszerének alapjául szolgáló megfelelőségi határozatot ([8]). Az FTC több közelmúltbeli panasza is tartalmazott olyan állításokat, amelyek szerint egyes vállalkozások megsértették az EU–USA adatvédelmi pajzs rendelkezéseit, többek között a Twitter ([9]), a CafePress ([10]) és a Flo ([11]) elleni eljárásokban. A Twitter elleni jogérvényesítési intézkedés keretében az FTC 150 millió USD összeget szedett be a Twittertől egy korábbi FTC-végzés megsértése miatt, amely több mint 140 millió ügyfelet érintő gyakorlatokat foglalt magában, és többek között megsértette az EU–USA adatvédelmi pajzs 5. alapelvét (Az adatok sértetlensége és a célhoz kötöttség). A hatóság végzése továbbá előírja, hogy a Twitter tegye lehetővé a felhasználók számára, hogy olyan biztonságos, többtényezős hitelesítési módszereket alkalmazzanak, amelyek nem követelik meg a felhasználóktól telefonszámaik megadását.

A CafePress-ügyben az FTC azt állította, hogy a vállalat nem biztosította a fogyasztók különleges adatainak védelmét, eltussolt egy jelentős adatvédelmi incidenst, és megsértette az EU–USA adatvédelmi pajzs 2. (Választási lehetőség), 4. (Biztonság) és 6. (Hozzáférés) elvét. Az FTC végzése előírja a vállalat számára, hogy a nem megfelelő hitelesítési intézkedéseket többtényezős hitelesítéssel váltsa fel, lényegesen korlátozza az általa gyűjtött és őrzött adatok mennyiségét, titkosítsa a társadalombiztosítási azonosítókat, és harmadik féllel vizsgáltassa meg információbiztonsági programjait, valamint bocsásson az FTC rendelkezésére egy nyilvánosságra hozható másolatot.

A Flo-ügyben az FTC azt állította, hogy a cikluskövető alkalmazás közölt bizonyos felhasználói egészségügyi információkat külső adatelemző szolgáltatókkal, miután kötelezettséget vállalt arra, hogy ezeket az információkat bizalmasan kezeli. Az FTC panasza kifejezetten felhívja a figyelmet a vállalatnak az uniós fogyasztókkal való interakciójára, valamint arra, hogy a Flo megsértette az EU–USA adatvédelmi pajzs 1. (Értesítés), 2. (Választási lehetőség), 3. (Újbóli adattovábbításért való elszámoltathatóság) és 5. (Az adatok sértetlensége és célhoz kötöttség) elvét. Az FTC végzése többek között előírja a Flo számára, hogy értesítse az érintett felhasználókat személyes adataik nyilvánosságra hozataláról, és utasítsa a felhasználók egészségügyi adataihoz hozzájutó harmadik feleket, hogy semmisítsék meg ezeket az adatokat. Nagy jelentőségű, hogy az FTC végzései védelmet nyújtanak azoknak a fogyasztóknak az egész világon, akik kapcsolatba lépnek egy egyesült államokbeli vállalkozással, nemcsak azoknak a fogyasztóknak, akik panaszt nyújtottak be.

Számos korábbi, az USA–EU védett adatkikötővel és az EU–USA adatvédelmi pajzs végrehajtásával kapcsolatos ügy érintett olyan szervezeteket, amelyek a Kereskedelmi Minisztériumon keresztül elvégezték az első öntanúsítást, de nem végezték el az éves újratanúsítást, miközben továbbra is aktuális résztvevőként tüntették fel magukat. Más ügyek olyan szervezetek hamis részvételi állításaival voltak kapcsolatosak, amelyek soha nem teljesítették az első öntanúsítást a Kereskedelmi Minisztériumon keresztül. A jövőben arra számítunk, hogy proaktív jogérvényesítési erőfeszítéseinket olyan típusú, az EU–USA adatvédelmi keret elveinek súlyos megsértését jelentő esetekre összpontosítjuk, mint amilyenekre a Twitter-, a CafePress- és a Flo-ügyben állítólagosan sor került. Eközben a Kereskedelmi Minisztérium irányítja és felügyeli az öntanúsítási folyamatot, vezeti az EU–USA adatvédelmi keretben részt vevő szervezetek hiteles listáját, és foglalkozik a programban való részvételre vonatkozó állításokkal kapcsolatos egyéb kérdésekkel ([12]). Fontos megjegyezni, hogy azon szervezetekkel szemben, melyek azt állítják, hogy részt vesznek az EU–USA adatvédelmi keretben, akkor is lehet az EU–USA adatvédelmi keret elveinek érdemi érvényesítését célzó intézkedést foganatosítani, ha a Kereskedelmi Minisztériumon keresztül nem végzik el vagy nem újítják meg az öntanúsításukat.

([8]) *Lásd* az FTC által a védett adatkikötővel és az adatvédelmi pajzzsal kapcsolatban indított eljárások listáját az A. függelékben.

([9]) *Lásd:* Sajtóközlemény, Szövetségi Kereskedelmi Bizottság, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads [Az FTC azzal vádolja a Twittert, hogy a felhasználói profilok biztonsági adatait célzott hirdetések eladásához használja] (2022. május 25.), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *Lásd:* Sajtóközlemény, Szövetségi Kereskedelmi Bizottság, FTC Takes Action against CafePress for Data Breach Cover Up [Az FTC eljárást indít a CafePress ellen adatvédelmi incidens eltussolásáért] (2022. március 15.), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *Lásd*: Sajtóközlemény, Szövetségi Kereskedelmi Bizottság, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others [Az FTC véglegesíti a Flo Health cikluskövető alkalmazásra vonatkozó végzést, amely különleges adatokat osztott meg a Facebookkal, a Google-lel és másokkal] (2021. június 22.), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Marisa Lago, nemzetközi kereskedelemért felelős kereskedelmi miniszterhelyettes levele Didier Reynders, az Európai Bizottság jogérvényesülésért felelős biztosa részére (2022. december 12.).

II. **Megkeresések soron kívüli kezelése és vizsgálatok**

Amint azt az USA–EU védett adatkikötőre vonatkozó keretrendszer és az EU–USA adatvédelmi pajzs keretrendszere keretében tettük, az FTC kötelezettséget vállal arra, hogy kiemelt figyelmet fordít az EU–USA adatvédelmi keret elveivel kapcsolatos, a Kereskedelmi Minisztériumtól és az uniós tagállamoktól érkező megkeresésekre. Prioritásként kezeljük továbbá az adatvédelmi önszabályozó szervezetek és más független vitarendezési szervek által az EU–USA adatvédelmi keret elveinek való meg nem felelés miatt benyújtott megkeresések vizsgálatát.

Az EU–USA adatvédelmi keret alapján uniós tagállamokból érkező megkeresések elősegítése érdekében az FTC egy szabványos megkeresési folyamatot hozott létre és iránymutatást nyújtott az uniós tagállamoknak arról, hogy milyen típusú információk tudják a legjobban segíteni az FTC-t a megkeresés kivizsgálása során. Ennek keretében az FTC kijelölt egy hivatali kapcsolattartó pontot az uniós tagállamok megkeresései számára. Nagyon hasznos, ha a megkeresést benyújtó hatóság előzetesen megvizsgálja az állítólagos jogsértést, és együtt tud működni az FTC-vel a vizsgálatban.

A Kereskedelmi Minisztériumból, uniós tagállamból vagy önszabályozó szervezettől vagy más független vitarendezési szervtől jövő megkeresés kézhezvétele után az FTC számos intézkedést tehet a felvetett kérdések kezelésére. Például megvizsgálhatjuk a szervezet adatvédelmi szabályzatát, további információkat szerezhetünk be közvetlenül a szervezettől vagy harmadik felektől, tovább vizsgálódhatunk a megkeresést benyújtó jogi személlyel, megállapíthatjuk, hogy a jogsértés rendszeres-e vagy jelentős számú fogyasztó érintett-e, meghatározhatjuk, hogy a megkeresés olyan kérdéseket is felvet-e, amelyek a Kereskedelmi Minisztérium hatáskörébe tartoznak, megállapíthatjuk, hogy a piaci résztvevők figyelmeztetésére irányuló további erőfeszítések segíthetnek-e, és szükség esetén végrehajtási eljárást kezdeményezhetünk.

Amellett, hogy prioritásként kezeli az EU–USA adatvédelmi keret elveivel kapcsolatos, a Kereskedelmi Minisztériumtól, az uniós tagállamoktól, valamint a személyes adatok védelmével foglalkozó önszabályozó szervezetektől vagy más független vitarendezési szervektől érkező felkéréseket, ([13]) az FTC – számos eszköz felhasználásával – adott esetben továbbra kivizsgálja saját kezdeményezésére az EU–USA adatvédelmi keret elvei megsértésének jelentős eseteit. Az FTC kereskedelmi szervezeteket érintő adatvédelmi és biztonsági kérdések vizsgálatára irányuló programjának részeként az ügynökség rutinszerűen vizsgálta, hogy a szóban forgó jogi személy tett-e nyilatkozatot az EU–USA adatvédelmi pajzsra vonatkozóan. Ha a jogi személy ilyen nyilatkozatokat tett és a vizsgálat azt állapította meg, hogy nyilvánvalóan megsértette az EU–USA adatvédelmi pajzs elveit, az FTC a végrehajtási intézkedésének részeként az EU–USA adatvédelmi pajzs megsértését is vélelmezte. Folytatni fogjuk ezt a proaktív megközelítést, immár az EU–USA adatvédelmi keret elvei tekintetében.

III. **Végzések kibocsátása és nyomon követése**

Az FTC megerősíti azt a kötelezettségvállalását is, hogy végrehajtási végzéseket bocsát ki az EU–USA adatvédelmi keret elveinek való megfelelés biztosítása érdekében, és nyomon követi ezeket. Az EU–USA adatvédelmi keret elveinek történő megfelelést számos megfelelő, gyorsított beavatkozásra vonatkozó rendelkezés révén fogjuk megkövetelni, amelyek az FTC jövőbeli, az EU–USA adatvédelmi keret elveire vonatkozó végzéseiben fognak szerepelni. Az FTC közigazgatási végzéseinek a megsértése maximum 50 120 USD összegű bírságot eredményezhet jogsértésenként vagy folytonos jogsértés esetén napi 50 120 USD összegű bírságot ([14]), amely sok fogyasztót érintő gyakorlat esetén több millió dollárt is elérhet. Mindegyik önkéntes megállapodásról szóló végzésnek vannak jelentéskészítési és megfelelési rendelkezései. A végzés alanyának olyan dokumentumokkal kell rendelkeznie, amely bemutatja a megfelelését a meghatározott, többéves időszakban. A végzéseket a végzés teljesítéséért felelős munkatársakhoz is továbbítani kell.

Az FTC szisztematikusan nyomon követi az EU–USA adatvédelmi pajzs elveinek való megfelelés kapcsán már kiadott végzéseket, csakúgy, mint az összes végzését, és szükség esetén intézkedéseket tesz azok érvényesítése érdekében ([15]). Nagy jelentőségű, hogy az FTC végzései továbbra is védelmet nyújtanak mindazon fogyasztóknak az egész világon, akik kapcsolatba lépnek egy vállalkozással, nemcsak azoknak a fogyasztóknak, akik panaszt nyújtottak be. Végezetül az FTC online jegyzéket vezet azokról a vállalatokról, amelyek az EU–USA adatvédelmi keret elveinek érvényesítésével kapcsolatos végzések hatálya alá tartoznak ([16]).

([13]) Habár az FTC egyéni fogyasztói panaszokat nem rendez, valamint nem közvetít ezekben, az FTC megerősíti, hogy elsőbbséget biztosít az uniós adatvédelmi hatóságok EU–USA adatvédelmi kerettel kapcsolatos megkereséseinek. Ezenkívül, az FTC a panaszokat feltünteti a fogyasztóőr adatbázisában, amely hozzáférhető sok más bűnüldözési hivatal számára, a trendek azonosítása, a végrehajtási prioritások meghatározása és a vizsgálatok célpontjainak az azonosítása érdekében. Az uniós polgárok ugyanazt a panaszkezelő rendszert használhatják, amely az egyesült államokbeli fogyasztók számára rendelkezésre áll a panaszok FTC-hez történő benyújtására a https://reportfraud.ftc.gov/ internetes címen. Az EU–USA adatvédelmi keret elveivel kapcsolatos panaszok esetén azonban a legjobb az lehet az uniós polgárok számára, ha a panaszokat a tagállami adatvédelmi hatósághoz vagy független vitarendezési szervhez nyújtják be.

([14]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Ezt az összeget időszakonként az inflációnak megfelelően kiigazítjuk.

([15]) Tavaly az FTC megszavazta a visszaeső elkövetők kivizsgálási folyamatának egyszerűsítését. *Lásd:* FTC Authorises Investigations in Key Enforcement Priorities [Az FTC engedélyezi a kulcsfontosságú végrehajtási prioritásokat érintő vizsgálatokat] (2021. július 1.), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Im.* FTC, Adatvédelmi pajzs, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Az uniós adatvédelmi hatóságokkal folytatott végrehajtási együttműködés**

Az FTC elismeri az uniós adatvédelmi hatóságok által az EU–USA adatvédelmi keretnek való megfeleléssel kapcsolatban játszott fontos szerepet, és támogatja a fokozott együttműködést a tanácskozás és a végrehajtás során. A jelenlegi digitális piaci fejlemények és az adatintenzív üzleti modellek jelentette kihívások összehangolt megközelítése egyre kritikusabb fontosságú. Az FTC információcserét fog folytatni a megkeresésekre vonatkozóan a megkeresést benyújtó végrehajtási hatóságokkal, beleértve a megkeresések státusát, a titkosságra vonatkozó jogszabályok vagy korlátozások teljesítése mellett. A fogadott megkeresések számától és típusától függően, amennyiben lehetséges, a nyújtott tájékoztatás tartalmazza a tárgyi ügyek értékelését, beleértve a felvetett jelentős kérdések leírását és az FTC hatáskörébe tartozó jogsértések kezelése érdekében foganatosított intézkedéseket. Az FTC visszajelzést is ad a megkeresést benyújtó hatóságnak a kapott megkeresések típusáról a jogsértő magatartás kezelése érdekében tett erőfeszítések hatékonyságának növelése érdekében. Ha a megkeresést benyújtó hatóság információt kér egy adott megkeresés státusáról annak érdekében, hogy a saját végrehajtási eljárását lefolytathassa, az FTC a vizsgálat alatt álló megkeresések számát figyelembe véve, a titkosságra vonatkozó és más jogi előírások betartása mellett válaszolni fog.

Az FTC szorosan együttműködik az uniós adatvédelmi hatóságokkal a végrehajtáshoz történő segítségnyújtás érdekében is. Adott esetben ebbe beletartozhat információk megosztása és segítségnyújtás vizsgálatban az USA „SAFE WEB" (biztonságos web) törvénye szerint, amely felhatalmazza az FTC-t arra, hogy segítséget nyújtson külföldi bűnüldözési hatóságoknak, ha a külföldi hivatal olyan gyakorlatokat megtiltó jogszabályokat érvényesít, amelyek lényegileg hasonlóak azokhoz a jogszabályokhoz, amelyeket az FTC hajt végre ([17]). Az ilyen segítségnyújtás részeként az FTC megoszthatja az FTC vizsgálatával kapcsolatban kapott információkat, kötelező erejű eljárást indíthat a saját vizsgálatát lefolytató uniós adatvédelmi hatóság nevében, és szóbeli vallomást kérhet tanúktól vagy alperesektől az adatvédelmi hatóság végrehajtási eljárásával kapcsolatban, az USA biztonságos web törvénye előírásainak teljesítése mellett. Az FTC rendszeresen él ezzel a jogkörével, hogy segítsen más hatóságoknak a világban az adatvédelmi és fogyasztóvédelmi ügyekben.

Az esetspecifikus ügyekben megkeresést benyújtó uniós adatvédelmi hatóságokkal folytatott tanácskozás mellett az FTC rendszeres megbeszéléseken vesz részt az Európai Adatvédelmi Testület kijelölt képviselőivel annak megvitatása érdekében, hogyan lehet általánosságban javítani a végrehajtási együttműködést. Az FTC részt vesz a Kereskedelmi Minisztériummal, az Európai Bizottsággal és az EDPB képviselőivel együtt az EU–USA adatvédelmi keret időszakos felülvizsgálatában, ahol megvitatják annak megvalósítását. Az FTC bátorítja olyan eszközök kidolgozását is, amelyek javítják az uniós adatvédelmi hatóságokkal, valamint a világ más adatvédelmi végrehajtó hatóságaival a végrehajtás során folytatott együttműködést. Az FTC örömmel erősíti meg elkötelezettségét az EU–USA adatvédelmi keret kereskedelmi ágazati vonatkozásainak érvényesítése mellett. Úgy véljük, hogy az uniós kollégákkal való partnerségünk döntő fontosságú ahhoz, hogy mind a mi polgáraink, mind az Önök polgárai számára biztosítsuk a magánélet védelmét.

Üdvözlettel:

Lina M. Khan
a Szövetségi Kereskedelmi Bizottság elnöke

([17]) Annak meghatározása során, hogy éljen-e az USA biztonságos web törvénye szerinti jogkörével, az FTC többek között az alábbiakat mérlegeli: „A) a kérelmező hatóság elfogadta-e, hogy kölcsönösen segítséget nyújt vagy fog nyújtani a jövőben a Bizottságnak, B) a kérelem teljesítése sérti-e az Egyesült Államok közérdekét, és C) a kérelmező hatóság vizsgálata vagy végrehajtási eljárása olyan cselekményekre vagy gyakorlatokra vonatkozik-e, amelyek sérelmet okoznak vagy várhatóan okozhatnak jelentős számú személy számára." 15 U.S.C. § 46(j)(3). Ez a jogkör nem vonatkozik versenyjogi jogszabályok érvényesítésére.

A. függelék

Az adatvédelmi pajzzsal és a védett adatkikötővel kapcsolatos jogérvényesítés

	Docket/FTC file (ügyszám)	**Ügy**	**Link**
1.	FTC File No. 2023062 3:22-cv-03070. sz. bírósági ügy (N. D. Cal.)	US kontra **Twitter, Inc.**	Twitter
2.	FTC File No. 192 3209	Residual Pumpkin Entity, LLC, korábban: d/b/a **CafePress**, és PlanetArt, LLC, d/b/a **CafePress**	CafePress
3.	FTC File No. 192 3133 Docket No. C-4747	Flo Health, Inc.	Flo Health
4.	FTC File No. 192 3050 Docket No. C-4723	Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5.	FTC File No. 192 3092 Docket No. C-4709	T&M Protection, LLC	T&M Protection
6.	FTC File No. 192 3084 Docket No. C-4704	TDARX, Inc.	TDARX
7.	FTC File No. 192 3093 Docket No. C-4706	Global Data Vault, LLC	Global Data
8.	FTC File No. 192 3078 Docket No. C-4703	Incentive Services, Inc.	Incentive Services
9.	FTC File No. 192 3090 Docket No. C-4705	Click Labs, Inc.	Click Labs
10.	FTC File No. 182 3192 Docket No. C-4697	Medable, Inc.	Medable
11.	FTC File No. 182 3189 Docket No. 9386	NTT Global Data Centers Americas, Inc., mint a **RagingWire Data Centers, Inc.** jogutódja	RagingWire
12.	FTC File No. 182 3196 Docket No. C-4702	Thru, Inc.	Thru
13.	FTC File No. 182 3188 Docket No. C-4698	DCR Workforce, Inc.	DCR Workforce
14.	FTC File No. 182 3194 Docket No. C-4700	LotaData, Inc.	LotaData
15.	FTC File No. 182 3195 Docket No. C-4701	EmpiriStat, Inc.	EmpiriStat

16.	FTC File No. 182 3193 Docket No. C-4699	214 Technologies, Inc., **Trueface.ai** név alatt is kereskedik	Trueface.ai
17.	FTC File No. 182 3107 Docket No. 9383	Cambridge Analytica, LLC	Cambridge Analytica
18.	FTC File No. 182 3152 Docket No. C-4685	SecureTest, Inc.	SecurTest
19.	FTC File No. 182 3144 Docket No. C-4664	VenPath, Inc.	VenPath
20.	FTC File No. 182 3154 Docket No. C-4666	SmartStart Employment Screening, Inc.	SmartStart
21.	FTC File No. 182 3143 Docket No. C-4663	**mResourceLLC,** Loop Works LLC név alatt kereskedik	mResource
22.	FTC File No. 182 3150 Docket No. C-4665	Idmission LLC	IDmission
23.	FTC File No. 182 3100 Docket No. C-4659	ReadyTech Corporation	ReadyTech
24.	FTC File No. 172 3173 Docket No. C-4630	Decusoft, LLC	Decusoft
25.	FTC File No. 172 3171 Docket No. C-4628	Tru Communication, Inc.	Tru
26.	FTC File No. 172 3172 Docket No. C-4629	Md7, LLC	Md7
30.	FTC File No. 152 3198 Docket No. C-4543	Jhayrmaine Daniels (California Skate-Line név alatt kereskedik)	Jhayrmaine Daniels
31.	FTC File No. 152 3190 Docket No. C-4545	Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32.	FTC File No. 152 3141 Docket No. C-4540	Golf Connect, LLC	Golf Connect
33.	FTC File No. 152 3202 Docket No. C-4546	Inbox Group, LLC	Inbox Group
34.	File No. 152 3187 Docket No. C-4542	IOActive, Inc.	IOActive
35.	FTC File No. 152 3140 Docket No. C-4549	Jubilant Clinsys, Inc.	Jubilant
36.	FTC File No. 152 3199 Docket No. C-4547	Just Bagels Manufacturing, Inc.	Just Bagels

37.	FTC File No. 152 3138 Docket No. C-4548	NAICS Association, LLC	NAICS
38.	FTC File No. 152 3201 Docket No. C-4544	One Industries Corp.	One Industries
39.	FTC File No. 152 3137 Docket No. C-4550	Pinger, Inc.	Pinger
40.	FTC File No. 152 3193 Docket No. C-4552	SteriMed Medical Waste Solutions	SteriMed
41.	FTC File No. 152 3184 Docket No. C-4541	Contract Logix, LLC	Contract Logix
42.	FTC File No. 152 3185 Docket No. C-4551	Forensics Consulting Solutions, LLC	Forensics Consulting
43.	FTC File No. 152 3051 Docket No. C-4526	American Int'l Mailing, Inc.	AIM
44.	FTC File No. 152 3015 Docket No. C-4525	TES Franchising, LLC	TES
45.	FTC File No. 142 3036 Docket No. C-4459	American Apparel, Inc.	American Apparel
46.	FTC File No. 142 3026 Docket No. C-4469	Fantage.com, Inc.	Fantage
47.	FTC File No. 142 3017 Docket No. C-4461	Apperian, Inc.	Apperian
48.	FTC File No. 142 3018 Docket No. C-4462	Atlanta Falcons Football Club, LLC	Atlanta Falcons
49.	FTC File No. 142 3019 Docket No. C-4463	Baker Tilly Virchow Krause, LLP	Baker Tilly
50.	FTC File No. 142 3020 Docket No. C-4464	BitTorrent, Inc.	BitTorrent
51.	FTC File No. 142 3022 Docket No. C-4465	Charles River Laboratories, Int'l	Charles River
52.	FTC File No. 142 3023 Docket No. C-4466	DataMotion, Inc.	DataMotion
53.	FTC File No. 142 3024 Docket No. C-4467	**DDC Laboratories, Inc.**, d/b/a DNA Diagnostics Center	DDC
54.	FTC File No. 142 3028 Docket No. C-4470	Level 3 Communications, LLC	Level 3

55.	FTC File No. 142 3025 Docket No. C-4468	**PDB Sports, Ltd.**, d/b/a the Denver Broncos Football Club, LLP	Broncos
56.	FTC File No. 142 3030 Docket No. C-4471	Reynolds Consumer Products, Inc.	Reynolds
57.	FTC File No. 142 3031 Docket No. C-4472	Receivable Management Services Corporation	Receivable Mgmt
58.	FTC File No. 142 3032 Docket No. C-4473	Tennessee Football, Inc.	Tennessee Football
59.	FTC File No. 102 3058 Docket No. C-4369	Myspace LLC	Myspace
60.	FTC File No. 092 3184 Docket No. C-4365	Facebook, Inc.	Facebook
61.	FTC File No. 092 3081 Polgári per száma: 09-CV-5276 (C. D. Cal.)	FTC kontra Javian Karnani, és **Balls of Kryptonite, LLC**, Bite Size Deals, LLC, és Best Priced Brands, LLC néven kereskedik	Balls of Kryptonite
62.	FTC File No. 102 3136 Docket No. C-4336	Google, Inc.	Google
63.	FTC File No. 092 3137 Docket No. C-4282	World Innovators, Inc.	World Innovators
64.	FTC File No. 092 3141 Docket No. C-4271	Progressive Gaitways LLC	Progressive Gaitways
65.	FTC File No. 092 3139 Docket No. C-4270	Onyx Graphics, Inc.	Onyx Graphics
66.	FTC File No. 092 3138 Docket No. C-4269	ExpatEdge Partners, LLC	ExpatEdge
67.	FTC File No. 092 3140 Docket No. C-4281	Directors Desk LLC	Directors Desk
68.	FTC File No. 092 3142 Docket No. C-4272	Collectify LLC	Collectify

V. MELLÉKLET

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

2023. július 6.

Didier Reynders biztos
Európai Bizottság
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Tisztelt Reynders biztos úr!

Az Egyesült Államok Közlekedési Minisztériuma (a továbbiakban: Minisztérium vagy DOT) nagyra értékeli a lehetőséget, hogy ismertetheti az EU–USA adatvédelmi keret elveinek végrehajtásában játszott szerepét. Egyre inkább összekapcsolt világunkban az EU–USA adatvédelmi keret kritikus szerepet játszik a kereskedelmi tranzakciók keretében továbbított személyes adatok védelmében. Lehetővé teszi a vállalkozások számára, hogy fontos tevékenységeket végezzenek a globális gazdaságban, ugyanakkor biztosítja az uniós fogyasztók fontos adatvédelmének fenntartását.

A DOT először az Európai Bizottságnak több mint 22 évvel ezelőtt küldött levelében nyilvánította ki nyilvánosan az elkötelezettségét az Egyesült Államok és az EU közötti védett adatkikötőre vonatkozó keretrendszer érvényre juttatása mellett. Ezeket a kötelezettségvállalásokat az EU–USA adatvédelmi pajzs keretéről szóló 2016. évi levélben megismételték és kiegészítették. A DOT az említett levelekben ígéretet tett arra, hogy szigorúan érvényesíti az USA–EU védett adatkikötő adatvédelmi elveit, majd az EU–USA adatvédelmi pajzs elveit. A DOT ezt a kötelezettségvállalást kiterjeszti az EU–USA adatvédelmi keret elveire, és ez a levél emlékeztet e kötelezettségvállalásra.

A DOT megerősíti elkötelezettségét a következő kulcsfontosságú területeken: 1. az EU–USA adatvédelmi keret elvei állítólagos megsértései kivizsgálásának rangsorolása, 2. megfelelő végrehajtási intézkedések az EU–USA adatvédelmi keretben való részvételre vonatkozó hamis vagy megtévesztő állításokat benyújtó szervezetekkel szemben, valamint 3. az EU–USA adatvédelmi keret elvei megsértésének nyomon követése és az azokkal kapcsolatos hatósági végrehajtási határozatok meghozatala. Tájékoztatást adunk az egyes kötelezettségvállalásokról és a szükséges mértékben a DOT eddigi szerepéről a fogyasztói adatvédelem területén és az EU–USA adatvédelmi keret elveinek végrehajtása során.

1. **Háttér**

A. A DOT adatvédelmi hatásköre

A Minisztérium erősen elkötelezett a fogyasztók által a légitársaságok és jegyértékesítők számára megadott adatok védelmének biztosítása iránt.

A DOT e területen való fellépésére vonatkozó hatásköre a Szövetségi Törvénykönyv 49. címének 41712. szakaszában (49 U.S.C. 41712) található, amely megtiltja a fuvarozónak vagy a jegyértékesítőnek, hogy „tisztességtelen vagy megtévesztő gyakorlatot” folytasson a légi közlekedés vagy a légi közlekedés értékesítése terén. A 41712. szakasz a Szövetségi Kereskedelmi Bizottságról (FTC) szóló törvény (15 U. S. C. 45) 5. szakasza mintájára épül fel.

A DOT a közelmúltban olyan rendeleteket adott ki, amelyek meghatározzák a tisztességtelen és megtévesztő gyakorlatokat, összhangban a DOT és az FTC által kiadott korábbi határozatokkal (14 CFR § 399.79). Egy gyakorlat akkor tisztességtelen, ha olyan jelentős sérelmet okoz vagy várhatóan okoz, amelyet észszerű módon nem tudnak a fogyasztók elkerülni, vagy a számukra biztosított előnyökkel vagy verseny révén ellensúlyozni.

Egy gyakorlat „megtévesztőnek” minősül a fogyasztók számára, ha valószínűsíthetően megtéveszti az adott körülmények között észszerűen eljáró fogyasztót egy lényeges kérdésben. Egy kérdés akkor lényeges, ha valószínűleg hatással volt a fogyasztó valamely termékkel vagy szolgáltatással kapcsolatos magatartására vagy döntésére. Ezen általános elveken kívül a DOT a 41712. szakaszt úgy értelmezi, hogy az megtiltja a fuvarozóknak és a jegyértékesítőknek az alábbiakat: 1. az adatvédelmi szabályzatuk rendelkezéseinek megsértése, 2. a Minisztérium által kiadott bármely olyan szabály megsértése, amely bizonyos adatvédelmi gyakorlatokat tisztességtelennek vagy megtévesztőnek minősít, vagy 3. a gyermekek személyes adatainak az online térben való védelméről szóló törvény (COPPA) vagy a COPPA-t végrehajtó FTC-szabályok megsértése, vagy 4. az EU–USA adatvédelmi keret résztvevőjeként a keret elveinek való meg nem felelés ([1]).

A fentiek szerint a szövetségi jogszabályok szerint a DOT kizárólagos jogkörrel rendelkezik a légitársaságok adatvédelmi gyakorlatainak a szabályozására, és az FTC-vel közös hatásköre van a jegyértékesítők légi közlekedés értékesítése során folytatott adatvédelmi gyakorlata tekintetében.

Ennek keretében, ha egy légi fuvarozó vagy légi közlekedés értékesítő nyilvánosan kötelezettséget vállal az EU–USA adatvédelmi keret elveinek betartására, akkor a Minisztérium a 41712. szakasz szerinti törvényi jogkörében biztosítani tudja az elvek betartását. Amennyiben tehát egy utas információt közöl egy olyan fuvarozóval vagy jegyértékesítővel, amely vállalta az EU–USA adatvédelmi keret elveinek a követését, akkor az elvek be nem tartása a 41712. szakasz megsértésének minősülne.

B. Végrehajtási gyakorlat

A Minisztérium Légi Közlekedési Fogyasztóvédelmi Hivatala (OACP) ([2]) vizsgálatot indít és eljár a 49 U. S. C. 41712 alá tartozó esetekben. Elsősorban tárgyalások útján – abbahagyásra kötelező közigazgatási határozatok kiadása és polgári bírságokat kirovó végzések révén – érvényesíti a tisztességtelen vagy megtévesztő gyakorlatok 41712. szakasz szerinti törvényi tilalmát. A hivatal az esetleges jogsértésekről leginkább magánszemélyektől, utazási irodáktól, légitársaságoktól, valamint az Egyesült Államok és más országok kormányzati ügynökségeitől értesül. A fogyasztók a DOT honlapját használhatják a légitársaságok és jegyértékesítők elleni adatvédelmi panaszok benyújtására ([3]).

Ha egy ügyben nem jutnak észszerű és megfelelő megállapodásra, az OACP hatáskörében áll végrehajtási eljárást kezdeményezni, amelynek része a DOT közigazgatási bírája (ALJ) előtti bizonyítási célú meghallgatás. Az ALJ hatáskörében áll abbahagyásra kötelező közigazgatási határozatok kiadása és polgári bírságok kiszabása. A 41712. szakasz megsértése abbahagyásra kötelező közigazgatási határozat kiadását és polgári bírság kiszabását vonhatja maga után, amelynek összege a 41712. szakasz minden egyes megsértése esetén maximum 37 377 USD.

A Minisztériumnak nem áll hatáskörében kártérítés vagy pénzügyi jóvátétel megítélése az egyéni felperes számára. A Minisztérium azonban hatáskörrel rendelkezik az OACP által folytatott vizsgálatok eredményeképpen elért olyan megállapodások jóváhagyására, amelyek a fogyasztók közvetlen kártalanítását eredményezik (pl. készpénz, kupon) az egyébként az Egyesült Államok kormánya számára fizetendő bírságok kiváltására. A múltban így történt, és amennyiben a körülmények szükségessé teszik, az EU–USA adatvédelmi keret elvei kapcsán is így történhet. Ha egy légitársaság ismételten megsérti a 41712. szakasz rendelkezéseit, ez megkérdőjelezi a társaság hajlandóságát az elvek betartására, ami szélsőséges esetekben oda vezethet, hogy a társaságot működésre alkalmatlannak minősítik, és ezáltal elveszti jogát a gazdasági működésre.

Eddig a DOT viszonylag kevés olyan panaszt kapott, amely adatvédelmi rendelkezések jegyértékesítők vagy légitársaságok általi állítólagos megsértésére vonatkozott. Ilyen esetekben a fenti elvek szerint történik a vizsgálat.

C. A DOT által az uniós fogyasztóknak nyújtott jogvédelem

A 41712. szakasz alapján a tisztességtelen vagy megtévesztő gyakorlatok tilalma a légi közlekedésben vagy légi közlekedés értékesítésében egyesült államokbeli és külföldi légi fuvarozókra, valamint jegyértékesítőkre vonatkozik. A DOT gyakran intézkedik egyesült államokbeli és külföldi légitársaságok ellen olyan gyakorlatok miatt, amelyek mind külföldi, mind egyesült államokbeli fogyasztókat érintenek annak alapján, hogy a légitársaság gyakorlata az Egyesült Államokba irányuló vagy onnan kiinduló közlekedés során történik. A DOT igénybe vesz minden olyan jogorvoslatot, amely rendelkezésre áll mind a külföldi, mind az egyesült államokbeli fogyasztók szabályozott jogi személyek légi közlekedésben folytatott tisztességtelen vagy megtévesztő gyakorlatai elleni védelme érdekében, és továbbra is így fog tenni.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Korábban a Légi Közlekedési Végrehajtási és Eljárási Hivatal néven volt ismert.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

A DOT a légitársaságok tekintetében más célzott jogszabályokat is végrehajt, amelyek a nem egyesült államokbeli fogyasztókat is védik, ideértve például a gyermekek személyes adatainak az online térben való védelméről szóló törvényt (a továbbiakban: COPPA). Többek között a COPPA előírja, hogy a gyermekeket célzó honlapok és online szolgáltatások, vagy az általános közönségnek szánt oldalak, amelyek tudatosan gyűjtenek személyes adatokat 13 évnél fiatalabb gyermekektől, tartalmazzanak a szülőknek szóló figyelmeztetést, és kérjenek ellenőrizhető szülői hozzájárulást. A COPPA hatálya alá eső egyesült államokbeli honlapoknak és szolgáltatásoknak, amelyek személyes adatokat gyűjtenek külföldi gyermekektől, meg kell felelniük a COPPA rendelkezéseinek. A külföldön levő honlapoknak és online szolgáltatásoknak is meg kell felelniük a COPPA rendelkezéseinek, ha az Egyesült Államokban levő gyermekeket célozzák, vagy ha tudatosan gyűjtenek személyes adatokat az Egyesült Államokban levő gyermekektől. Amennyiben az Egyesült Államokban üzleti tevékenységet folytató egyesült államokbeli vagy külföldi légitársaságok megsértik a COPPA rendelkezéseit, a DOT hatáskörrel rendelkezik végrehajtási intézkedés meghozatalára.

II. **Az EU–USA adatvédelmi keret elveinek érvényesítése**

Ha egy légitársaság vagy jegyértékesítő úgy dönt, hogy részt vesz az EU–USA adatvédelmi keretben és a Minisztériumhoz olyan panasz érkezik, amely szerint a légitársaság vagy a jegyértékesítő állítólagosan megsértette a keret elveit, a Minisztérium az alábbi lépéseket teszi a keret hatékony végrehajtása érdekében.

A. Állítólagos jogsértések soron kívüli kivizsgálása

A Minisztérium Légi Közlekedési Fogyasztóvédelmi Hivatala kivizsgál minden egyes panaszt, amely az EU–USA adatvédelmi keret megsértését állítja, beleértve az uniós adatvédelmi hatóságoktól kapott panaszokat, és végrehajtási intézkedéseket tesz, ha bizonyíték van a jogsértésre.

Ezenkívül az OACP együttműködik az FTC-vel és a Kereskedelmi Minisztériummal és soron kívül foglalkozik azokkal az állításokkal, amelyek szerint a szabályozás alá eső jogi személyek nem teljesítik az adatvédelmi kerettel összefüggő adatvédelmi kötelezettségvállalásaikat.

Az EU–USA adatvédelmi keret elveinek állítólagos megsértésére vonatkozó panasz kézhezvétele után az OACP számos intézkedést tehet a vizsgálatának részeként. Például kivizsgálhatja a jegyértékesítő vagy a légitársaság adatvédelmi szabályzatát, további információkat szerezhet be a jegyértékesítőtől vagy légitársaságtól vagy harmadik felektől, tovább vizsgálódhat a megkeresést benyújtó személlyel, megállapíthatja, hogy rendszeres-e a jogsértés, vagy jelentős számú fogyasztó érintett-e. Ezenkívül meghatározhatja, hogy a kérdés a Kereskedelmi Minisztérium vagy az FTC hatáskörébe eső ügyeket érint-e, hogy fogyasztói vagy vállalkozói képzés segíthet-e, és szükség esetén végrehajtási eljárást kezdeményezhet.

Ha a Minisztérium tudomást szerez arról, hogy a jegyértékesítők esetlegesen megsértik az EU–USA adatvédelmi keret elveit, egyeztetni fog az FTC-vel az ügyben. Emellett tájékoztatást adunk az FTC és a Kereskedelmi Minisztérium számára az EU–USA adatvédelmi keret elveinek érvényesítésére irányuló intézkedések eredményéről.

B. Hamis vagy megtévesztő részvételi nyilatkozatok kezelése

A Minisztérium továbbra is elkötelezett az EU–USA adatvédelmi keret elvei megsértésének kivizsgálása iránt, beleértve az abban való részvételre vonatkozó hamis vagy megtévesztő nyilatkozatokat. Soron kívül vizsgáljuk a Kereskedelmi Minisztérium által olyan szervezetekkel kapcsolatban benyújtott megkereséseket, amelyekről a Minisztérium megállapítja, hogy helytelenül állítják magukról, hogy jelenleg az EU–USA adatvédelmi keret résztvevői vagy engedély nélkül használják a keret tanúsító védjegyét.

Ezenkívül kiemeljük, hogy ha egy szervezet adatvédelmi szabályzata azt állítja, hogy megfelel az EU–USA adatvédelmi keret elveinek, akkor ha elmulasztja az öntanúsítást a Kereskedelmi Minisztériumnál vagy annak megújítását, az várhatóan önmagában nem mentesíti a szervezetet az alól, hogy a DOT kikényszerítse a kötelezettségvállalását.

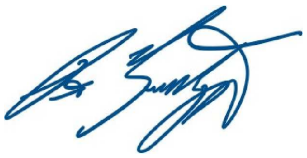
C. Az EU–USA adatvédelmi kerettel kapcsolatos végrehajtási végzések nyomon követése és közzététele

A Minisztérium Légi Közlekedési Fogyasztóvédelmi Hivatala továbbra is elkötelezett aziránt, hogy nyomon kövesse a végrehajtási végzéseket az EU–USA adatvédelmi keret elvei teljesítésének biztosítása érdekében. Konkrétan, ha a hivatal olyan végzést ad ki, amely utasítja a légitársaságot vagy jegyértékesítőt az EU–USA adatvédelmi keret elvei és a 41712. szakasz jövőbeli megsértésének abbahagyására, akkor nyomon követi a végzésben foglalt, abbahagyásra vonatkozó rendelkezés teljesítését. Ezenkívül a hivatal biztosítja, hogy az EU–USA adatvédelmi keret elveivel kapcsolatos ügyekből eredő végzések elérhetők legyenek a honlapján.

Várakozással tekintünk a szövetségi partnereinkkel és uniós érintett felekkel végzett munkánk folytatása elé az EU–USA adatvédelmi kerettel kapcsolatos ügyekben.

Remélem, hogy a fenti tájékoztatás hasznosnak bizonyul. Amennyiben még kérdése van, vagy további felvilágosításra volna szüksége, kérem, forduljon hozzám bizalommal.

Üdvözlettel:



Pete Buttigieg

VI. MELLÉKLET

Az USA Igazságügyi Minisztériuma

Büntetőjogi Főosztály

Főügyészhelyettesi Hivatal Washington, 20530

2023. június 23.

Ana Gallego Torres asszony
Jogérvényesülési és Fogyasztópolitikai Főigazgatóság
Európai Bizottság
Rue Montoyer/Montoyerstraat 59
1049 Brüsszel
Belgium

Tisztelt Gallego Torres főigazgató asszony!

Ez a levél rövid áttekintést nyújt az Egyesült Államokban a kereskedelmi adatok és más vállalati információk bűnüldözési vagy közérdekű (polgári és közigazgatási) célú beszerzésére használt elsődleges nyomozati eszközökről, ideértve az ezekben a hatáskörökben meghatározott betekintési korlátokat ([1]). Az e levélben ismertetett jogi eljárások megkülönböztetésmentesek annyiban, hogy azokat használják az Egyesült Államokban a vállalatoktól történő információszerzéshez, ideértve azokat a vállalatokat is, amelyek önmaguk tanúsítják az EU–USA adatvédelmi keretnek való megfelelésüket, tekintet nélkül az érintett állampolgárságára vagy tartózkodási helyére. Emellett azok a vállalatok, amelyek ellen az Egyesült Államokban jogi eljárás indul, azt az alább kifejtettek szerint bíróságon megtámadhatják ([2]).

A hatóságok általi adatelkobzás tekintetében különösen jelentős az Egyesült Államok Alkotmányának negyedik kiegészítése, amely kimondja, hogy „[a]z emberek jogát személyük, házuk, okmányaik és tulajdonuk biztonságához, valamint megalapozatlan házkutatások és lefoglalások elleni védelmét nem lehet megsérteni; ilyen parancsokat csak alapos indokkal, esküvel vagy fogadalommal alátámasztott ügyben lehet kibocsátani, és részletesen meg kell jelölni a házkutatás helyét és a lefoglalandó dolgot, illetve a letartóztatandó személyt". az Egyesült Államok Alkotmányának IV. kiegészítése. Ahogy az Egyesült Államok Legfelsőbb Bírósága a Berger kontra State of New York ügyben kimondta, „[a] kiegészítés alapvető célja, amint azt ezen bíróság számos döntése is elismerte, az egyének magánéletének és biztonságának a kormányzati tisztviselők önkényes beavatkozásával szembeni védelme". 388 U.S. 41, 53 (1967) (idézi a Camara kontra Mun. Court of San Francisco ügyet, 387 U.S. 523, 528 [1967]). Belföldi bűnügyi nyomozásokban a negyedik alkotmánykiegészítés általánosságban megköveteli a bűnüldözési tisztviselőktől a kutatás megkezdése előtt bírósági végzés beszerzését. Lásd a Katz kontra Egyesült Államok ügyet, 389 U.S. 347, 357(1967). A parancs kibocsátására vonatkozó előírások, például a valószínű okra és a lefoglalandó tárgy konkrét meghatározására vonatkozó követelmények

([1]) Ez az áttekintés nem ismerteti a terrorizmussal kapcsolatos bűnüldözés és más nemzetbiztonsági nyomozások által alkalmazott nemzetbiztonsági nyomozati eszközöket, ideértve a hiteljelentésekben szereplő egyes adatokra, pénzügyi adatokra, elektronikus előfizetői és ügyleti adatokra vonatkozó nemzetbiztonsági leveleket, lásd: 12 U.S.C.§ 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, valamint elektronikus megfigyelésre, házkutatási parancsokra, üzleti adatokra vonatkozó nemzetbiztonsági leveleket, és más adatok külföldi hírszerzői tevékenység megfigyeléséről szóló törvény szerinti gyűjtését, lásd: 50 U. S.C. § 1801 és azt követő szakaszai.

([2]) Ez a levél a szövetségi bűnüldöző és szabályozó hatóságokat tárgyalja. Az állami jog megsértése ügyében az állami bűnüldöző hatóságok nyomoznak, és e jogszabálysértések tárgyalása az állami bíróságokon történik. Az állami bűnüldözési hatóságok az állami jog alapján kiadott parancsokat és idézéseket lényegében az itt ismertetett módon használják, de azzal a lehetőséggel, hogy az állami jogi eljárásra az USA alkotmányában előírt védelmet meghaladó, az állami alkotmányban vagy törvényekben előírt kiegészítő védelem vonatkozhat. Az állami jogban előírt védelemnek legalább az USA Alkotmányában – a negyedik alkotmánykiegészítést is beleértve – nyújtott védelemmel azonos szintűnek kell lennie.

alkalmazandók a fizikai átvizsgálásra és lefoglalásra vonatkozó parancsokra, valamint az elektronikus hírközlési eszközök tárolt tartalmára vonatkozó, a tárolt hírközlési információkról szóló törvény alapján kiadott parancsokra, az alábbiak szerint. Amennyiben a végzés követelménye nem érvényesül, a kormányzati tevékenységnek a negyedik alkotmánykiegészítés szerinti „észszerűségi" tesztnek kell megfelelnie. Ezért maga az Alkotmány biztosítja, hogy az USA kormánya ne rendelkezzen korlátlan vagy önkényes hatalommal magánadatok megszerzésére ([3]).

Büntetőügyekben eljáró bűnüldöző hatóságok:

A szövetségi ügyészek, akik az Igazságügyi Minisztérium (a továbbiakban: DOJ) tisztviselői, és a szövetségi nyomozó ügynökök, beleértve a Szövetségi Nyomozó Iroda (Federal Bureau of Investigation – FBI) – a DOJ keretében működő bűnüldöző szerv – ügynökeit, többféle típusú kötelező bírósági eljáráson keresztül kérhetik az Egyesült Államokban vállalati dokumentumok és más adatok kiadását, beleértve az esküdtszék által kibocsátott idézéseket, közigazgatási idézéseket és házkutatási parancsokat, és a szövetségi bűnügyi lehallgatási és kimenő hívások adatainak rögzítésére vonatkozó hatáskörök szerint más kommunikációkhoz is hozzáférhetnek.

Bizonyításfelvételben vagy a tárgyaláson való közreműködésre kötelező vádesküdtszéki parancs: A bizonyításfelvételben való közreműködésre kötelező parancsot célzott bűnüldözési nyomozások alátámasztására használják. Az esküdtszék által kiadott parancs a vádesküdtszék általi hivatalos kötelezés (rendszerint a szövetségi ügyész kérésére) egy adott büntetőjogi jogsértés esküdtszéki vizsgálatának támogatására. A vádesküdtszékek a bíróság vizsgáló ága, és azokat bíró vagy nyomozási bíró egy listáról választja. A parancs előírhatja, hogy valaki tanúskodjon az eljárásban vagy mutasson be vagy bocsásson rendelkezésre üzleti adatokat, elektronikusan tárolt információkat vagy más ingókat. Az információknak a nyomozáshoz relevánsnak kell lennie és a parancs nem lehet észszerűtlen annak túlzó hatóköre, elnyomó vagy terhes jellege miatt. A címzett indítványt terjeszthet be a parancs ezen okok miatti vitatására. Lásd: Fed. R. Crim. P. 17 (A szövetségi büntetőeljárásjog 17. szabálya). Korlátozott körülmények között a dokumentumokra vonatkozó tárgyalási közreműködési parancsok azt követően használhatóak, hogy az esküdtszék az ügyben vádat emel.

Bizonyításfelvételben való közreműködésre kötelező hatósági határozat: A bizonyításfelvételben való közreműködésre kötelező határozat meghozatalára vonatkozó hatáskör büntető vagy polgári nyomozásban használható. Büntetőjogi bűnüldözési összefüggésben több szövetségi törvény ad felhatalmazást a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatok kiadására üzleti adatok, elektronikusan tárolt információk vagy más ingók egészségügyi csalással, gyermekbántalmazással, titkosszolgálati védelemmel, ellenőrzött anyagok használatával kapcsolatos vizsgálatok vagy kormányzati hivatalokat érintő legfőbb ügyészi vizsgálatok kapcsán történő bemutatása vagy rendelkezésre bocsátása céljából. Ha a kormány a bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatot bíróságon kívánja érvényesíteni, a közigazgatási határozat címzettje – az esküdtszéki parancs címzettjéhez hasonlóan – vitathatja a határozat észszerűségét annak túlzott hatóköre, elnyomó vagy terhes jellege miatt.

Kimenő és bejövő hívásadatok rögzítésére vonatkozó bírósági végzések: A kimenő és bejövő hívások adatainak rögzítésére vonatkozó büntetőjogi rendelkezések értelmében a bűnüldöző szervek bírósági végzést kaphatnak abból a célból, hogy megszerezzék valamely telefonszám vagy e-mail-cím valós idejű, tartalmat nem felfedő hívásindítási, átirányítási, hívásfogadási és jelzési adatait, amennyiben igazolják, hogy az így megszerzett adatok egy folyamatban levő bűnügyi nyomozásban jelentőséggel bírnak. Lásd: 18 U. S. C. §§ 3121–3127. Ilyen eszközök jogellenes használata vagy beszerelése szövetségi bűncselekmény.

Az elektronikus kommunikáció adatvédelméről szóló törvény (ECPA): További szabályok irányadóak az internetszolgáltató telefontársaságok és más harmadik személy szolgáltatók által tárolt előfizetői adatokhoz, forgalmi adatokhoz és tárolt tartalomhoz való, az ECPA II. címe szerinti kormányzati hozzáférésre, amely törvényt a tárolt hírközlési információkról szóló törvénynek is nevezik (Stored Communications Act – SCA), 18 U.S.C. §§ 2701–2712. Az SCA fekteti le a törvényes adatvédelmi jogok azon rendszerét, amely korlátozza az adatokba történő, az alkotmányjog szerint a fogyasztók és internetszolgáltatók előfizetői részéről szükséges mértéket meghaladó, bűnüldözési célú betekintést. Az SCA az adatvédelmi garanciák szintjének emeléséről rendelkezik attól függően, hogy az adatgyűjtés mennyire tolakodó jellegű. Az előfizetői regisztrációs adatok, internetprotokoll- (IP)-címek és kapcsolódó időbélyegek esetében a büntetőügyekben eljáró

([3]) Tekintettel a negyedik alkotmánykiegészítésben foglalt, fent tárgyalt, a magánélet és a biztonsági érdekek védelmére vonatkozó elvekre, az amerikai bíróságok rendszeresen alkalmazzák ezeket az elveket a technológia fejlődésével megjelenő új típusú bűnüldözési nyomozati eszközökre. 2018-ban például a Legfelsőbb Bíróság úgy határozott, hogy az a tény, hogy a kormány a bűnüldözési nyomozás során egy mobiltelefon-társaságtól hosszabb időszakra vonatkozóan megszerezte a visszamenőleges cellaalapú helyinformációkat, olyan „keresésnek" minősül, amely a negyedik alkotmánykiegészítés házkutatási parancsokra vonatkozó követelményének hatálya alá tartozik. Carpenter kontra Egyesült Államok, 138 S. Ct. 2206 (2018).

bűnüldöző hatóságoknak idézést kell beszerezniük. A legtöbb egyéb tárolt, tartalmat nem felfedő információ – így a tárgy nélküli e-mail-fejlécek – esetében a bűnüldöző hatóságoknak konkrét tényekkel kell a bíró számára igazolniuk, hogy a kért információ releváns és lényeges egy folyamatban levő bűnügyi nyomozásban. Az elektronikus kommunikáció tárolt tartalmának megszerzéséhez általában a büntető ügyekben eljáró bűnüldöző hatóságoknak az arra vonatkozó alapos gyanú alapján kell beszerezniük bírói parancsot, hogy a szóban forgó felhasználói fiók bűncselekmény bizonyítékát tartalmazza. Az SCA rendelkezik a polgári jogi helytállásról és a büntetőjogi szankciókról is ([4]).

A szövetségi lehallgatási törvény szerinti megfigyelésre vonatkozó bírósági végzések: Emellett a bűnüldöző hatóságok a szövetségi lehallgatási törvény szerint bűnügyi nyomozási célokra lehallgathatnak valós idejű telefonos, szóbeli vagy elektronikus kommunikációt. Lásd: 18 U. S. C. §§ 2510–2523. Ez a hatáskör csak bírósági végzésre elérhető, amelyben a bíró egyebek között megállapítja annak megalapozott gyanúját, hogy a telefonos vagy elektronikus lehallgatás szövetségi bűncselekményre, vagy a büntetőeljárás elől menekülő tartózkodási helyére vonatkozó bizonyítékot nyújt. A törvény polgári jogi helytállást és büntetőjogi szankciókat ír elő a lehallgatási rendelkezések megszegése esetére.

Házkutatási parancs – Fed. R. Crim. P. 41 (A szövetségi büntetőeljárásjog 41. szabálya): A bűnüldöző szervek az Egyesült Államokban átvizsgálhatnak helyiségeket, ha ezt bíró engedélyezi. A bűnüldöző szerveknek a bíró felé az alapos gyanú bizonyításával kell igazolniuk bűncselekmény elkövetését vagy a készülő bűncselekményt, és hogy a parancsban megadott helyen valószínűleg a bűncselekményhez köthető tárgyak találhatóak. Ezt a hatáskört gyakorta használják akkor, ha a helyiség rendőrség általi fizikai átvizsgálása azért szükséges, mert fennáll annak a veszélye, hogy a bizonyítékokat megsemmisítik, ha idézést vagy a bemutatást előíró egyéb végzést küldenek a vállalatnak. Az a személy, akivel szemben kutatást folytatnak, vagy akinek az ingóságait átkutatják, kérheti a jogellenes kutatásból szerzett vagy abból származó bizonyítékok felhasználásától való eltekintést, ha e bizonyítékot büntetőeljárás során próbálják felhasználni vele szemben. Lásd a Mapp kontra Ohio ügyet, 367 U.S. 643 (1961). Ha az adattulajdonos parancs alapján köteles adatokat közölni, a kötelezett fél megtámadhatja a közzétételre vonatkozó követelményt azon az alapon, hogy az indokolatlanul megterhelő. Lásd az Egyesült Államoknak a 3. körzet fellebbviteli bíróságához benyújtott kérelmét, 610 F.2d 1148, 1157 (3d Cir. 1979) (amely szerint a jogszerű eljárásnak feltétele, hogy mielőtt a távközlési vállalatot házkutatásban való segítségnyújtásra kötelezné, ennek megterhelő voltáról meghallgatást kell tartani); lásd továbbá az Egyesült Államoknak a 9. körzet fellebbviteli bíróságához benyújtott kérelmét, 616 F.2d 1122 (9th Cir. 1980), (amely a bíróság felügyeleti hatásköre alapján ugyanezen következtetésre jutott).

DOJ irányelvek és szabályzatok: Az adatokba való kormányzati betekintés ezen alkotmányos, törvényi és szabályalapú korlátai mellett a legfőbb ügyész is kibocsátott irányelveket, amelyek további korlátokat szabnak a bűnüldöző szervek adatbetekintése tekintetében, és amelyek a magánélet és az alapvető szabadságok védelmére vonatkozó védelmi eszközöket is tartalmaznak. Például a legfőbb ügyésznek az FBI belföldi nyomozási műveleteire vonatkozó irányelvei (2008. szeptember) (a továbbiakban: a legfőbb ügyész FBI-irányelvei, amely elérhető itt: http://www.justice.gov/archive/opa/docs/guidelines.pdf), korlátokat szabnak a nyomozati eszközök szövetségi bűncselekmények nyomozásához kapcsolódó információk felkutatása céljából történő használata tekintetében. Ezek az irányelvek előírják, hogy az FBI a lehető legkevésbé beavatkozó nyomozati módszereket használja, figyelembe véve a magánélet és az az alapvető szabadságjogok védelmére gyakorolt hatásokat és a hírnévcsorbulás kockázatát. Megjegyzik továbbá, hogy „evidens, hogy az FBI-nak a vizsgálatait és egyéb tevékenységeit jogszerűen és észszerűen kell végeznie, az alapvető szabadságjogokat és a magánéletet tiszteletben tartva és kerülve a jogkövető emberek életébe történő szükségtelen beavatkozást”. Lásd a legfőbb ügyész FBI-irányelveinek 5. pontját. Az FBI ezeket az irányelveket az FBI belföldi nyomozásokra és műveletekre vonatkozó útmutatójával (Domestic Investigations and Operations Guide – DIOG) hajtotta végre, amely elérhető itt: https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29; az útmutató egy olyan átfogó kézikönyv, amely részletes korlátokat szab a nyomozati eszközök használatára vonatkozóan, és útmutatást ad annak érdekében, hogy a magánélet és az alapvető szabadságjogok minden nyomozásban védelmet kapjanak. A szövetségi ügyészek nyomozati tevékenységének korlátait ismertető további szabályokat és szabályzatokat az Igazságügyi kézikönyv tartalmazza, amely elérhető az alábbi címen: https://www.justice.gov/jm/justice-manual.

Polgári és szabályozó hatóságok (közérdek):

([4]) Ezenkívül az SCA 2705. szakaszának b) pontja felhatalmazza a kormányt arra, hogy bírósági végzést szerezzen be a közzététellel szembeni védelem bizonyított igénye alapján, megtiltva a hírközlési szolgáltató számára, hogy önként értesítse felhasználóit az SCA jogi eljárására vonatkozó értesítés kézhezvételéről. 2017 októberében Rod Rosenstein főügyészhelyettes feljegyzést küldött a DOJ ügyvédeinek és ügynökeinek, amelyben iránymutatást fogalmazott meg annak biztosítása érdekében, hogy az ilyen védelmi végzések iránti kérelmek igazodjanak a nyomozás konkrét tényeihez és törekvéseihez, és általános egyéves felső határt állapított meg arra vonatkozóan, hogy a kérelem meddig késleltetheti az értesítést. 2022 májusában Lisa Monaco főügyészhelyettes kiegészítő iránymutatást adott ki a témában, amely többek között meghatározta a DOJ belső jóváhagyási követelményeit a védelmi végzésnek a kezdeti egyéves időszakon túli meghosszabbítása iránti kérelmek tekintetében, és előírta a védelmi végzéseknek a vizsgálat lezárásakor történő megszüntetését.

Jelentős korlátozások érvényesülnek az Egyesült Államokban a vállalati adatokba való polgári vagy szabályozói (azaz „közérdekű") betekintés tekintetében is. A polgári és szabályozó feladatkörrel felruházott hivatalok bizonyításfelvételben való közreműködésre kötelező határozatokat adhatnak ki vállalatoknak üzleti adatok, elektronikusan tárolt információk vagy más ingóságok tárgyában. Ezeket a hivatalokat a bizonyításfelvételben való közreműködésre kötelező közigazgatási vagy polgári határozat kiadására vonatkozó hatáskör gyakorlásában nem csak szervezeti alapszabályuk korlátozza, hanem az ilyen határozatok esetleges bírósági végrehajtás előtti független bírósági felülvizsgálata is. Lásd pl. Fed. R. Civ. P. 45 A hivatalok csak olyan adatokba kérhetnek betekintést, amelyek a szabályozási feladatkörük kapcsán jelentőséggel bírnak. A bizonyításfelvételben való közreműködésre kötelező közigazgatási határozat címzettje továbbá bíróságon vitathatja az adott határozat végrehajtását annak bizonyításával, hogy a hivatal nem a korábban tárgyalt alapvető észszerűségi normák szerint járt el.

Vannak más, az adott ágazaton és a birtokukban lévő adatok típusán alapuló jogalapok is a közigazgatási hivatalok adatkéréseinek vitatására. Például a pénzügyi intézmények vitathatják a bizonyos típusú adatokat kérő, bizonyításfelvételben való közreműködésre kötelező közigazgatási határozatokat azon az alapon, hogy azok a banktitokról szóló törvénybe és annak végrehajtási rendeleteibe ütköznek. Az Egyesült Államok Szövetségi Törvénykönyve, 31. cím, 5318. §; 31 C.F.R. X. fejezet. Más vállalkozások a tisztességes hiteljelentésekről szóló törvényre hagyatkozhatnak, lásd: 15 U.S.C. § 1681b, vagy sok más ágazati jogszabályra. A hivatal idézési hatáskörével való visszaélés a hivatal helytállási kötelezettségét vagy a hivatal tisztviselőinek személyes helytállási kötelezettségét alapozhatja meg. Lásd pl. a pénzügyi adatvédelemhez való jogról szóló törvényt, 12 U.S.C. §§ 3401–3423. Az Egyesült Államok bíróságai ennélfogva óvnak a nem helyénvaló szabályozói adatkérésektől, és ellátják a szövetségi hivatalok fellépéseinek független felügyeletét.

Végül az Egyesült Államokban a közigazgatási hatóságok vállalati adatok közigazgatási házkutatás keretében történő fizikai lefoglalására fennálló törvényi hatásköreinek meg kell felelniük a negyedik alkotmánykiegészítésen alapuló követelményeknek. Lásd a See kontra City of Seattle ügyet, 387 U. S. 541 (1967).

Következtetés:

Az Egyesült Államokban minden bűnüldözési és szabályozási tevékenységnek meg kell felelnie a vonatkozó jogszabályoknak, beleértve az USA Alkotmányát, törvényeit, szabályozásait és rendeleteit. Az ilyen tevékenységeknek meg kell felelniük a vonatkozó szabályzatoknak is, ideértve a legfőbb ügyész szövetségi bűnüldözési tevékenységekre vonatkozó irányelveit. A fenti ismertetett jogi keret korlátozza az USA bűnüldözési és szabályozó hivatalait abban, hogy az Egyesült Államokban vállalatoktól adatokat szerezzenek, tekintet nélkül arra, hogy az információ egyesült államokbeli személyekre vagy külföldi országok polgáraira vonatkozik-e, és emellett lehetővé teszi az e hatáskörök szerinti kormányzati adatkérések bírói felülvizsgálatát.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

VII. MELLÉKLET

A NEMZETI HÍRSZERZÉSI HIVATAL VEZETŐ JOGTANÁCSOSÁNAK HIVATALA

WASHINGTON, DC, 20511

2022. december 9.

Leslie B. Kiernan
vezető jogtanácsos
Egyesült Államok Kereskedelmi
Minisztériuma, 1401 Constitution Ave.,
NW Washington, DC 20230

Tisztelt Kiernan asszony!

2022. október 7-én Biden elnök aláírta az *Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről* szóló 14086. sz. elnöki rendeletet, amely megerősíti az Egyesült Államok jelfelderítési tevékenységei kapcsán a személyes adatok védelmére és a polgári szabadságjogokra vonatkozó szigorú biztosítékokat. Ezek a biztosítékok a következők: a jelfelderítési tevékenységeknek meghatározott jogszerű célokat kell szolgálniuk; az ilyen tevékenységeket kifejezetten tilos meghatározott tiltott célokból végezni; új eljárások bevezetése annak biztosítására, hogy a jelfelderítési tevékenységek előmozdítsák ezeket a jogszerű célokat, és ne segítsenek elő tiltott célokat; annak előírása, hogy a jelfelderítési tevékenységekre egyrészt csak azt követően kerülhet sor, hogy az összes releváns tényező észszerű értékelése alapján megállapítást nyert, hogy e tevékenységek szükségesek egy validált hírszerzési prioritás előmozdításához, másrészt csak olyan mértékben és módon, amely arányos azzal a validált hírszerzési prioritással, amelyre engedélyezték őket; valamint az Egyesült Államok Hírszerző Közösségébe (IC) tartozó szervezetek utasítása arra, hogy aktualizálják szabályzataikat és eljárásaikat annak érdekében, hogy azok tükrözzék az elnöki rendeletben előírt jelfelderítési biztosítékokat. A legfontosabb, hogy az elnöki rendelet egy olyan független és kötelező erejű mechanizmust is bevezet, amely lehetővé teszi az elnöki rendelet alapján kijelölt „megfelelőnek minősülő államokból" származó személyek számára, hogy jogorvoslatért folyamodjanak, ha úgy vélik, hogy az Egyesült Államok jogellenes jelfelderítési tevékenységei érintették őket, ideértve az elnöki rendeletben meghatározott biztosítékokat sértő tevékenységeket is.

A Biden elnök által kiadott 14086. sz. elnöki rendelet az Európai Bizottság (EB) és az Egyesült Államok képviselői közötti, jóval több mint egy évig tartó részletes tárgyalások csúcspontját jelentette, és irányt szab abban a tekintetben, hogy az Egyesült Államok milyen lépéseket fog tenni az EU–USA adatvédelmi keret szerinti kötelezettségvállalásainak végrehajtása érdekében. Tudomásom szerint a keret alapját képező együttműködés szellemében Ön két kérdéscsoportot kapott az Európai Bizottságtól arra vonatkozóan, hogy a Hírszerző Közösség hogyan fogja végrehajtani az elnöki rendeletet. Örömömre szolgál, hogy ezeket a kérdéseket e levélben megválaszolhatom.

A külföldi hírszerzői tevékenység megfigyeléséről szóló 1978. évi törvény 702. szakasza (FISA 702. szakasz)

Az első kérdéscsoport a FISA 702. szakaszára vonatkozik, amely lehetővé teszi a külföldi hírszerzési információk gyűjtését az elektronikus hírközlési szolgáltatók kényszerű segítségével olyan nem egyesült államokbeli személyek megcélzása révén, akikről észszerűen feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak. A kérdések konkrétan e rendelkezés és a 14086. sz. elnöki rendelet közötti kölcsönhatásra, valamint a FISA 702. szakasza alapján folytatott tevékenységekre vonatkozó egyéb biztosítékokra vonatkoznak.

Először is megerősíthetjük, hogy a Hírszerző Közösség alkalmazni fogja a 14086. sz. elnöki rendeletben meghatározott biztosítékokat a FISA 702. szakasza alapján végzett tevékenységekre.

Emellett számos egyéb biztosíték vonatkozik a FISA 702. szakaszának a kormány általi alkalmazására. Például a FISA 702. szakasza szerinti valamennyi tanúsítványt mind a főügyésznek, mind a Nemzeti Hírszerzési Hivatal igazgatójának (DNI) alá kell írnia, és a kormánynak minden ilyen tanúsítványt jóváhagyásra be kell nyújtania a Külföldi Hírszerzést Felügyelő Bírósághoz (a továbbiakban: FISC), amely független, élethosszig tartó időtartamra kinevezett bírákból áll, akik a FISC-ben nem megújítható hétéves hivatali időt töltenek be. A tanúsítványok meghatározzák a gyűjtendő külföldi hírszerzési információk kategóriáit, amelyeknek meg kell felelniük a külföldi hírszerzési információ jogszabályban foglalt fogalommeghatározásának, és amelyeket olyan nem egyesült államokbeli személyek célba vétele révén gyűjtenek, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak. A tanúsítványok a nemzetközi terrorizmussal és más témákkal, például a tömegpusztító fegyverekkel kapcsolatos információkra terjednek ki. Minden éves tanúsítványt be kell nyújtani a FISC-hez jóváhagyásra egy tanúsítási kérelemcsomagban, amely magában foglalja a legfőbb ügyész és a Nemzeti Hírszerzési Hivatal igazgatója tanúsítványait, a hírszerző ügynökségek egyes vezetőinek eskü alatt tett nyilatkozatait, valamint a célzási eljárásokat, a minimalizálási eljárásokat és a kormányra nézve kötelező lekérdezési eljárásokat. A célzási eljárások többek között megkövetelik, hogy a Hírszerző Közösség a körülmények összessége alapján észszerűen értékelje, hogy a célzás valószínűleg a PISA 702. szakasza szerinti tanúsítványban azonosított külföldi hírszerzési információk gyűjtéséhez vezet.

Ezenkívül a FISA 702. szakasza szerinti információgyűjtés során a Hírszerző Közösségnek: a célba vétel időpontjában írásbeli magyarázatot kell adnia arra vonatkozóan, hogy a célpont várhatóan rendelkezik a PISA 702. szakasza szerinti tanúsítványban azonosított külföldi hírszerzési információkkal, vagy várhatóan kapni fog vagy közölni fog ilyen információkat; meg kell erősítenie, hogy a PISA 702. szakaszában meghatározott célzási előírás továbbra is teljesül; és meg kell szüntetnie az információgyűjtést, ha ezen előírás már nem teljesül. *Lásd* az Egyesült Államok kormányának beadványát a Külföldi Hírszerzést Felügyelő Bírósághoz, *2015 Summary of Notable Section 702 Requirements* [A 702. szakasszal kapcsolatos fontosabb követelmények összefoglalója, 2015], 2–3. pont (2015. július 15.).

Annak előírása, hogy a Hírszerző Közösség írásban rögzítse és rendszeresen erősítse meg azon értékelését, miszerint a FISA 702. szakasza szerinti célok megfelelnek az alkalmazandó célzási normáknak, megkönnyíti a Hírszerző Közösség célzási tevékenységeinek FISC általi felügyeletét. Minden rögzített célzási értékelést és indoklást kéthavonta felülvizsgálnak az Igazságügyi Minisztérium (DOJ) hírszerzési felügyeleti jogászai, akik ezt a felügyeleti funkciót a külföldi hírszerzési műveletektől függetlenül látják el. Ezt követően az e feladatot ellátó DOJ-részleg a FISC régóta fennálló szabálya alapján felelős azért, hogy jelentést tegyen a FISC-nek az alkalmazandó eljárások bármilyen megsértéséről. Ez a jelentéstétel, valamint a FISC és e DOJ-részleg közötti, a FISA 702. szakasza szerinti célzás felügyeletével kapcsolatos rendszeres találkozók lehetővé teszik a FISC számára, hogy kikényszerítse a FISA 702. szakasza szerinti célzásnak és más eljárásoknak való megfelelést, és egyéb módon biztosítsa a kormány tevékenységeinek jogszerűségét. A FISC ezt több módon is megteheti, többek között olyan kötelező erejű korrekciós határozatok kibocsátásával, amelyek megszüntetik a kormány arra vonatkozó hatáskörét, hogy egy adott cél tekintetében adatokat gyűjtsön, vagy módosítják vagy késleltetik a FISA 702. szakasza szerinti adatgyűjtést. A FISC azt is megkövetelheti a kormánytól, hogy nyújtson be további jelentést vagy adjon további tájékoztatást a célzási és egyéb eljárásoknak való megfeleléséről, vagy megkövetelheti ezen eljárások módosítását.

Jelfelderítési adatok tömeges gyűjtése

A második kérdéscsoport a jelfelderítési adatok tömeges gyűjtésére vonatkozik, amelyet a 14086. sz. elnöki rendelet a következőképpen határoz meg: „olyan nagy mennyiségű jelfelderítési adat engedélyezett gyűjtése, amelyet műszaki vagy működtetési megfontolásokból megkülönböztető elemek (például egyedi azonosítók vagy kiválasztási kritériumok) használata nélkül szereznek meg.”

E kérdések kapcsán először is megjegyezzük, hogy sem a FISA, sem nemzetbiztonsági levelek nem engedélyezik a nagy mennyiségű gyűjtést. A FISA tekintetében:

– A FISA elektronikus megfigyelést engedélyező I. és fizikai kutatást engedélyező III. címe is előírja a bírósági végzést (korlátozott kivételekkel, mint pl. rendkívüli körülmények), és minden esetben követelmény annak alapos gyanúja, hogy a célpont egy külföldi hatalom vagy külföldi hatalom megbízottja. *Lásd:* 50 U. S. C. §§ 1805, 1824.

– A 2015. évi USA FREEDOM törvény módosította a FISA IV. címét – amely bírósági végzés alapján engedélyezi a kimenő és bejövő hívások adatait rögzítő eszközök használatát (kivéve vészhelyzet esetén) –, és előírja a kormány számára, hogy kérelmeit „meghatározott kiválasztási kritériumra” alapozza. *Lásd:* 50 U. S. C. § 1842(c)3.

– A FISA V. címe lehetővé teszi a Szövetségi Nyomozóiroda (FBI) számára, hogy megszerezzen bizonyos típusú üzleti nyilvántartásokat, ehhez azonban bírósági végzést ír elő, amelynek olyan kérelmen kell alapulnia, amelyben szerepel, hogy „konkrét és megmagyarázható tények alapján feltételezhető, hogy az a személy, akire a nyilvántartás vonatkozik, külföldi hatalom vagy külföldi hatalom ügynöke". *Lásd:* 50 U.S.C. § 1862(b)(2)(B) ([1]).

– Végezetül a FISA 702. szakasza külföldi hírszerzési információk szerzése céljából lehetővé teszi olyan személyek célba vételét, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak. *Lásd:* 50 U.S.C. § 188la(a). Tehát, amint azt az adatvédelmi és polgári szabadságjogi felügyelő tanács megállapította, a kormány által a FISA 702. szakasza alapján végzett adatgyűjtés „szinte teljes egészében olyan magánszemélyek megcélzásából és e személyek hírközlési adatainak megszerzéséből áll, akik kapcsán a kormány észszerűen feltételezi, hogy bizonyos típusú külföldi hírszerzési adatot szerez tőlük", ezért „a program nem úgy működik, hogy tömegesen szereznek meg hírközlési adatokat". Adatvédelmi és polgári szabadságjogi felügyelő tanács, „Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" [Jelentés a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakasza szerint működtetett megfigyelési programról] 103. pont (2014. július 2.) ([2]).

Ami a nemzetbiztonsági leveleket illeti, a 2015. évi USA FREEDOM törvény „meghatározott kiválasztási kritérium" alkalmazásának követelményét írja elő az ilyen levelek használatára vonatkozóan. *Lásd:* 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

A 14086. sz. elnöki rendelet továbbá úgy rendelkezik, hogy „[a] célzott adatgyűjtést előnyben kell részesíteni", és amennyiben a Hírszerző Közösség tömeges adatgyűjtést végez, „a jelfelderítési adatok tömeges gyűjtése csak annak megállapítása alapján engedélyezhető, hogy a validált hírszerzési prioritás előmozdításához szükséges információ célzott gyűjtéssel észszerűen nem érhető el". *Lásd*: 14086. sz. elnöki rendelet, § 2(c)(ii)(A).

Továbbá, ha a Hírszerző Közösség megállapítja, hogy a tömeges gyűjtés megfelel ezeknek az előírásoknak, a 14086. sz. elnöki rendelet további biztosítékokat nyújt. Az elnöki rendelet konkrétan előírja, hogy a Hírszerző Közösségnek a tömeges adatgyűjtés során „észszerű módszereket és technikai intézkedéseket kell alkalmaznia annak érdekében, hogy az összegyűjtött adatokat a validált hírszerzési prioritás előmozdításához szükséges mértékre korlátozza, ugyanakkor minimalizálja a nem releváns információk gyűjtését". *Lásd ugyanott*. A rendelet azt is kimondja, hogy „a jelfelderítési tevékenységek", amelyek magukban foglalják a tömeges gyűjtéssel nyert jelfelderítési adatok lekérdezését, „csak azt követően végezhetők, hogy az összes releváns tényező észszerű értékelése alapján megállapítást nyer, hogy a tevékenységek szükségesek egy validált hírszerzési prioritás előmozdításához". *Lásd uo*. § 2(a)(ii)(A). A rendelet ezt az elvet továbbá annak kimondásával valósítja meg, hogy a Hírszerző Közösség csak hat megengedhető cél elérése érdekében kérdezhet le tömegesen szerzett, nem minimalizált jelfelderítési adatokat, és az ilyen lekérdezéseket olyan szabályzatoknak és eljárásoknak megfelelően kell lefolytatni, amelyek „megfelelően figyelembe veszik [a lekérdezések] valamennyi érintett személy magánéletére és polgári szabadságjogaira gyakorolt hatását, állampolgárságuktól vagy tartózkodási helyüktől függetlenül". *Lásd uo*. § 2(c)(iii.)(D). Végül a rendelet rendelkezik az összegyűjtött adatok kezeléséről, biztonságáról és a hozzáférés ellenőrzéséről. *Lásd uo*. § 2(c)(iii)(A) és § 2(c)(iii)(B).

*****

Reméljük, hogy ezek a pontosítások segítséget jelentenek. Kérjük, forduljon hozzánk bizalommal, ha további kérdései vannak azzal kapcsolatban, hogy az Egyesült Államok Hírszerző Közössége hogyan tervezi a 14086. sz. elnöki rendelet végrehajtását.

([1]) 2001 és 2020 között a FISA V. címe lehetővé tette az FBI számára, hogy engedélyt kérjen a FISC-től olyan „ingók" megszerzésére, amelyek bizonyos engedélyezett vizsgálatok szempontjából relevánsak. *Lásd*: USA PATRIOT törvény, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Ez a rendelkezés – amely már lejárt, tehát már nem törvényi előírás – olyan felhatalmazást adott, amely alapján a kormány egyszerre gyűjthetett telefonos metaadatokat tömegesen. Ezt a rendelkezést azonban már lejárta előtt módosította az USA FREEDOM törvény, előírva, hogy a kormánynak a FISC-hez benyújtott kérelmet „meghatározott kiválasztási kritériumra" kell alapoznia. *Lásd*: USA FREEDOM törvény, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015).

([2]) A 703. és a 704. szakasz, amelyek felhatalmazzák a Hírszerző Közösséget arra, hogy külföldön tartózkodó amerikai személyeket célozzon meg, bírósági végzést írnak elő (a szükséghelyzetek kivételével), és minden esetben megkövetelik, hogy valószínűsíthető legyen, hogy a célpont külföldi hatalom, külföldi hatalom ügynöke, vagy külföldi hatalom tisztviselője vagy alkalmazottja. *Lásd: 50U. S.C.*§§ 1881b, 1881c.

Christopher C. FONZONE
vezető jogtanácsos

VIII. MELLÉKLET

Rövidítések jegyzéke

Ebben a határozatban a következő rövidítések szerepelnek:

AAA	American Arbitration Association (Amerikai Választottbírósági Szövetség)
főügyészi rendelet	az Egyesült Államok főügyésze által kiadott, az adatvédelmi felülvizsgálati bíróságról szóló rendelet
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations (a belföldi FBI-műveletekre vonatkozó főügyészi iránymutatás)
APA	Administrative Procedure Act (az államigazgatási eljárásról szóló törvény)
CIA	Central Intelligence Agency (Központi Hírszerző Ügynökség)
CNSS	Committee on National Security Systems (nemzetbiztonsági rendszerekkel foglalkozó bizottság)
Bíróság	az Európai Unió Bírósága
határozat	az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerinti, a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő szintű védelméről szóló bizottsági végrehajtási határozat
DHS	Department of Homeland Security (Belbiztonsági Minisztérium)
DNI	Director of National Intelligence (nemzeti hírszerzési igazgató)
DoC	U.S. Department of Commerce (az USA Kereskedelmi Minisztériuma)
DoJ	U.S. Department of Justice (az USA Igazságügyi Minisztériuma)
DoT	U.S. Department of Transportation (az USA Közlekedési Minisztériuma)
DPA	adatvédelmi hatóság
DPF lista	az adatvédelmi keretben részt vevő szervezetek listája
DPRC	adatvédelmi felülvizsgálati bíróság
ECOA	Equal Credit Opportunity Act (az egyenlő hitellehetőségről szóló törvény)
ECPA	az elektronikus kommunikáció adatvédelméről szóló törvény
EGT	Európai Gazdasági Térség
12333. elnöki rendelet	az Egyesült Államok hírszerzési tevékenységeiről szóló, 12333. elnöki rendelet
14086. elnöki rendelet, az elnöki rendelet	az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről szóló, 14086. elnöki rendelet
EU–USA adatvédelmi keret vagy adatvédelmi keret	az EU–USA adatvédelmi keret
az EU–USA DPF testület	az EU–USA adatvédelmi kerettel foglalkozó testület
FBI	Federal Bureau of Investigation (Szövetségi Nyomozóiroda)
FCRA	Fair Credit Reporting Act (a méltányos hitelminősítésről szóló törvény)
FISA	Foreign Intelligence Surveillance Act (a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény)
FISC	Foreign Intelligence Surveillance Court (a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság)
FISCR	Foreign Intelligence Surveillance Court of Review (a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróság)
FOIA	Freedom of Information Act (az információhoz való szabad hozzáférésről szóló törvény)
FRA	Federal Records Act (a szövetségi nyilvántartásról szóló törvény)

FTC	az Egyesült Államok Szövetségi Kereskedelmi Bizottsága
HIPAA	az egészségbiztosítás hordozhatóságáról és elszámolási kötelezettségéről szóló törvény
ICDR	International Centre for Dispute Resolution (Nemzetközi Vitarendezési Központ)
IOB	Intelligence Oversight Board (Hírszerzési Felügyeleti Testület)
NIST	National Institute of Standards and Technology (Amerikai Nemzeti Szabványügyi és Technológiai Hivatal)
NSA	Nemzetbiztonsági Ügynökség
NSL	National Security Letter(s) (nemzetbiztonsági levél/levelek)
ODNI	Office of the Director of National Intelligence (a nemzeti hírszerzés igazgatójának hivatala)
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence (a nemzeti hírszerzési igazgató polgári szabadságjogok védelmével foglalkozó tisztviselője)
OMB	Office of Management and Budget (Igazgatási és Költségvetési Hivatal)
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (az Igazságügyi Minisztérium adatvédelmi és polgári szabadságjogi hivatala)
PCLOB	Privacy and Civil Liberties Oversight Board (Polgári Szabadságjogi Felügyelő Tanács)
PIAB	President's Intelligence Advisory Board (elnöki hírszerzési tanácsadó testület)
PPD 28	28. elnöki politikai irányelv
(EU) 2016/679 rendelet	Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.
SAOP	a magánélet védelmével foglalkozó magas beosztású ügynökségi tisztviselő
az elvek	az EU–USA adatvédelmi keret elvei
USA	Egyesült Államok
Unió	Európai Unió