II

(Nem jogalkotási aktusok)

HATÁROZATOK

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

(az értesítés a C(2016) 4176. számú dokumentummal történt)

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvre ([1]) és különösen annak 25. cikke (6) bekezdésére,

Az európai adatvédelmi biztossal folytatott konzultációt követően ([2]),

1. BEVEZETÉS

(1) A 95/46/EK irányelv meghatározza a tagállamokból harmadik országokba történő személyesadat-továbbításra vonatkozó szabályokat, amennyiben az ilyen adattovábbítás a hatálya alá tartozik.

(2) A 95/46/EK irányelv 1. cikke, valamint (2) és (10) preambulumbekezdése nem csupán a természetes személyek alapvető jogainak és szabadságainak – különösen a személyes adatok kezelése tekintetében a magánélet tiszteletben tartásához fűződő alapvető jognak – a hatékony és teljes védelmét kívánja biztosítani a személyes adatok kezelése tekintetében, hanem ezen alapvető jogok és szabadságok magas szintű védelmét is ([3]).

(3) A Bíróság ítélkezési gyakorlata ([4]) hangsúlyozta az Európai Unió Alapjogi Chartájának 7. cikkében garantált, a magánélet tiszteletben tartásához való alapvető jog, és a Charta 8. cikkében garantált, a személyes adatok védelméhez való alapvető jog fontosságát is.

(4) A 95/46/EK irányelv 25. cikkének (1) bekezdése alapján a tagállamoknak rendelkezniük kell arról, hogy személyes adatok harmadik országba történő továbbítása csak akkor történhessen meg, ha a szóban forgó harmadik ország megfelelő szintű védelmet biztosít, és ha az irányelv más rendelkezéseit végrehajtó tagállami jogszabályokat az adattovábbítást megelőzően figyelembe vették. A Bizottság megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít a belföldi jog, vagy az egyének jogainak védelme érdekében vállalt nemzetközi kötelezettségek alapján. Ebben az esetben – az irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül – személyes adatok továbbíthatók a tagállamokból, anélkül hogy további garanciákra lenne szükség.

([1]) HL L 281., 1995.11.23., 31. o.
([2]) Lásd: 4/2016. sz. vélemény az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről, közzététel: 2016. május 30.
([3]) A C-362/14. sz., *Maximillian Schrems kontra adatvédelmi biztos* („*Schrems-ügy*") ügyben hozott ítélet (EU:C:2015:650) 39. pontja.
([4]) A C-553/07. sz., *Rijkeboer*-ügyben hozott ítélet (EU:C:2009:293) 47. pontja; a C-293/12. és C-594/12. sz., *Digital Rights Ireland és társai* egyesített ügyekben hozott ítélet (EU:C:2014:238) 53. pontja; a C-131/12. sz., *Google Spain and Google* ügyben hozott ítélet (EU:C:2014:317) 53., 66. és 74. pontja.

(5) A 95/46/EK irányelv 25. cikkének (2) bekezdése értelmében a harmadik ország által nyújtott védelem szintjét az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni, beleértve adott harmadik országban hatályos, általános és ágazati jogrendet.

(6) A 2000/520/EK irányelv ([5]) – a 95/46/EK irányelv 25. cikke (2) bekezdésének alkalmazásában – megfelelőnek tekintette az Unióból az Egyesült Államokban letelepedett szervezethez továbbított személyes adatok védelmének szintjét az Egyesült Államok Kereskedelmi Minisztériuma által kiadott, úgynevezett „gyakran felvetődő kérdésekben" nyújtott iránymutatásnak megfelelően végrehajtott, „védett adatkikötőre vonatkozó elvek" alapján.

(7) A Bizottság 2013. november 27-i COM(2013) 846 végleges ([6]) és COM(2013) 847 végleges ([7]) közleményeiben úgy ítélte meg, hogy felül kell vizsgálni és meg kell erősíteni a védett adatkikötő rendszerének alapját számos tényező tekintetében, ilyen például az adatáramlások exponenciális növekedése és kiemelkedő fontossága az Atlanti-óceán mindkét partján működő gazdaság számára, a védett adatkikötő rendszeréhez csatlakozó amerikai vállalatok számának gyors növekedése, továbbá az egyes amerikai hírszerzési programok nagyságrendjével és hatókörével kapcsolatban napvilágra került olyan új információk, amelyek kérdésessé teszik, hogy a rendszer milyen szintű védelmet képes garantálni. A Bizottság emellett több hiányosságot azonosított a védett adatkikötő rendszerében.

(8) A Bizottság 13 ajánlást fogalmazott meg a védett adatkikötő rendszerének felülvizsgálatáról az által összegyűjtött bizonyítékok, többek között EU-USA adatvédelmi kapcsolattartó csoport ([8]) munkájából származó információk, valamint az EU-USA eseti munkacsoportban ([9]) kapott, az amerikai hírszerzési programokkal kapcsolatos tájékoztatás alapján. Ezek az ajánlások az alábbiakra fókuszáltak: az érdemi adatvédelmi elvek megerősítése, az átláthatóság fokozása az egyesült államokbeli öntanúsított vállalkozások adatvédelmi szabályzatára vonatkozóan, a szóban forgó elveknek való megfelelés tekintetében az amerikai hatóságok által ellátott felügyelet, ellenőrzés és jogérvényesítés javítása, megfizethető vitarendezési mechanizmusok rendelkezésre állása, valamint annak szükségessége, hogy az 2000/520/EK határozatban előírt nemzetbiztonsági kivétel alkalmazását a feltétlenül szükséges és arányos mértékűre korlátozzák.

(9) Az Európai Unió Bírósága a C-362/14. sz., *Maximillian Schrems kontra adatvédelmi biztos* ([10]) ügyben hozott 2015. október 6-i ítéletében érvénytelenné nyilvánította az 2000/520/EK határozatot. A Bíróság – a védett adatkikötőre vonatkozó elvek tartalmi vizsgálata nélkül – úgy ítélte meg, hogy a Bizottság nem állapította meg ebben a határozatban, hogy az Egyesült Államok belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján ténylegesen megfelelő védelmi szintet „biztosít" ([11]).

(10) A Bíróság e tekintetben kifejtette, hogy a 95/46/EK irányelv 25. cikkének (6) bekezdésében szereplő „megfelelő védelmi szint" kifejezés nem jelent az uniós jogrendben biztosítottal megegyező védelmi szintet, úgy kell érteni, mint amely megköveteli, hogy e harmadik ország az Unióban a Chartával összefüggésben értelmezett 95/46 irányelv által biztosított védelmi szinttel „lényegében azonos" védelmi szintet biztosítson az alapvető jogok és szabadságok számára. Jóllehet azok az eszközök, amelyeket a harmadik ország az e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket az Unióban alkalmaznak, ezen eszközöknek a gyakorlatban mégis hatékonynak kell lenniük ([12]).

(11) A Bíróság bírálta, hogy a 2000/520/EK határozat nem tartalmaz elegendő megállapítást azzal kapcsolatban, hogy az Egyesült Államokban léteznek azon személyek alapvető jogaiba való esetleges beavatkozások korlátozására irányuló állami szabályok, akiknek az adatait az Unióból az Egyesült Államokba továbbítják, e beavatkozásokat az állami szervek megengedik, amennyiben azok jogszerű célokat követnek, mint például a nemzetbiztonság, valamint hogy hatékony bírói védelem létezik az ilyen jellegű beavatkozásokkal szemben ([13]).

([5]) A Bizottság 2000. július 26-i 2000/520/EK határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről (HL L 215., 2000.8.28., 7. o.).

([6]) A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – A bizalom helyreállítása az EU-USA adatáramlások tekintetében, COM(2013) 846 final, 2013. november 27.

([7]) A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – A védett adatkikötő működése az uniós polgárok és az EU-ban letelepedett vállalatok szempontjából, COM(2013) 847 final, 2013. november 27.

([8]) Lásd pl. Az Európai Unió Tanácsa, Az információcserével, valamint a magánélet és a személyes adatok védelmével foglalkozó EU–USA magas szintű kapcsolattartó csoport végső jelentése, 9831/08. sz. közlemény, 2008. május 28., az alábbi internetcímen érhető el: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Az EU-USA eseti munkacsoport uniós társelnökeinek adatvédelmi megállapításairól szóló, 2013. november 27-i jelentés, az alábbi internetcímen érhető el: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Lásd a 3. lábjegyzetet.

([11]) *Schrems-ügy*, 97. pont.

([12]) *Schrems-ügy*, 73–74. pont.

([13]) *Schrems-ügy*, 88–89. pont.

(12) A Bizottság 2014-ben megbeszéléseket kezdett az amerikai hatóságokkal, hogy a COM(2013) 847 final közleményben foglalt 13 ajánlásnak megfelelően megvitassák a védett adatkikötő rendszerének megerősítését. Az Európai Unió Bíróságának *Schrems*-ügyben hozott ítéletét követően fokozták a szóban forgó megbeszélések intenzitását annak érdekében, hogy a 95/46/EK irányelv – a Bíróság értelmezése szerinti – 25. cikkében foglalt követelményeket teljesítő, esetleges új megfelelőségi határozat szülessen. E megbeszélések eredményekként keletkeztek az e határozathoz melléklet dokumentumok, amelyeket az USA Szövetségi Közlönyében is közzé fognak tenni. Az adatvédelmi elvek (II. melléklet) az I., III–VII. mellékletben szereplő dokumentumokba foglalt, különféle amerikai hatóságok hivatalos nyilatkozataival és kötelezettségvállalásaival együtt alkotják az „EU–USA adatvédelmi pajzsot".

(13) A Bizottság gondosan elemezte az Egyesült Államok jogát és gyakorlatát, többek között a hivatalos nyilatkozatokat és kötelezettségvállalásokat. A (136)–(140) preambulumbekezdésben kifejtett megállapítások alapján a Bizottság arra a következtetésre jutott, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az EU–USA adatvédelmi pajzs alapján az Unióból az egyesült államokbeli öntanúsított szervezetekhez továbbított személyes adatok védelme tekintetében.

2. AZ „EU–USA ADATVÉDELMI PAJZS"

(14) Az EU–USA adatvédelmi pajzs olyan öntanúsítási rendszeren nyugszik, amelynek keretében az egyesült államokbeli szervezetek kötelezettséget vállalnak egy sor adatvédelmi elv – az EU–USA adatvédelmi pajzs keretelvei, köztük a kiegészítő elvek (a továbbiakban együttesen: „az elvek") – betartására. Ezeket az elveket az Egyesült Államok Kereskedelmi Minisztériuma bocsátotta ki, és megtalálhatók e határozat II. mellékletében. A pajzs egyaránt vonatkozik az adatkezelőkre és az adatfeldolgozókra (megbízottakra), azzal a sajátossággal, hogy az adatfeldolgozók szerződéses kötelezettsége, hogy kizárólag az uniós adatkezelő utasításai alapján járhatnak el, és segítséget kell nyújtaniuk az utóbbinak ahhoz, hogy választ adjon az elvek alapján a jogaikat gyakorló egyéneknek ([14]).

(15) A 95/46/EK irányelv alapján elfogadott nemzeti rendelkezések sérelme nélkül e határozat azzal a joghatással jár, hogy engedélyezett az Unión belüli adatkezelő vagy adatfeldolgozó által azon egyesült államokbeli szervezetekhez történő adattovábbítás, amelyek saját maguk tanúsították az elvek elfogadását az Egyesült Államok Kereskedelmi Minisztériuma számára, és kötelezettséget vállaltak azok betartására. Az elvek kizárólag abban az esetben vonatkoznak az amerikai szervezetek általi személyesadat-kezelésre, amennyiben az e szervezetek általi személyesadat-kezelés nem tartozik az uniós jogszabályok hatálya alá ([15]). Az adatvédelmi pajzs nem érinti a személyes adatok tagállamokon belüli kezelését szabályozó uniós jogszabályokat ([16]).

([14]) Lásd a II. melléklet III. szakasza 10. pontjának a. alpontját. Az I. szakasz 8. pontjának c. alpontjába foglalt fogalommeghatározásnak megfelelően az uniós adatkezelő meghatározza a személyes adatok kezelésének célját és eszközeit. Ezenfelül a megbízottal kötött szerződésnek egyértelművé kell tennie, hogy a harmadik fél részére történő adattovábbítás engedélyezett-e (lásd a III. szakasz 10. pontja a. pontja ii. alpontjának 2. pontját).

([15]) Ez az Unióból továbbított – munkaviszonnyal kapcsolatos – humánerőforrás-adatokra is vonatkozik. Jóllehet az elvek hangsúlyozzák az uniós munkáltató „elsődleges felelősségét" (lásd a II. melléklet III. szakasza 9. pontja d. alpontjának i. pontját), ugyanakkor világossá teszik, hogy annak magatartása az Unióban és/vagy az érintett tagállamban alkalmazandó szabályok, nem pedig az elvek hatálya alá tartozik. Lásd a II. melléklet III. szakasza 9. pontja a. alpontjának i. pontját, b. alpontjának ii. pontját, c. alpontjának i. pontját és d. alpontjának i. pontját.

([16]) Ez arra az adatkezelésre is vonatkozik, amelyre az Unión belül található olyan berendezés segítségével kerül sor, amelyet azonban az Unió területén kívül letelepedett szervezet használ (lásd a 95/46/EK irányelv 4. cikke (1) bekezdésének c) pontját). 2018. május 25-től az általános adatvédelmi rendeletet kell alkalmazni a személyes adatoknak i. az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére (még ha az adatkezelés az Egyesült Államok területén történik is), vagy ii. Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek: a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unión belül tanúsított viselkedésükről van szó. Lásd a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló, 2016. április 27-i (EU) 2016/679 rendelet (HL L 119., 2016.5.4., 1. o.) 3. cikkének (1) és (2) bekezdését.

(16) Az adatvédelmi pajzs révén a személyes adatok tekintetében biztosított védelem bármely uniós érintettre vonatkozik ([17]), akinek a személyes adatait az Unióból olyan egyesült államokbeli szervezetekhez továbbították, amelyek saját maguk tanúsították az elvek elfogadását az Egyesült Államok Kereskedelmi Minisztériuma számára.

(17) Az elvek a tanúsítást követően azonnal alkalmazandók. Egy kivétel a harmadik fél részére történő adattovábbításért való elszámoltathatóság elvével kapcsolatos, amikor az adatvédelmi pajzs tekintetében önmagát tanúsító szervezetnek már korábban meglévő üzleti kapcsolatai vannak harmadik felekkel. Mivel valamennyi időt vehet igénybe, amíg ezeket az üzleti kapcsolatokat összhangba hozzák a harmadik fél részére történő adattovábbításért való elszámoltathatóság elve alapján alkalmazandó szabályokkal, a szervezetek kötelesek ezt a lehető leghamarabb, és mindenképpen az öntanúsítástól számított legkésőbb kilenc hónapon belül megtenni (feltéve, hogy erre az adatvédelmi pajzs hatálya lépésének napját követő első két hónapban kerül sor). Az átmeneti időszak folyamán a szervezetnek a tájékoztatás és a választási lehetőség elvét kell alkalmaznia (így lehetővé téve az uniós érintett kívülmaradását), és amennyiben megbízottként eljáró harmadik személy számára továbbít személyes adatokat, gondoskodnia kell arról, hogy ez utóbbi legalább az elvekben előírtakkal azonos szintű védelmet biztosítson ([18]). Ez az átmeneti időszak ésszerű, megfelelő egyensúlyt biztosít az adatvédelemhez való alapvető jog tiszteletben tartása, valamint a vállalkozások azon jogos igénye között, hogy elegendő idővel rendelkezzenek az új kerethez való alkalmazkodásra, amennyiben az alkalmazkodás a harmadik felekhez fűződő üzleti kapcsolataikon is múlik.

(18) A rendszert a Kereskedelmi Minisztérium igazgatja és ellenőrzi, az Egyesült Államok kereskedelmi miniszterének nyilatkozataiban meghatározott kötelezettségvállalások (e határozat I. melléklete) alapján. Az Egyesült Államok Szövetségi Kereskedelmi Bizottsága (Federal Trade Commission, a továbbiakban: FTC) és Közlekedési Minisztériuma nyilatkozatokat tett az elvek érvényesítéséről, amelyek megtalálhatók a jelen határozat IV. és V. mellékletében.

2.1. *Adatvédelmi elvek*

(19) Az EU–USA adatvédelmi pajzs szerinti öntanúsítás keretében a szervezeteknek vállalniuk kell az elvek betartását ([19]).

(20) A *tájékoztatás elve* alapján a szervezetek kötelesek tájékoztatni az érintetteket a személyes adataik kezelésével kapcsolatos több lényeges elemről (pl. a gyűjtött adatok típusa, az adatkezelés célja, a hozzáférési és választási jog, a harmadik fél részére történő adattovábbítások feltételei és a felelősség kérdése). További biztosítékok alkalmazandók, különösen az a kötelezettség, hogy a szervezetek nyilvánosságra hozzák (az elveket tükröző) adatvédelmi szabályzatukat, és a Kereskedelmi Minisztérium weboldalára (amely részletesebben ismerteti az öntanúsítást, az érintettek jogait és a rendelkezésre álló jogorvoslati mechanizmusokat), az adatvédelmi pajzsban részt vevő szervezetek ((30) preambulumbekezdésben említett) listájára és egy megfelelő alternatív vitarendezési szolgáltatóra mutató linket kell feltüntetniük.

(21) Az *adatok sértetlensége és a célhoz kötöttség elve* alapján a személyes adatok körét a kezelés célja szempontjából releváns mértékűre kell korlátozni, az említett adatoknak a tervezett felhasználás szempontjából megbízhatónak, pontosnak, teljesnek és időszerűnek kell lenniük. A szervezet nem kezelhet személyes adatokat a gyűjtés eredeti céljaival vagy az egyén által a későbbiekben engedélyezett célokkal összeegyeztethetetlen módon. A szervezeteknek gondoskodniuk kell arról, hogy a személyes adatok a tervezett felhasználás szempontjából megbízhatóak, pontosak, teljesek és időszerűek legyenek.

([17]) E határozat EGT-vonatkozású. Az Európai Gazdasági Térségről szóló megállapodás (EGT-megállapodás) az Európai Unió belső piacát kierjeszti a három EGT-államra: Izlandra, Liechtensteinre és Norvégiára. Az uniós adatvédelmi jogszabályok, így a 95/46/EK irányelv az EGT-megállapodás hatálya alá tartoznak, és az említett jogszabályokat beépítették annak XI. mellékletébe. Az EGT Vegyes Bizottságnak kell döntenie arról, hogy e határozatot beépítik az EGT-megállapodásba. Amint e határozat Izlandra, Liechtensteinre és Norvégiára is alkalmazandóvá válik, az EU–USA adatvédelmi pajzs ezekre az országokra is ki fog terjedni, és az adatvédelmi pajzsra vonatkozó csomagban foglalt, az EU-ra és annak tagállamaira vonatkozó hivatkozásokat úgy kell értelmezni, hogy azok Izlandot, Liechtensteint és Norvégiát is magukba foglalják.

([18]) Lásd a II. melléklet III. szakasza 6. pontjának e. alpontját.

([19]) További biztosítékokat nyújtanak az adatvédelmi elvek og„humánerőforrás-adatokra" vonatkozó kiegészítő elvében megállapított különös szabályok, amelyek a munkaviszonnyal kapcsolatosan gyűjtött humánerőforrás-adatokra vonatkoznak (lásd a II. melléklet III. szakaszának 9. pontját). Például a munkáltatóknak a személyes adatokhoz való hozzáférés korlátozása, bizonyos adatok anonimizálása, illetve kódok vagy álnevek hozzárendelése révén igazodniuk kell az alkalmazottak adatvédelmi preferenciáihoz. A szervezetek az ilyen adatok tekintetében mindenekelőtt kötelesek együttműködni az Unió adatvédelmi hatóságaival, és követni azok ajánlásait.

(22) Ha egy új (megváltozott) cél lényegesen eltérő, azonban mégis összeegyeztethető az eredeti céllal, a *választási lehetőség elve* kifogásolási jogot (kívülmaradás) biztosít az érintetteknek. A *választási lehetőség elve* nem helyezheti hatályon kívül az összeegyeztethetetlen adatkezelés kifejezett tilalmát ([20]). A különös szabályok általában véve „bármikor" lehetővé teszik a kívülmaradást a személyes adatok közvetlen üzletszerzési célú felhasználásából ([21]). Érzékeny adatok esetében a szervezeteknek általában be kell szerezniük az érintettek megerősítő kifejezett hozzájárulását (részvételi döntés).

(23) Ugyancsak az *adatok sértetlensége és a célhoz kötöttség elve* alapján a személyes adatok csak addig őrizhetők meg az adott egyén személyazonosságát meghatározó vagy azt lehetővé tévő formában (tehát személyes adatként), amíg arra a célra/azokra a célokra szolgálnak, amely(ek)re eredetileg gyűjtötték őket, vagy amely(ek)et később engedélyeztek. Ez a kötelezettség nem akadályozza meg, hogy az adatvédelmi pajzsban részt vevő szervezetek hosszabb időszakokon keresztül folytassák a személyes adatok kezelését, azonban csupán annyi ideig és oly mértékben, ameddig ez az adatkezelés ésszerűen az alábbi konkrét célok valamelyikét szolgálja: közérdekű archiválás, újságírás, irodalom és művészet, tudományos és történeti kutatás, valamint statisztikai elemzés. A személyes adatok említett célokból történő hosszabb megőrzése az elvek által nyújtott biztosítékok hatálya alá tartozik.

(24) A *biztonság elve* értelmében a személyes adatokat létrehozó, fenntartó, felhasználó vagy terjesztő szervezeteknek „indokolt és megfelelő" biztonsági intézkedéseket kell hozniuk, szem előtt tartva az adatok kezeléséhez és jellegéhez kapcsolódó kockázatokat. További adatfeldolgozó általi kezelés esetén a szervezeteknek az elvekben előírtakkal azonos szintű védelmet garantáló szerződést kell kötniük a második adatfeldolgozóval, és lépéseket kell tenniük annak megfelelő végrehajtása érdekében.

(25) A *hozzáférés elve* ([22]) szerint az érintetteknek jogukban áll, hogy indokolási kötelezettség nélkül és csupán nem túlzott mértékű díj ellenében megerősítést kapjanak a szervezettől arra nézve, hogy a szóban forgó szervezet kezel-e velük kapcsolatos személyes adatokat, továbbá az adatokat ésszerű időn belül kell közölni. Ez a jog csak kivételes körülmények között korlátozható; a hozzáférési jog megtagadásának vagy korlátozásának minden esetben szükségesnek kell lennie, és azt megfelelően indokolni kell, valamint az említett követelmények teljesülésének igazolása a szervezetet terheli. Az érintetteknek képesnek kell lenniük arra, hogy javítsák, módosítsák vagy töröljék a személyes adatokat, amennyiben azok pontatlanok, vagy azokat az elvek megsértésével kezelik. Azokon a területeken, ahol a vállalatok a legvalószínűbben alkalmazzák a személyes adatok automatikus kezelését egyéneket érintő döntések meghozatalához (pl. hitelnyújtás, jelzáloghitel-ajánlatok, foglalkoztatás), az Egyesült Államok joga különleges védintézkedéseket biztosít a kedvezőtlen döntésekkel szemben ([23]). 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. E szabályok védintézkedéseket nyújtanak azokban a meglehetősen ritka esetekben, amikor az adatvédelmi pajzsban részt vevő szervezetek maguk hoznak automatizált döntéseket ([24]). Mivel azonban a modern digitális gazdaságban egyre gyakrabban alkalmaznak automatizált kezelést (többek között profilalkotást) az egyéneket érintő döntések meghozatalának alapjaként, ezt a területet szoros figyelemmel kell kísérni. Ezen ellenőrzés megkönnyítése érdekében az Egyesült Államok hatóságaival megállapodás született arról, hogy az automatizált döntéshozatalra vonatkozó párbeszéd – így az ezzel kapcsolatos uniós és amerikai megközelítés hasonlóságait és különbségeit érintő eszmecsere – részét képezi majd az első éves felülvizsgálatnak, és adott esetben a későbbi felülvizsgálatoknak.

([20]) Ez az adatvédelmi pajzs alapján történő valamennyi adattovábbításra vonatkozik, így akkor is alkalmazandó, amikor ezek munkaviszony keretében gyűjtött adatokat érintenek. Bár az öntanúsított amerikai szervezetek 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. 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.

([21]) Lásd a II. melléklet III. szakaszának 12. pontját.

([22]) Lásd még a „hozzáférés" kiegészítő elvet (a II. melléklet III. szakaszának 8. pontja).

([23]) Lásd pl. az egyenlő hitellehetőségről szóló törvényt (ECOA, 15 U.S.C. 1691 és azt követő szakaszai), a méltányos hitelminősítésről szóló törvényt (FRCA, 15 USC § 1681 és azt követő szakaszai), vagy a méltányos lakhatásról szóló törvényt (42 U.S.C. 3601 és azt követő szakaszai).

([24]) Az EU-n belül gyűjtött személyes adatok továbbítása keretében az egyénekhez kapcsolódó szerződéses jogviszony a legtöbb esetben az uniós adatvédelmi szabályok hatálya alá tartozó uniós adatkezelőhöz fűződik, és ezért általában ő fogja meghoznia az automatikus adatkezelésen alapuló döntéseket is. Ez azokra a forgatókönyvekre is kiterjed, amikor az uniós adatkezelő nevében megbízottként eljáró adatvédelmi pajzs szervezet végzi az adatkezelést.

(26) A *jogorvoslat, végrehajtás és felelősség elve* ([25]) szerint a részt vevő szervezeteknek erőteljes mechanizmusokat kell biztosítaniuk ahhoz, hogy megfeleljenek az egyéb elveknek és fellebbezési lehetőséget – így hatékony jogorvoslatokat – biztosítsanak azoknak az uniós érintetteknek, akiknek a személyes adatait a megfelelés megsértésével kezelték. Ha egy szervezet önkéntesen az EU–USA adatvédelmi pajzs szerinti öntanúsítás ([26]) mellett dönt, az elvek tényleges betartása számára kötelező. Az ilyen szervezeteknek évente ismételten tanúsítaniuk kell a keretben való részvételüket, hogy továbbra is igénybe vehessék az adatvédelmi pajzsot az Unióból érkező személyes adatok fogadásához. A szervezeteknek intézkedéseket kell hozniuk annak ellenőrzésére is ([27]), hogy közzétett 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 vagy a szúrópróbaszerű ellenőrzések. A szervezetnek ezenfelül hatékony jogorvoslati mechanizmust kell kialakítania a panaszok kezelésére (lásd még e tekintetben a (43) preambulumbekezdést). Az FTC-nek, a Közlekedési Minisztériumnak vagy más, erre feljogosított állami szervnek az adott szervezetre kiterjedő vizsgálati és jogérvényesítési hatáskörrel kell rendelkeznie, ami hatékonyan biztosítja az elvek betartását.

(27) Különös szabályok vonatkoznak az úgynevezett „harmadik fél részére történő adattovábbításra", vagyis arra, amikor egy 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. E szabályok célja annak biztosítása, hogy ne lehessen aláásni az uniós érintettek személyes adatai számára garantált védelmi normákat, és azok ne legyenek megkerülhetők oly módon, hogy harmadik felek részére továbbítják az adatokat. Ez különösen fontos a napjainak digitális gazdaságára jellemző, bonyolultabb adatkezelési láncok esetében.

(28) A *harmadik fél részére történő adattovábbításért való elszámoltathatóság elve* ([28]) értelmében harmadik fél részére történő bármely adattovábbításra kizárólag i. korlátozott és meghatározott célokból, ii. szerződés (vagy vállalatcsoporton belüli hasonló szabályozás ([29])) alapján, valamint csak abban az esetben kerülhet sor, iii. ha a szerződés az elvekben garantálttal azonos szintű védelmet biztosít, ami arra követelményre is kiterjed, hogy az elvek csak a nemzetbiztonsági, bűnüldözési és egyéb közérdekű célok eléréséhez szükséges mértékben korlátozhatók ([30]). Ezt a *tájékoztatás* és – harmadik fél adatkezelő részére történő adattovábbítás esetén ([31]) – 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. Az *adatok sértetlensége és a célhoz kötöttség elve* alapján az elvekben garantálttal azonos szintű védelem biztosításának kötelezettsége az előfeltételezi, hogy a harmadik fél kizárólag olyan célokból kezelheti a részére továbbított személyes adatokat, amelyek nem összeegyeztethetetlenek azokkal a célokkal, amelyek érdekében eredetileg gyűjtötték azokat, vagy amelyeket az érintett egyén később engedélyezett.

(29) 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. A harmadik fél adatátvevővel kötött szerződésnek minden esetben elő kell írnia, hogy az utóbbi értesíti az adatvédelmi pajzs szervezetét, ha megállapítja, hogy a továbbiakban nem tud megfelelni ennek a kötelezettségnek. Ha ilyen megállapítás történik, a harmadik fél általi adatkezelés megszűnik, vagy más ésszerű és megfelelő lépéseket kell tenni a helyzet

([25]) Lásd továbbá a „vitarendezés és végrehajtás" kiegészítő elvet (a II. melléklet III. szakaszának 11. pontja).
([26]) Lásd továbbá az „öntanúsítás" kiegészítő elvet (a II. melléklet III. szakaszának 6. pontja).
([27]) Lásd továbbá az „ellenőrzés" kiegészítő elvet (a II. melléklet III. szakaszának 7. pontja).
([28]) Lásd továbbá a „harmadik fél részére történő adattovábbításra vonatkozó kötelező szerződések" elnevezésű kiegészítő elvet (a II. melléklet III. szakaszának 10. pontja).
([29]) Lásd a „harmadik fél részére történő adattovábbításra vonatkozó kötelező szerződések" elnevezésű kiegészítő elvet (a 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 az öntanúsított amerikai vállalat változatlanul felelős lesz az elvek betartásáért, erős ösztönzést kap ahhoz, hogy olyan eszközöket alkalmazzon, amelyek valóban hatékonyak a gyakorlatban.
([30]) Lásd a II. melléklet I. szakaszának 5. pontját.
([31]) 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 jogkörélve élve garantálja az elvek szerint biztosított védintézkedéseket.

orvoslására ([32]). Amennyiben megfelelési probléma merül fel az (al)kezelési láncban, a személyes adatok adatkezelőjeként eljáró adatvédelmi pajzs szervezetnek kell majd bizonyítania, hogy nem felelős a kárt okozó eseményért, vagy a *jogorvoslat, végrehajtás és felelősség elve* szerint felelősséget kell vállalnia. További védintézkedések alkalmazandók harmadik fél megbízott részére történő adattovábbítás esetén ([33]).

2.2. *Az EU–USA adatvédelmi pajzs átláthatósága, igazgatása és felügyelete*

(30) Az EU–USA adatvédelmi pajzs felügyeleti és érvényesítési mechanizmusokat ír elő annak ellenőrzése és biztosítása céljából, hogy az amerikai öntanúsított vállalatok betartják az elveket és a megfelelés minden esetleges hiányosságát orvosolják. Ezeket a mechanizmusokat az elvek (II. melléklet), valamint a Kereskedelmi Minisztérium (I. melléklet), az FTC (IV. melléklet), és a Közlekedési Minisztérium (V. melléklet) által tett kötelezettségvállalások határozzák meg.

(31) Az EU–USA adatvédelmi pajzs megfelelő alkalmazása érdekében az érdekelt feleknek, például az érintetteknek, az adatátadóknak és a nemzeti adatvédelmi hatóságoknak tudniuk kell azonosítani az elveket elfogadó szervezeteket. E célból az Egyesült Államok Kereskedelmi Minisztériuma vállalta az olyan szervezetek listájának vezetését és a nyilvánosság számára hozzáférhetővé tételét, amelyek saját maguk tanúsítják az elvek elfogadását, és az e határozat I. és II. mellékletében (az adatvédelmi pajzsban részt vevő szervezetek listája) ([34]) említettek közül legalább egy végrehajtó hatóság hatáskörébe tartoznak. Az Egyesült Államok Kereskedelmi Minisztériuma frissíti a listát a szervezetek éves ismételt tanúsítási beadványai alapján, és valahányszor egy szervezet kilép vagy törlésre kerül az EU–USA adatvédelmi pajzsból. A Minisztérium vezeti továbbá a listáról eltávolított szervezetek nyilvános és hiteles listáját, amely minden esetben meghatározza az ilyen eltávolítás okát. A Minisztérium végezetül feltüntet egy linket, amely az FTC weboldalán nyilvántartott, az adatvédelmi pajzzsal kapcsolatos jogérvényesítési ügyek listájára vezet.

(32) A Kereskedelmi Minisztérium e célra létrehozott külön weboldalán közzéteszi az adatvédelmi pajzsban részt vevő szervezetek listáját és az ismételt tanúsítási beadványokat. Az öntanúsított szervezeteknek pedig fel kell tüntetniük a az adatvédelmi pajzs listáját tartalmazó minisztériumi webcímet. Ezenfelül amennyiben a szervezetek adatvédelmi szabályzata online elérhető, abban fel kell tüntetniük egy, az adatvédelmi pajzs weboldalára vezető hiperlinket, valamint a megoldatlan panaszok kivizsgálására rendelkezésre álló, független jogorvoslati mechanizmus weboldalára vagy panasz benyújtására szolgáló formanyomtatványára mutató másik hivatkozást. Az Egyesült Államok Kereskedelmi Minisztériuma a szervezeteknek a kerettel kapcsolatos tanúsításával és ismételt tanúsításával összefüggésben rendszeresen ellenőrzi, hogy azok adatvédelmi szabályzata megfelel-e az elveknek.

(33) Azokat a szervezeteket, amelyek tartósan nem felelnek meg az elveknek, el fogják távolítani az adatvédelmi pajzsban részt vevő szervezetek listájáról. E szervezeteknek vissza kell küldeniük vagy törölniük kell az EU–USA adatvédelmi pajzs keretében kapott személyes adatokat. Az eltávolítás egyéb eseteiben – például a részvételből való önkéntes kilépés vagy az ismételt tanúsítás elmulasztása esetén – a szervezet megőrizheti ezeket az adatokat, ha évente megerősíti az Egyesült Államok Kereskedelmi Minisztériuma 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). Ebben az esetben a szervezetnek meg kell határoznia a szervezeten belül az adatvédelmi pajzzsal kapcsolatos kérdések megválaszolására szolgáló kapcsolattartó pontot.

(34) A Kereskedelmi Minisztérium figyelemmel kíséri majd azokat a szervezeteket, amelyek már nem tagjai az EU–USA adatvédelmi pajzsnak, mivel önként kiléptek abból vagy lejárt a tanúsításuk, annak ellenőrzése céljából, hogy az érintettek visszaküldték, törölték vagy megőrizték-e ([35]) a keret alapján korábban kapott személyes adatokat.

([32]) 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 ésszerű és megfelelő lépéseket tesz a helyzet orvoslására. A második esetben az adatvédelmi pajzs szervezetének – amely az általa adott utasítások alapján ellenőrzi a megbízott által végzett kezelést – feladata, hogy intézkedéseket hozzon.

([33]) Ilyen esetben az egyesült államokbeli szervezetnek szintén ésszerű 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.

([34]) Az adatvédelmi pajzsban részt vevő szervezetek listájának kezelésével kapcsolatos információk az I. és II. mellékletben (az I. szakasz 3. pontja, az I. szakasz 4. pontja, a III. szakasz 6. pontjának d. alpontja és a III. szakasz 11. pontjának g. alpontja) találhatók.

([35]) Lásd pl. a II. melléklet I. szakaszának 3. pontját, III. szakasza 6. pontjának f. alpontját és III. szakasza 11. pontja g. alpontjának i. pontját.

Ha megőrzik ezeket az adatokat, a szervezetek kötelesek továbbra is alkalmazni az elveket azok vonatkozásában. Azokban az esetekben, amikor a Kereskedelmi Minisztérium az elvek teljesítésének tartós elmulasztása miatt távolítja el a szervezetet a keretből, a Minisztérium gondoskodni fog arról, hogy e szervezet visszaküldje vagy törölje a keret alapján megkapott személyes adatokat.

(35) Ha egy szervezet bármely okból kilép az EU–USA adatvédelmi pajzsból, el kell távolítania valamennyi olyan nyilvános állítást, amely szerint továbbra is részt vesz az EU–USA adatvédelmi pajzsban vagy jogosult annak előnyeire, különösen a közzétett adatvédelmi szabályzatába foglalt, az EU–USA adatvédelmi pajzsra történő bármely hivatkozást. A Kereskedelmi Minisztérium felkutatja és kezeli majd a keretben való részvétellel kapcsolatban – többek között a korábbi tagok által – megfogalmazott hamis állításokat ([36]). Az FTC, az Egyesült Államok Közlekedési Minisztériuma vagy egyéb érintett amerikai végrehajtó hatóságok jogérvényesítési 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,) ([37]) alapján perelhetők.

(36) Az Egyesült Államok Kereskedelmi Minisztériuma hivatalból ellenőrzi az adatvédelmi pajzsban való részvételre vonatkozó valamennyi hamis állítást vagy az adatvédelmi pajzs tanúsító védjegyének nem megfelelő használatát, továbbá az adatvédelmi hatóságok a Minisztérium szakosított kapcsolattartó pontjához utalhatják a szervezeteket felülvizsgálat céljából. Ha egy szervezet kilép az EU–USA adatvédelmi pajzsból, nem tesz ismételt tanúsítást vagy eltávolításra kerül az adatvédelmi pajzsban részt vevő szervezetek listájáról, az Egyesült Államok Kereskedelmi Minisztériuma folyamatosan ellenőrzi, hogy az adott szervezet törölte-e a közzétett adatvédelmi szabályzatából az adatvédelmi pajzsra történő összes olyan hivatkozást, amely a pajzsban való folyamatos részvételére enged következtetni, és ha a szervezet továbbra is hamis állításokat tesz, az FTC, az Egyesült Államok Közlekedési Minisztériuma vagy egyéb illetékes hatóság elé utalja az ügyet esetleges jogérvényesítési intézkedés céljából. A Minisztérium továbbá kérdőíveket küld azoknak az szervezeteknek, amelyeknek az öntanúsítása lejár vagy amelyek önként kiléptek az EU–USA adatvédelmi pajzsból, annak ellenőrzése céljából, hogy az adott szervezet visszaküldi vagy törli az EU–USA adatvédelmi pajzsban való részvétele során kapott személyes adatokat, vagy továbbra is alkalmazza azokra az adatvédelmi elveket, és ha a személyes adatokat meg kell őrizni, ellenőrzi, hogy a szervezeten belül ki/mely szerv látja el az adatvédelmi pajzzsal kapcsolatos kérdések megválaszolására szolgáló folyamatos kapcsolattartó pont szerepét.

(37) Az Egyesült Államok Kereskedelmi Minisztériuma hivatalból folyamatosan végzi majd az öntanúsított szervezetek megfelelőségének felülvizsgálatát ([38]), többek között részletes kérdőívek kiküldésével. Továbbá rendszeres felülvizsgálatot fog végezni minden olyan alkalommal, ha konkrét (nem komolytalan) panasz érkezik hozzá, ha egy szervezet nem ad kielégítő választ a megkereséseire, vagy ha hiteles bizonyítékok utalnak arra, hogy egy szervezet nem felel meg az elveknek. Adott esetben a Kereskedelmi Minisztérium az adatvédelmi hatóságokkal is konzultációt folytat az ilyen megfelelőségi felülvizsgálatokról.

2.3. *Jogorvoslati mechanizmusok, panaszkezelés és jogérvényesítés*

(38) Az EU–USA adatvédelmi pajzs a *jogorvoslat, végrehajtás és felelősség elve* révén arra kötelezi a szervezeteket, hogy biztosítsanak jogorvoslati lehetőséget a megfelelés hiánya által érintett egyéneknek, és így tegyék lehetővé az uniós érintetteknek, hogy panaszt nyújtsanak be az egyesült államokbeli öntanúsított vállalatok megfelelésének hiányával kapcsolatban, továbbá hogy szükség esetén hatékony jogorvoslatot biztosító határozatokkal kényszerítsék ki e panaszok rendezését.

(39) A szervezeteknek az öntanúsításuk részeként eleget kell tenniük a jogorvoslat, végrehajtás és felelősség elvének 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.

(40) A szervezetek az Unióban vagy az Egyesült Államokban található független jogorvoslati mechanizmusokat választhatják, így arra is lehetőségük van, hogy önként vállalják az együttműködést az uniós adatvédelmi hatóságokkal.

([36]) Lásd az I. melléklet „Hamis részvételi nyilatkozatok keresése és kezelése" című szakaszát.
([37]) Lásd a II. melléklet III. szakasza 6. pontjának h. alpontját és III. szakasza 11. pontjának f. alpontját.
([38]) Lásd az I. mellékletet.

Nincs azonban a szervezeteknek ilyen választási lehetőségük, ha humánerőforrás-adatokat dolgoznak fel, mivel ilyenkor kötelező együttműködniük az adatvédelmi hatóságokkal. A további alternatívák közé tartoznak a független, alternatív vitarendezés vagy azok a magánszektorban kidolgozott *adatvédelmi programok*, amelyek az adatvédelmi elveket beépítik a szabályozásukba. Az utóbbiaknak hatékony jogérvényesítési mechanizmusokat kell tartalmazniuk a jogorvoslat, végrehajtás és felelősség elve követelményeinek megfelelően. A szervezetek kötelesek orvosolni a megfelelés hiányával kapcsolatos valamennyi problémát. Azt is rögzíteniük kell, hogy az FTC, a Közlekedési Minisztérium vagy bármely más, erre feljogosított egyesült államokbeli állami szerv vizsgálati és jogérvényesítési hatáskörébe tartoznak.

(41) Következtetésképpen az adatvédelmi pajzs kerete számos lehetőséget kínál az érintetteknek, hogy érvényesítsék a jogaikat, panaszt nyújtsanak be az egyesült államokbeli öntanúsított vállalatok megfelelésének hiányával 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 vagy az FTC-hez nyújthatják be panaszukat.

(42) Ha a fenti jogorvoslati vagy jogérvényesítési mechanizmusok egyike sem vezet a panaszaik rendezéséhez, az egyének jogosultak továbbá igénybe venni az adatvédelmi pajzzsal foglalkozó testület keretén belüli kötelező választott bíráskodást is (e határozat II. mellékletének 1. 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. Tanácsos ugyanakkor egy bizonyos logikai sorrendet követni, az alábbiak szerint.

(43) Az uniós érintettek először az *egyesült államokbeli öntanúsított vállalkozással* való közvetlen kapcsolatfelvétel révén indíthatnak eljárást az elvek be nem tartása miatt. 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) és a független panaszkezelő mechanizmusokról.

(44) 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. E válasznak ki kell térnie a panasz megalapozottságának értékelésére, és az arra vonatkozó tájékoztatásra, hogy a szervezet hogyan orvosolja a problémát. Ehhez hasonlóan a szervezetek kötelesek gyorsan választ adni a Kereskedelmi Minisztériumtól vagy egy adatvédelmi hatóságtól ([39]) (ha a szervezet kötelezettséget vállalt az adatvédelmi hatósággal való együttműködésre) érkező, az elvek általuk történő elfogadásával kapcsolatos megkeresésekre és egyéb információkérésekre. A szervezeteknek meg kell őrizniük az adatvédelmi szabályzatuk végrehajtására vonatkozó nyilvántartásaikat, és kérelemre a független jogorvoslati mechanizmus vagy az FTC (vagy egyéb, a tisztességtelen és megtévesztő gyakorlatok kivizsgálására hatáskörrel rendelkező hatóság) rendelkezésére kell bocsátaniuk azokat egy adott vizsgálat vagy egy, a megfelelőség hiányával kapcsolatos panasz keretében.

(45) 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. 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 megfelelés hiányára vonatkozó megállapítások nyilvánosságát. A szervezetek által kijelölt független vitarendezési szervek kötelesek feltüntetni a nyilvános weboldalaikon az EU–USA adatvédelmi pajzzsal kapcsolatos lényeges információkat, valamint az annak alapján általuk nyújtott szolgáltatásokat. Évente közzé kell tenniük egy éves jelentést, amelyben összesített statisztikai adatokat közölnek ezekről a szolgáltatásokról ([40]).

([39]) Ez az adatvédelmi hatóságok testülete által kijelölt ügykezelő hatóság, amelyet „Az adatvédelmi hatóságok szerepe” kiegészítő elv irányoz elő (a II. melléklet III. szakaszának 5. pontja).

([40]) Az éves jelentésnek az alábbiakat kell tartalmaznia: (1) a jelentéstételi év folyamán beérkezett, adatvédelmi pajzzsal 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.

(46) A Kereskedelmi Minisztérium a megfelelőség felülvizsgálatára vonatkozó eljárásai keretében ellenőrizni fogja továbbá, hogy az egyesült államokbeli öntanúsított vállalatok valóban regisztrálták-e magukat azoknál a független jogorvoslati mechanizmusoknál, ahol állításuk szerint ezt megtették. A szervezetek és a felelős független jogorvoslati mechanizmusok egyaránt kötelesek gyorsan választ adni a Kereskedelmi Minisztérium adatvédelmi pajzzsal kapcsolatos információk iránti kérdéseire és kéréseire.

(47) Azokban az esetben, amikor a szervezet nem tesz eleget a vitarendezési vagy önszabályozási szerv döntésének, az utóbbinak értesítenie kell a teljesítés elmulasztásáról az Egyesült Államok Kereskedelmi Minisztériumát és az FTC-t (vagy a tisztességtelen és megtévesztő gyakorlatok kivizsgálására hatáskörrel rendelkező más amerikai hatóságot) vagy az illetékes bíróságot ([41]). 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, ezt a teljesítés tartós elmulasztásának fogják tekinteni, 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 ([42]). Ha a listáról való törlést követően a szervezet továbbra is az adatvédelmi pajzs szerinti tanúsítványra vonatkozó állítást tesz, a Kereskedelmi Minisztérium az FTC vagy más jogérvényesítési ügynökség elé utalja az ügyet ([43]).

(48) Harmadrészt az egyének valamely *nemzeti adatvédelmi hatóság* elé terjeszthetik a panaszaikat. A szervezetek kötelesek együttműködni az adatvédelmi hatóság általi vizsgálat és panaszrendezés során, amennyiben az adatfeldolgozás munkaviszony keretében gyűjtött humánerőforrás-adatokra vonatkozik, vagy ha az adott szervezet önként vállalta az adatvédelmi hatóságok általi felügyeletet. 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 hatós számára, hogy ilyen intézkedés meghozatalára került sor.

(49) Az adatvédelmi hatóságok ajánlását az adatvédelmi hatóságok uniós szinten ([44]) létrehozott nem hivatalos testülete kézbesíti, amely segíti majd a konkrét panasszal kapcsolatos összehangolt és összefüggő megközelítés biztosítását. Az ajánlást azután adják ki, hogy a jogvitában érdekelt mindkét fél megfelelő lehetőséget kapott a magyarázatra és a kívánt bizonyítékok benyújtására. A testület olyan gyorsan ad ajánlást, amint ezt a jogszerű eljárás követelménye megengedi, főszabály szerint a panasz beérkezésétől számított 60 napon belül. 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 megállapítja, hogy az együttműködési kötelezettségvállalást súlyosan megszegték. Az első alternatíva szerint ez az FTC-ről szóló törvény 5. szakaszán (vagy hasonló törvényen) alapuló jogérvényesítési intézkedéséhez vezethet. A második alternatíva szerint a testület tájékoztatni fogja az Egyesült Államok Kereskedelmi Minisztériumát, 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 pajzsban részt vevő szervezetek listájáról.

(50) 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 tagállam nemzeti bíróságai előtt megtámadja az ilyen intézkedést (mulasztást).

(51) 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 adatvédelmi pajzsban részt vevő szervezetek nemteljesítésével kapcsolatos ügyekben történő együttműködés megkönnyítése és fokozása érdekében az Egyesült Államok Kereskedelmi Minisztériuma 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 ([45]). Az FTC hasonlóan vállalta, hogy e célra létrehoz egy külön kapcsolattartó pontot ([46]), és az U.S. SAFE WEB (Biztonságos web) törvény ([47]) alapján vizsgálati segítséget nyújt az adatvédelmi hatóságok számára.

([41]) Lásd a II. melléklet III. szakasza 11. pontjának e. alpontját.
([42]) Lásd a II. melléklet III. szakasza 11. pontjának g. alpontját, különösen az ii. és az iii. pontot.
([43]) Lásd az I. melléklet „Hamis részvételi nyilatkozatok keresése és kezelése" című szakaszát.
([44]) 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.
([45]) Lásd az I. melléklet „Az együttműködés fokozása az adatvédelmi hatóságokkal" és „Nemteljesítéssel kapcsolatos panaszok megoldásának elősegítése" című szakaszait, valamint a II. melléklet II. szakasza 7. pontjának e. alpontját.
([46]) Lásd a IV. mellékletet, 6. o.
([47]) *ua.*

(52) Negyedrészt az Egyesült Államok *Kereskedelmi Minisztériuma* kötelezettséget vállalt arra, hogy fogadja és felülvizsgálja az adott szervezet elveknek való megfelelésének hiányával kapcsolatos panaszokat, és megteszi a legmegfelelőbb erőfeszítéseket e panaszok rendezésére. Az Egyesült Államok Kereskedelmi Minisztériuma ennek érdekében külön eljárásokat biztosít az adatvédelmi hatóságoknak, amelynek során azok az e célra létrehozott kapcsolattartó ponthoz utalhatják a panaszokat, figyelemmel kísérhetik azokat, és a rendezés elősegítése érdekében biztosíthatják a vállalati nyomonkövetést. 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. Ez lehetővé teszi, hogy az egyesült államokbeli öntanúsított vállalatok megfelelésének hiányával kapcsolatos panaszokat az érintettek közvetlenül nemzeti adatvédelmi hatóságuk elé terjesszék, és e hatóság jutassa el azokat az Egyesült Államok Kereskedelmi Minisztériumához, amely az EU–USA adatvédelmi pajzs igazgatásáért felelős amerikai hatóság. A Kereskedelmi Minisztérium arra is kötelezettséget vállalt, hogy – az EU–USA adatvédelmi pajzs működésének éves felülvizsgálata során – jelentést készít, amelyben összesítve elemzi az évente hozzá beérkező panaszokat ([48]).

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

(54) Ötödrészt az adatvédelmi pajzs szervezeteinek az Egyesült Államok hatóságai, különösen a *Szövetségi Kereskedelmi Bizottság* ([49]) vizsgálati és jogérvényesítési hatáskörébe kell tartozniuk, amely hatékonyan biztosítja majd az elvek betartását. 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 adatvédelmi elvek nem teljesítése ügyében elé utalt panaszok vizsgálatának, annak eldöntése érdekében, hogy sor került-e az FTC-ről szóló törvény 5. szakaszának megsértésére ([50]). 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 elfogadja a közvetlenül magánszemélyektől érkező panaszokat is, valamint hivatalból végez majd vizsgálatokat az adatvédelmi pajzzsal kapcsolatosan, kiváltképpen az adatvédelmi kérdésekkel kapcsolatos tágabb vizsgálatok részeként.

(55) Az FTC igazgatási végzések („hozzájárulási végzések") segítségével kikényszerítheti a megfelelést, és rendszeresen ellenőrizni fogja e végzések betartását. Ha a szervezetek nem tartják be ezeket, az FTC az illetékes bíróság elé terjesztheti az ügyet, hogy polgári jogi szankciókat vagy egyéb jogorvoslatokat igényeljen, többek között a jogellenes cselekmény okozta károk megtérítését követelje. Ennek alternatívájaként az FTC közvetlenül igényelhet ideiglenes vagy állandó meghagyást, illetve egyéb jogorvoslatot egy szövetségi bíróságtól. Az adatvédelmi pajzsban részt vevő szervezetek számára kiadott mindegyik hozzájárulási végzés önbejelentési rendelkezéseket ([51]) tartalmaz majd, és arra fogja kötelezni a szervezeteket, hogy hozzák nyilvánosságra az FTC-hez benyújtott valamennyi megfelelési vagy értékelő jelentésnek az adatvédelmi pajzzsal kapcsolatos, lényeges szakaszait. Végezetül az FTC fenntartja majd azoknak a vállalatoknak az online listáját, amelyek az FTC vagy valamely bíróság adatvédelmi pajzzsal kapcsolatos ügyekben hozott végzéseinek hatálya alá tartoznak.

(56) 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 *„adatvédelmi pajzzsal foglalkozó testület"* kötelező erejű választott bírósági eljárását. A szervezeteknek tájékoztatniuk kell az egyéneket arról a lehetőségről, hogy bizonyos feltételekkel kötelező választott bíráskodást vehetnek igénybe, és amennyiben az egyének az érintett szervezetnek küldött értesítés útján élnek az említett lehetőséggel, azok kötelesek választ adni ([52]).

([48]) Lásd az I. melléklet „Nemteljesítéssel kapcsolatos panaszok megoldásának elősegítése" című szakaszát.

([49]) Az adatvédelmi pajzsban részt vevő szervezetnek nyilvánosan közzé kell tennie azt a kötelezettségvállalását, hogy teljesíti az elveket, nyilvánosságra hozza az említett elveknek megfelelő adatvédelmi szabályzatát és teljes körűen 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.

([50]) 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.

([51]) 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.

([52]) Lásd a II. melléklet II. szakasza 1. pontjának xi. alpontját és III. szakasza 7. pontjának c. alpontját.

(57) E választott bírói testületet legalább 20 választott bíróból álló állomány alkotja, akiket a függetlenségük, feddhetetlenségük és az Egyesült Államok és az Unió adatvédelmi jogával kapcsolatos tapasztalataik alapján az Egyesült Államok Kereskedelmi Minisztériuma és a Bizottság jelöl ki. A felek minden egyes jogvita esetén kiválasztanak ebből az állományból egy választott bírót vagy egy három választott bíróból ([53]) álló tanácsot. Az eljárásra az Egyesült Államok Kereskedelmi Minisztériuma és a Bizottság által közösen elfogadandó egységes választott bírósági szabályok lesznek irányadók. E szabályok kiegészítik a már megkötött keretet, amely több olyan elemet tartalmaz, amelyek hozzáférhetőbbé teszik ezt a mechanizmust az uniós érintettek számára: i. a választott bíróság előtti követelés előkészítése során az érintett segítséget kaphat nemzeti adatvédelmi hatóságától; ii. bár a választott bírósági 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 választott bíróságon főszabály szerint az angol nyelvet használják, általában ([54]) ésszerű, indoklással ellátott kérésre a választott bírósági 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 választott bíróság előtt, az Egyesült Államok Kereskedelmi Minisztériuma az adatvédelmi pajzs szervezeteinek éves hozzájárulásaival létrehoz majd egy alapot, amely az amerikai hatóságok által – a Bizottsággal való konzultációt követően – meghatározott maximális összegek erejéig fedezni fogja a választott bírósági eljárás támogatható költségeit.

(58) Az adatvédelmi pajzzsal foglalkozó testület jogosult lesz arra, hogy az elveknek való megfelelés hiányának orvoslásához szükséges, „egyénspecifikus, nem pénzbeli méltányos jogorvoslatot" ([55]) rendeljen el. Bár a választott bíróság határozatának meghozatalakor figyelembe veszi majd az adatvédelmi pajzs egyéb mechanizmusaiból már megkapott más jogorvoslatokat, az egyének ennek ellenére választott bírósághoz fordulhatnak, ha úgy ítélik meg, hogy az említett egyéb jogorvoslatok nem elegendőek. Ez lehetővé teszi, hogy az uniós érintettek minden olyan esetben választott bírósághoz folyamodjanak, amikor az illetékes amerikai hatóságok (például az FTC) intézkedése vagy mulasztása nem rendezi kielégítően a panaszukat. Nem lehet választott bírósághoz folyamodni, ha egy adatvédelmi hatóság hatáskörrel rendelkezik egy egyesült államokbeli öntanúsított vállalattal 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 választott bírósági törvény alapján érvényesíthetik a választott bírósági határozatokat az Egyesült Államok bíróságain, így biztosítva jogorvoslatot, ha a vállalat nem teljesít.

(59) Hetedrészt, amennyiben egy szervezet nem tesz eleget annak a kötelezettségvállalásának, hogy tiszteletben tartja az elveket és a közzétett adatvédelmi szabályzatot, további jogorvoslatok vehetők igénybe az Egyesült Államok tagállamainak joga alapján, amelyek jogorvoslatokról rendelkeznek a deliktuális felelősségi jog keretében, valamint csalárd megtévesztés, tisztességtelen vagy megtévesztő cselekmények vagy gyakorlatok, illetve szerződésszegés esetén.

(60) Ezenfelül, ha egy adatvédelmi hatóság egy uniós érintettől érkező állítás alapján úgy ítéli meg, hogy az egyén személyes adatainak egy egyesült államokbeli szervezethez való továbbítását az uniós adatvédelmi jog megsértésével végezték, többek között akkor, ha az uniós adatexportőr alapos okkal feltételezi, hogy a szervezet nem teljesíti az elveket, a hatóság az adatexportőrrel szemben is élhet a jogkörével, és szükség esetén elrendelheti az adattovábbítás felfüggesztését.

(61) A Bizottság az e szakaszban szereplő információk alapján úgy véli, hogy az Egyesült Államok Kereskedelmi Minisztériuma által kibocsátott elvek önmagukban véve a személyes adatok védelmének olyan szintjét biztosítják, amely lényegében azonos a 95/46/EK irányelvben meghatározott érdemi alapelvek révén garantálttal.

(62) Továbbá az elvek tényleges alkalmazását szavatolják az átláthatósági kötelezettségek, valamint az, hogy az adatvédelmi pajzs igazgatását és megfelelőségi felülvizsgálatát az Egyesült Államok Kereskedelmi Minisztériuma végzi.

(63) A Bizottság ezenfelül úgy ítéli meg, hogy az adatvédelmi pajzs által előírt felügyeleti, jogorvoslati és jogérvényesítési mechanizmusok összességében véve lehetővé teszik, hogy a gyakorlatban azonosítsák és szankcionálják azt, ha az adatvédelmi pajzsban részt vevő szervezetek megsértik az elveket, továbbá hogy jogorvoslatot biztosítsanak az érintetteknek arra vonatkozóan, hogy betekinthessenek a rájuk vonatkozó személyes adatokba, és esetleg helyesbítsék vagy töröljék ezeket az adatokat.

([53]) A feleknek meg kell állapodniuk a választott bíróságban részt vevő választott bírák számáról.

([54]) A választott bíróság ugyanakkor megállapíthatja, hogy a konkrét választott bírósági eljárás körülményei között a felek kiadásainak fedezése indokolatlan vagy aránytalan költségekhez vezetne.

([55]) Az egyének a választott bírósági eljárásban nem igényelhetnek kártérítést, azonban a választott bírósághoz folyamodás nem zárja ki azt a lehetőséget, hogy az Egyesült Államok rendes bíróságai előtt kártérítést követeljenek.

3. AZ EGYESÜLT ÁLLAMOK HATÓSÁGAINAK HOZZÁFÉRÉSE AZ EU–USA ADATVÉDELMI PAJZS ALAPJÁN TOVÁBBÍTOTT SZEMÉLYES ADATOKHOZ, ÉS AZOK ÁLTALUK TÖRTÉNŐ FELHASZNÁLÁSA

(64) Amint a II. melléklet I. szakaszának 5. pontjából következik, az elvek elfogadása a nemzetbiztonsági, a közérdekkel összefüggő vagy a bűnüldözési követelmények teljesítéséhez szükséges mértékben korlátozható.

(65) A Bizottság megvizsgálta az Egyesült Államok jogában rendelkezésre álló korlátozásokat és biztosítékokat az Egyesült Államok hatóságainak az EU–USA adatvédelmi pajzs alapján továbbított személyes adatokhoz való nemzetbiztonsági, bűnüldözési és egyéb közérdekű célokból történő hozzáférése, és azok ilyen célokból történő felhasználása tekintetében. Ezenfelül az Egyesült Államok kormánya a nemzeti hírszerzés igazgatójának hivatala (ODNI) ([56]) útján részletes nyilatkozatokat és kötelezettségvállalásokat szolgáltatott a Bizottságnak, amelyeket e határozat VI. melléklete tartalmaz. A külügyminiszter által aláírt és e határozat III. mellékletében csatolt levélben az Egyesült Államok kormánya kötelezettséget vállalt arra is, hogy létrehoz egy új, a nemzetbiztonsági beavatkozással foglalkozó felügyeleti mechanizmust, az adatvédelmi ombudsmant, aki független a hírszerzéstől. Végezetül az Egyesült Államok Igazságügyi Minisztériumának e határozat VII. mellékletébe foglalt nyilatkozata ismerteti a hatóságok bűnüldözési és egyéb közérdekű célokból történő adathozzáférésére és -használatára vonatkozó korlátozásokat és biztosítékokat. Az említett kötelezettségvállalások átláthatóságának fokozása és jogi jellegének kidomborítása érdekében az e határozatban felsorolt és ahhoz melléklet minden egyes dokumentumot közzé fognak tenni az Egyesült Államok Szövetségi Közlönyében.

(66) A továbbiakban részletesebben kifejtjük a Bizottság arra vonatkozó megállapításait, hogy az amerikai hatóságok milyen korlátozásokkal férhetnek hozzá az Európai Unióból az Egyesült Államokba továbbított személyes adatokhoz és használhatják fel azokat, továbbá hogy létezik-e hatékony jogi védelem.

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

(67) A Bizottság által végzett elemzésből megállapítható, hogy az Egyesült Államok joga számos korlátozást tartalmaz az EU–USA adatvédelmi pajzs alapján továbbított személyes adatokhoz való nemzetbiztonsági célú hozzáférés és az ilyen adatok felhasználása tekintetében, valamint olyan felügyeleti és jogorvoslati mechanizmusokat foglal magában, amelyek elegendő biztosítékokat szolgáltatnak arra, hogy az említett adatok hatékony védelemben részesüljenek a jogellenes beavatkozással és a visszaélés kockázatával szemben ([57]). 2013 óta, amikor a Bizottság kiadta két közleményét (lásd a (7) preambulumbekezdést), jelentős mértékben megerősítették ezt a jogi keretet, amint ezt az alábbiakban ismertetjük.

3.1.1. Korlátozások

(68) Az Egyesült Államok Alkotmánya értelmében a nemzetbiztonság biztosítása az elnök hatásköre főparancsnoki és államfői minőségében, a külföldi hírszerzés vonatkozásában pedig az Egyesült Államok külpolitikájának irányítójaként ([58]). Bár a Kongresszus hatásköre, hogy korlátozásokat állapítson meg, és ezt sokféle tekintetben meg is tette, e határok között az elnök irányíthatja az Egyesült Államok hírszerzésének tevékenységét elsősorban elnöki rendeletek és irányelvek révén. Ez természetesen azokra a területekre is vonatkozik, ahol nincs kongresszusi iránymutatás. Jelenleg a két központi jogi eszköz e tekintetben az 12333. sz. elnöki rendelet ([59]) és a 28. sz. elnöki politikai irányelv.

([56]) A nemzeti hírszerzés igazgatója (DNI) a hírszerzés vezetője, valamint az elnök és a Nemzetbiztonsági Tanács főtanácsadójaként jár el. Lásd: A hírszerzés reformjáról és a terrorizmus megelőzéséről szóló 2004. évi törvény, Pub. L. 108-458 of 2004.12.17. Többek között az ODNI határozza meg a hírszerzés feladatkörére, adatgyűjtésére, elemzésére, a hírszerzési termékekre és azok megismertetésére vonatkozó követelményeket, valamint igazgatja és irányítja ezeket a tevékenységeket, többek között úgy, hogy iránymutatásokat dolgoz ki az információkhoz és hírszerzési értesülésekhez való hozzáférés, továbbá azok felhasználásának és megosztásának módjáról. Lásd az 12333. sz. elnöki rendelet 1.3 (a), (b) szakaszát.

([57]) Lásd: *Schrems-ügy*, 91. pont.

([58]) Az Egyesült Államok Alkotmányának II. cikke. Lásd még a 28. sz. elnöki politikai irányelv bevezetőjét.

([59]) 12333. elnöki rendelet: Az Egyesült Államok hírszerzési tevékenységei, Szövetségi Közlöny 40. kötet 235. sz. (1981. december 8.). Az elnöki rendelet nyilvánosan hozzáférhető részében meghatározza az Egyesült Államok hírszerzési erőfeszítéseinek célját, irányvonalait, feladat- és felelősségi körét (ideértve a hírszerzés különböző szervezeteinek szerepét), valamint ismerteti a hírszerzési tevékenység végzésének általános paramétereit (elsősorban a külön eljárási szabályok kiadásának szükségességét). Az 12333. sz. elnöki rendelet 3.2. szakasza szerint az elnök a nemzeti biztonsági tanács és a nemzeti hírszerzési igazgató támogatásával kiadja a rendelet végrehajtásához szükséges megfelelő irányelveket, eljárásokat és iránymutatásokat.

(69) A 2014. január 17-én kiadott, 28. elnöki politikai irányelv (a továbbiakban: PPD-28) több korlátozást határoz meg a jelfelderítési műveletekre ([60]). Ez az elnöki irányelv jogilag kötelező erővel rendelkezik az Egyesült Államok hírszerzési hatóságaira nézve ([61]), és az Egyesült Államok kormányának megváltozásáig marad hatályban ([62]). A PPD-28 különösen fontos a nem amerikai személyek, így az uniós érintettek számára. Többek között az alábbiakat írja elő:

a) a jelfelderítési adatgyűjtésnek törvényen vagy elnöki engedélyen kell alapulnia, és az Egyesült Államok alkotmányának (különösen a negyedik alkotmánykiegészítésnek) és törvényeinek megfelelően kell azt végezni;

b) valamennyi személyt méltósággal és tisztelettel kell kezelni, függetlenül az állampolgárságától és lakóhelyétől;

c) valamennyi személynek jogos adatvédelmi érdekei fűződnek személyes adatai kezeléséhez;

d) az adatvédelem és a polgári szabadságjogok szerves részét kell, hogy képezzék azoknak a megfontolásoknak, amelyek alapján megtervezik az Egyesült Államok jelfelderítési tevékenységét;

e) az Egyesült Államok jelfelderítési tevékenységének tehát valamennyi személy személyes adatai tekintetében megfelelő biztosítékokat kell tartalmazniuk, függetlenül azok állampolgárságától és lakóhelyétől.

(70) A PPD-28 előírja, hogy jelfelderítési adatok gyűjtése kizárólag nemzeti vagy minisztériumi megbízatás támogatására irányuló külföldi hírszerzési vagy kémelhárítási célból végezhető, nem pedig bármely egyéb célból (például azért, hogy versenyelőnyt biztosítsanak az Egyesült Államok vállalatainak). E tekintetben az ODNI kifejti, hogy a hírszerzési szervezeti egységeknek „elő kell írniuk, hogy amennyiben az a gyakorlatban megvalósítható, az adatgyűjtést konkrét külföldi hírszerzési célpontokra vagy témakörökre kell koncentrálni, diszkriminánsok (*pl.* konkrét létesítmények, kiválasztási kritériumok és azonosítók) révén." ([63]) A nyilatkozatok továbbá biztosítékot nyújtanak arra, hogy a hírszerzési információgyűjtéssel kapcsolatos döntéseket nem bízzák az egyes hírszerzők mérlegelésére, hanem olyan politikák és eljárások hatálya alá tartoznak, amelyeket az Egyesült Államok hírszerzésének különböző szervezetei (az ügynökségek) kötelesek kialakítani a PPD-28 végrehajtása céljából ([64]). Ennek megfelelően a megfelelő kiválasztási tényezők kutatása és meghatározása az általános „nemzeti hírszerzési prioritási keretben" (NIPF) történik, amely gondoskodik arról, hogy magas szintű politikai döntéshozók tűzzék ki a hírszerzési prioritásokat, és rendszeresen felülvizsgálják azokat, hogy továbbra is reagáljanak a tényleges nemzetbiztonsági fenyegetésekre és figyelembe vegyék az esetleges kockázatokat, többek között azokat, amelyek az adatvédelmet érintik ([65]). A fentiek alapján az ügynökség személyzete kutatja fel és határozza meg azokat a konkrét kiválasztási kritériumokat, amelyek alapján várhatóan a prioritásoknak megfelelő külföldi hírszerzési értesüléseket gyűjtenek ([66]). A kiválasztási kritériumokat vagy „kiválasztási tényezőket" rendszeresen felül kell vizsgálni, hogy megbizonyosodjanak arról, hogy azok továbbra is a prioritásoknak megfelelő, értékes hírszerzési adatokat szolgáltatnak-e ([67]).

([60]) Az 12333. elnöki rendelet értelmében a Nemzetbiztonsági Ügynökség (NSA) igazgatója a jelfelderítésért felelős szervezeti vezető, aki egységes szervezetet működtet a jelfelderítési tevékenységek céljára.

([61]) A „hírszerzés" fogalmának meghatározása megtalálható az 12333. elnöki rendelet 3.5. szakaszának h) pontjában és a PPD-28 1.lábjegyzetében.

([62]) Lásd az Igazságügyi Minisztérium (DOJ) Jogi Tanácsadási Hivatalának Clinton elnök számára kiadott nyilatkozatát, 2000. január 29. E jogi vélemény szerint az elnöki irányelvek „az elnöki rendeletekkel azonos anyagi jogi joghatással" rendelkeznek.

([63]) ODNI-nyilatkozatok (VI. melléklet), 3. o.

([64]) Lásd a PPD-28 4(b),(c) szakaszát. A nyilvános információk szerint a 2015. évi felülvizsgálat megerősítette a meglévő hat célt. Lásd: ODNI, Jelfelderítési reform, 2016. évi eredményjelentés.

([65]) ODNI-nyilatkozatok (VI. melléklet), 6. o. (hivatkozással a hírszerzési szervezetekről szóló 204. irányelvre). Lásd továbbá a PPD-28 3. szakaszát.

([66]) ODNI-nyilatkozatok (VI. melléklet), 6. o. Lásd például: NSA Polgári Szabadságjogi és Adatvédelmi Hivatala (NSA CLPO), Az NSA 12333. sz. elnöki rendeleten alapuló polgári szabadságjogi és adatvédelmi tevékenysége a célzott SIGINT-tevékenységek tekintetében, 2014. október 7. Lásd továbbá az ODNI 2014. évi állapot jelentését. A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (FISA) 702. szakasza szerinti, hozzáférés iránti kérelmek esetében a kereséseket a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság (FISC) által jóváhagyott adatminimalizálási eljárások szabályozzák. Lásd: NSA CLPO, A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014. április 16.

([67]) Lásd: Jelfelderítési reform, 2015. évi évfordulós jelentés. Lásd továbbá az ODNI-nyilatkozatokat (VI. melléklet), 6., 8–9., 11. o.

(71) Továbbá a PPD-28-ban előírt követelmények, amelyek szerint az adatgyűjtésnek minden esetben ([68])„a lehető legcélzottabbnak kell lennie", és a hírszerzési szervezeteknek előnyben kell részesíteniük az elérhető egyéb információkat és a megfelelő és megvalósítható alternatívákat ([69]), azt tükrözik, hogy főszabály szerint előnyben kell részesíteni a célzott adatgyűjtést a nagy mennyiségűvel szemben. Az ODNI által szolgáltatott biztosíték szerint e követelmények különösen azt szavatolják, hogy a nagy mennyiségű adatgyűjtés ne legyen sem „tömeges", sem „megkülönböztetés nélküli", és a kivétel nem váljon erősebbé a szabálynál ([70]).

(72) Jóllehet a PPD-28 elmagyarázza, hogy a hírszerzési szervezeti egységeknek időnként nagy mennyiségű jelfelderítést kell végezniük bizonyos körülmények között, például az új vagy felbukkanó veszélyek azonosítása és értékelése érdekében, a PPD-28 olyan új iránymutatást ad a hírszerzés szervezeteinek, hogy részesítsék előnyben azokat az alternatívákat, amelyek lehetővé teszik a célzott jelfelderítési tevékenységet ([71]). Ebből következően nagy mennyiségű adatgyűjtésre kizárólag akkor kerül sor, ha diszkriminánsok – például egy konkrét célponttal társítható azonosító (pl. a célszemély e-mail-címe vagy telefonszáma) – felhasználásával történő célzott adatgyűjtés „műszaki vagy operatív megfontolásokból" nem lehetséges ([72]). Ez egyaránt vonatkozik a jelfelderítési adatgyűjtés módjára és arra, hogy ténylegesen milyen adatokat gyűjtenek ([72]).

(73) Az ODNI-tól származó nyilatkozatok szerint még ha a hírszerzési szervezetek nem is tudnak egyedi azonosítókat használni a célzott adatgyűjtéshez, arra törekednek, hogy a „lehető legnagyobb mértékben" szűkítsék az adatgyűjtést. Ennek érdekében „szűrőket és más technikai eszközöket alkalmaznak, hogy azokra az eszközökre összpontosítsák az adatgyűjtést, amelyek valószínűleg külföldi hírszerzési értékkel rendelkező kommunikációt tartalmaznak" (és így megfelelnek a fenti (70) preambulumbekezdésben ismertetett folyamat alapján az amerikai döntéshozók által megfogalmazott követelményeknek). Ennek következtében a nagy mennyiségű adatgyűjtés legalább kétféleképpen válik célzottá: egyrészt mindig konkrét külföldi hírszerzési célkitűzésekre vonatkozik (pl. jelfelderítési adatok beszerzése egy adott régióban működő terrorista csoport tevékenységével kapcsolatban), és az ilyen kapcsolattal rendelkező kommunikáció gyűjtésére fókuszál. Az ODNI által szolgáltatott biztosíték szerint ezt tükrözi az a tény, hogy az „Egyesült Államok jelfelderítési tevékenysége csak egy töredékét érinti az interneten zajló kommunikációnak" ([73]). Másrészt az ODNI nyilatkozatai kifejtik, hogy az alkalmazott szűrőket és más technikai eszközöket úgy alakítják ki, hogy a „lehető legpontosabban" fókuszálják az adatgyűjtést annak érdekében, hogy minimálisra csökkentsék a begyűjtött, „nem releváns információk" mennyiségét.

(74) Végezetül még azokban az esetekben is, amelyekben az Egyesült Államok szükségesnek tartja nagy mennyiségű jelfelderítési adat gyűjtését a (70)–(73) preambulumbekezdésben meghatározott feltételek között, a PPD-28 a hat konkrétan felsorolt nemzetbiztonsági célra korlátozza az ilyen adatok felhasználását annak érdekében, hogy állampolgárságtól és lakóhelytől függetlenül védelemben részesítse valamennyi személy magánéletét és polgári szabadságjogait ([74]). A megengedhető célok közé tartozik a kémkedésből, terrorizmusból, tömegpusztító

([68]) Lásd a 63. lábjegyzetet.

([69]) Meg kell jegyezni, hogy az 12333. sz. elnöki rendelet 2.4. szakasza szerint a hírszerzési szervezeti egységeknek az Egyesült Államokban megvalósítható, „legkevesebb beavatkozással járó adatgyűjtési technikákat kell alkalmazniuk". A nagy mennyiségű adatgyűjtés célzott adatgyűjtéssel való helyettesítésének korlátai tekintetében lásd a Nemzeti Kutatási Tanács vizsgálatának eredményeit, amelyről az Európai Unió Alapjogi Ügynöksége számol be, A hírszerző szolgálatok általi megfigyelés: alapvető jogok, biztosítékok és jogorvoslatok az EU-ban (2015), 18 o.

([70]) ODNI-nyilatkozatok (VI. melléklet), 4. o.

([71]) Lásd továbbá a PPD-28 5. szakaszának d) pontját, amely előírja a nemzeti hírszerzés igazgatójának, hogy az érintett hírszerzési szervezetek vezetőivel és a Tudomány- és Technológiapolitikai Hivatallal együttműködve tegyen jelentést az elnöknek, „megvizsgálva egy olyan szoftver létrehozásának megvalósíthatóságát, amely lehetővé tenné, hogy a hírszerzési szervezetek könnyebben végezhessenek célzott információszerzést a nagy mennyiségű adatgyűjtés helyett". A nyilvános információk szerint e jelentés arra az eredményre vezetett, hogy „nem létezik olyan szoftveralapú alternatíva, amely teljes mértékben helyettesítené a nagy mennyiségű adatgyűjtést egyes nemzetbiztonsági fenyegetések feltárása terén." Lásd: Jelfelderítési reform, 2015. évi évfordulós jelentés.

([72]) Lásd a 68. lábjegyzetet.

([73]) Az ODNI nyilatkozatai (VI. melléklet). Ez kifejezetten annak az aggodalomnak az eloszlatására szolgál, amit a nemzeti adatvédelmi hatóságok fejtettek ki a megfelelőségi határozat tervezetéről szóló véleményükben. Lásd a 29. cikk szerinti munkacsoport 01/2016. sz. véleményét az EU–USA adatvédelmi pajzs megfelelőségéről szólói határozattervezetről (elfogadás: 2016. április 13.), 38. o. és 47. lábjegyzet.

([74]) Lásd a PPD-28 2. szakaszát.

fegyverekből származó, a fegyveres erőket, a kiberbiztonságot, a hadsereget vagy a katonai személyzetet érő fenyegetések, valamint a többi öt céllal kapcsolatos nemzetközi bűnözési fenyegetések felderítése és elhárítása. E célokat legalább évente felül fogják vizsgálni. Az Egyesült Államok Kormányának nyilatkozatai szerint a hírszerzési szervezetek megerősítették elemzési gyakorlatukat és az alulértékelt jelfelderítési adatok lekérdezésekre vonatkozó normáikat, hogy összhangba hozzák azokat az említett követelményekkel; a célzott lekérdezések alkalmazása „biztosítja, hogy az elemzőkhöz csak azok az adatok kerüljenek vizsgálatra, amelyekről potenciális hírszerzési értéket feltételeznek.” ([75])

(75) Ezek a korlátozások különösen fontosak az EU–USA adatvédelmi pajzs alapján továbbított személyes adatok tekintetében, különösen abban az esetben, ha a személyes adatok gyűjtése az Egyesült Államok területén kívül – így a transzatlanti kábeleken az Unióból az Egyesült Államokba való továbbításuk során – történik. Amint az Egyesült Államok hatóságai az ODNI nyilatkozataiban megerősítették, az azokban ismertetett korlátozások – többek között a PPD-28-ban foglalt korlátozások – az ilyen adatgyűjtésre is vonatkoznak ([76]).

(76) Jóllehet nem ezzel a jogi kifejezéssel éltek, az említett elvek megragadják a szükségesség és arányosság elvének lényegét. Egyértelműen előnyben részesítik a célzott adatgyűjtést, a nagy mennyiségű adatgyűjtést pedig olyan (kivételes) helyzetekre korlátozzák, amikor műszaki vagy műveleti okokból nincs lehetőség célzott adatgyűjtésre. Amennyiben a *nagy mennyiségű adatgyűjtés* nem kerülhető el, az ilyen adatok további „használata” akkor is *szigorúan* a konkrét, jogos nemzetbiztonsági célokra *korlátozott* ([77]).

(77) Az elnök államfői minőségben kiadott irányelvébe foglalt, szóban forgó követelmények az összes hírszerzési szervezet számára kötelezőek, és további végrehajtásuk az ügynökségek azon szabályai és eljárásai szerint történik, amelyek az általános elveket átültetik a napi működés konkrét irányításába. Továbbá, bár maga a PPD-28 nem kötelező a Kongresszusra nézve, a Kongresszus szintén lépéseket tett annak érdekében, hogy az Egyesült Államokban a személyes adatok gyűjtése és az ilyen adatokhoz való hozzáférés célzottan, ne pedig „általános jelleggel” történjen.

(78) A rendelkezésre álló információkból – többek között az Egyesült Államok Kormányától kapott nyilatkozatokból – következően, miután az adatokat továbbították az Egyesült Államokban található, az EU–USA adatvédelmi pajzs alapján öntanúsított szervezetekhez, az Egyesült Államok hírszerzési ügynökségei kizárólag ([78]) akkor igényelhetnek személyes adatokat, ha a kérelmük megfelel a külföldi hírszerzői tevékenység megfigyeléséről szóló törvénynek (FISA), vagy ha azt a Szövetségi Nyomozóiroda (FBI) nyújtja be az úgynevezett nemzetbiztonsági levél (NSL) ([79]) alapján. A FISA keretében több olyan jogalap létezik, amely felhasználható az uniós érintettek EU–USA adatvédelmi pajzs alapján továbbított személyes adatainak gyűjtésére (és későbbi kezelésére). A FISA

([75]) ODNI-nyilatkozatok (VI. melléklet), 4. o. Lásd továbbá a hírszerzési szervezetekről szóló 203. irányelvet.
([76]) ODNI-nyilatkozatok (VI. melléklet), 2. o. Hasonlóan alkalmazni kell az 12333. sz. elnöki rendeletben meghatározott korlátozásokat (pl. azt, hogy a gyűjtött információknak az elnök által meghatározott hírszerzési prioritásokra kell vonatkozniuk).
([77]) Lásd: *Schrems-ügy*, 93. pont.
([78]) Az FBI általi adatgyűjtés ezenfelül bűnüldözési engedélyeken is alapulhat (lásd e határozat 3.2. szakaszát).
([79]) Az NSL használatára vonatkozóan további magyarázatok találhatók az ODNI nyilatkozatokban (VI. melléklet), 13–14. és 38. o. Amint azokban kifejtik, az FBI kizárólag arra használhatja az NSL-eket, hogy nem tartalmi információkat igényeljen a nemzetközi terrorizmussal vagy titkos hírszerzési tevékenységgel szembeni védelem céljából engedélyezett nemzetbiztonsági vizsgálatokkal kapcsolatosan. Ami az EU–USA adatvédelmi pajzs alapján történő adattovábbításokat illeti, a jelek szerint a legfontosabb jogi felhatalmazás az elektronikus távközlési adatvédelmi törvény (18 U.S.C. § 2709), amely előírja, hogy az előfizetői adatokkal vagy a tranzakciós naplófájllal kapcsolatos megkeresésekben „konkrétan meg kell határozni az adott személyt, szervezetet, telefonszámot vagy számlát”.

hagyományos egyéni elektronikus megfigyelésre vonatkozó 104. szakasza ([80]), valamint a lehallgató- és nyomkövető készülékek telepítéséről szóló 402. szakasza ([81]) mellett a két központi eszköz a FISA 501. szakasza (az USA PATRIOT törvény korábbi 215. szakasza) és a FISA 702. szakasza ([82]).

(79) Ehhez kapcsolódik, hogy a 2015. június 2-án elfogadott USA FREEDOM törvény megtiltja a naplófájlok nagy mennyiségű gyűjtését a FISA 402. szakasza (lehallgató- és nyomkövető eszközök engedélyezése) és 501. szakasza (az USA PATRIOT törvény korábbi 215. szakasza) ([83]) alapján és NSL alkalmazásával, és ehelyett „kiválasztási kritériumok" alkalmazását írja elő ([84]).

(80) Jóllehet a FISA további jogi felhatalmazásokat tartalmaz a nemzeti hírszerzési tevékenységek, többek között a jelfelderítés végzésére, a Bizottság vizsgálata azt mutatta, hogy ami az EU–USA adatvédelmi pajzs alapján továbbítandó személyes adatokat illeti, mostanáig ezek a hatóságok szintén a célzott adatgyűjtésre és betekintésre korlátozták a hatóságok beavatkozását.

(81) Ez egyértelmű a FISA 104. szakaszán alapuló hagyományos egyéni elektronikus megfigyelés esetében ([85]). Ami a FISA 702. szakaszát illeti, amely alapot szolgáltat az Egyesült Államok hírszerző ügynökségei által működtetett két fontos hírszerzési program (PRISM, UPSTREAM) számára, a kereséseket célzottan, olyan egyedi kiválasztási tényezők alapján végzik, amelyek meghatározzák a konkrét kommunikációs eszközöket, például az e-mail címre vagy telefonszámra irányulnak, azonban nem tartalmaznak kulcsszavakat vagy akár a célszemélyek nevét ([86]).

([80]) 50 U.S.C. § 1804. Jóllehet ez a jogi felhatalmazás szükségessé teszi azoknak a tényeknek és körülményeknek a megnevezését, amelyek alapján a kérelmező indokolja azt a meggyőződését, hogy (A) „az elektronikus megfigyelés célpontja külföldi hatalom vagy külföldi hatalom ügynöke", ez utóbbi kiterjedhet a nemzetközi terrorizmusban vagy tömegpusztító fegyverek nemzetközi terjesztésében (és azok előkészítő cselekményeiben) részt vevő nem amerikai állampolgárokra is (50 U.S.C. § 1801 (b)(1)). Az EU–USA adatvédelmi pajzs alapján történő személyesadat-továbbításokhoz fűződő kapcsolat mégis csupán elméleti jellegű, mivel a tényekre vonatkozó nyilatkozatban indokolni kell azt a meggyőződést is, hogy „az elektronikus megfigyelés célpontját jelentő létesítményeket vagy helyeket külföldi hatalom vagy külföldi hatalom ügynöke használja, vagy fogja felhasználni". E felhatalmazás alkalmazáshoz mindenestre kérelmet kell benyújtani a FISC-hez, amely többek között megvizsgálja, hogy az ismertetett tények alapján valószínűsíthető-e, hogy valóban ez a helyzet.

([81]) Az 50 U.S.C. 1842 §., 1841 §. (2) bekezdés, valamint a 18. cím 3127. szakasza. 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). A felhatalmazáshoz a FISC (vagy amerikai szövetségi bíró) végzését kell kérni, valamint alkalmazni kell egy, az 1841 §. (4) bekezdése értelmében vett konkrét kiválasztási kritériumot, vagyis egy olyan kritériumot, amely kifejezetten azonosít egy személyt, bankszámlát stb., és úgy kell azt felhasználni, hogy az ésszerűen lehetséges legnagyobb mértékben korlátozza az igényelt információk körét.

([82]) Míg a FISA 501. szakasza (az USA PATRIOT törvény korábbi 215. szakasza) felhatalmazza az FBI-t, hogy bírósági végzést kérjen „tárgyi bizonyítékok" (különösen telefon metaadatok, de cégnyilvántartásai adatok is) külföldi hírszerzési célokból történő megszerzése érdekében, a FISA 702. szakasza lehetővé teszi, hogy az Egyesült Államok hírszerzésének szervezetei az Egyesült Államokon belülről megkíséreljenek hozzájutni egyes információkhoz – többek között az internetes kommunikáció tartalmához – egyes Egyesült Államokon kívüli, nem amerikai célszemélyek tekintetében.

([83]) E rendelkezés alapján a FBI „tárgyi bizonyítékokat" (pl. nyilvántartások, iratok, dokumentumok) igényelhet, ha igazolja a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság (FISC) számára, hogy alapos indokkal feltételezhető, hogy azok lényegesek egy konkrét FBI-nyomozás szempontjából. E lekérdezések végzése során az FBI-nak azokat a FISC általi jóváhagyott kiválasztási kritériumokat kell használnia, amelyek esetében „ésszerű és megalapozott a gyanúja" annak, hogy az ilyen kritériumok a nemzetközi terrorizmusban vagy annak előkészítésében részt vevőkülföldi hatalomhoz vagy annak ügynökéhez társíthatók. Lásd: adatvédelmi és állampolgári jogi felügyeleti bizottság (PCLOB), a 215. szakaszra vonatkozó jelentés, 59. o.; NSA CLPO, Átláthatósági jelentés: Az USA FREEDOM törvény Cégnyilvántartási adatok FISA végrehajtás, 2016. január 15., 4–6. o.

([84]) Az ODNI nyilatkozatai (VI. melléklet), 13. o. (38. lábjegyzet).

([85]) Lásd a 81. lábjegyzetet.

([86]) PCLOB, a 702. szakaszra vonatkozó jelentés, 32–33. o., további hivatkozásokkal. Az NSA adatvédelmi hivatala szerint a szervezetnek ellenőriznie kell a célpont és a kiválasztási kritérium 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.

Ezért – amint az adatvédelmi és polgári szabadságjogi felügyelő tanács (PCLOB) megállapította – a 702. szakasz szerinti megfigyelés „teljes egészében konkrét [nem amerikai] személyekre irányul, akiknek a kilétét egyénenként határozzák meg” ([87]). A FISA 702. szakaszát 2017-ben felül kell majd vizsgálni egy hatályvesztésre vonatkozó rendelkezés miatt, és a Bizottságnak ekkor ismét meg kell vizsgálnia az uniós érintettek rendelkezésére álló biztosítékokat.

(82) Továbbá az Egyesült Államok kormányának az Európai Bizottság számára adott nyilatkozatai kifejezetten biztosítanak arról, hogy az Egyesült Államok hírszerzése „nem folytat bárkire – köztük egyszerű európai polgárokra – megkülönböztetés nélkül kiterjedő megfigyelést” ([88]). Ami az Egyesült Államokon belül gyűjtött személyes adatokat illeti, ezt a nyilatkozatot olyan empirikus bizonyítékok támasztják alá, amelyek azt mutatják, hogy az NSL útján benyújtott és a FISA-n alapuló *hozzáférés iránti megkeresések* egyedileg és együttesen is csupán viszonylag kis számú célpontra irányulnak az interneten zajló teljes adatáramláshoz viszonyítva ([89]).

(83) Ami a gyűjtött adatokhoz való *hozzáférést* és az *adatbiztonságot* illeti, a PPD-28 előírja, hogy „a hozzáférést az arra jogosult olyan személyzetre kell korlátozni, akinek feladatai ellátásához ismernie kell az információkat”, valamint hogy „a személyes adatokat olyan feltételek mellett kell kezelni és tárolni, amelyek megfelelő védelmet nyújtanak és megakadályozzák arra nem jogosult személyek hozzáférését, az érzékeny információkra vonatkozó megfelelő biztosítékokkal összhangban”. A nemzetbiztonsági személyzet megfelelő képzésben részesült a PPD-28-ban foglalt elvekről ([90]).

(84) Végezetül ami az Egyesült Államok hírszerzési hatóságai által az uniós érintettektől gyűjtött személyes adatok *tárolását* és további *terjesztését* illeti, a PPD-28 kimondja, hogy valamennyi személyt (így a nem amerikai személyeket is) méltósággal és tisztelettel kell kezelni, továbbá hogy minden személynek vannak jogos adatvédelmi érdekei személyes adatai kezelése tekintetében, továbbá hogy a hírszerzési szervezeti egységeknek ezért olyan politikákat kell kialakítaniuk, amelyek az ilyen adatok esetében megfelelő biztosítékokat nyújtanak arra, hogy azok „kialakítása ésszerűen a minimumra csökkenti a jelfelderítési tevékenységekből gyűjtött személyes adatok terjesztését és megőrzését” ([91]).

([87]) PCLOB, a 702. szakaszra vonatkozó jelentés, 111. o. Lásd még: az ODNI nyilatkozatai (VI. mellékletek), 9. o. („A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakasza szerinti adatgyűjtés nem »tömeges és megkülönböztetés nélküli«, hanem szűk körben a jogszerű célpontként azonosított magánszemélyekre vonatkozó külföldi hírszerzési adatok gyűjtésére irányul”), valamint 13. o., 36. lábjegyzet (hivatkozással a 2014. évi FISC véleményre); NSA CLPO, A külföldi hírszerzői tevékenységről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014. április 16. Az NSA még az UPSTREAM esetében is kizárólag a kiválasztási kritériumok szerinti hírszerzési tárgytól induló vagy ahhoz érkező, illetve azzal kapcsolatos elektronikus kommunikáció megszerzését igényelhet.

([88]) ODNI-nyilatkozatok (VI. melléklet), 18. o. Lásd még a 6. oldalt, amely szerint az alkalmazandó eljárások „egyértelmű elkötelezettséget tükröznek az önkényes és megkülönböztetés nélküli jelfelderítési adatgyűjtés megelőzése, valamint kormányunk legmagasabb szintje részéről az ésszerűség elvének érvényesítése mellett”.

([89]) Lásd a nemzeti biztonsági hatóságok alkalmazásával kapcsolatos statisztikai átláthatósági jelentést, 2015. április 22. A teljes internetes adatfolyamat tekintetében lásd például: Alapjogi Ügynökség, A hírszerző szolgálatok általi megfigyelés: Alapvető jogok, biztosítékok és jogorvoslatok az EU-ban (2015), 15–16 o. Ami az UPSTREAM programot illeti, a FISC titkosítás alól feloldott 2011-es véleménye szerint a FISA 702. szakasza szerint megszerzett elektronikus kommunikáció több, mint 90 %-a a PRISM programból származik, míg kevesebb, mint 10 %-a az UPSTREAM-ből. Lásd: FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 2011.3.10.), 21. sz. (elérhető az alábbi weboldalon: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Lásd a PPD-28 4(a)(ii). szakaszát. Lásd továbbá: ODNI, Mindenki személyes adatainak megóvása: Állapotjelentés a 28. elnöki politikai irányelv szerinti eljárások kidolgozásáról és végrehajtásáról, 2014. július 28., 5. o., amely szerint „A hírszerzési szervezeti egységek politikáinak erősíteniük kell a meglévő elemzési gyakorlatokat és előírásokat, amelyek szerint az elemzőknek strukturális lekérdezések vagy egyéb keresési kritériumok és technikák segítségével törekedniük kell arra, hogy azonosítsák az érvényes hírszerzési vagy bűnüldözési feladat szempontjából releváns hírszerzési információkat; a személyekre vonatkozó kereséseket valamely hírszerzési vagy bűnüldözési követelménynek megfelelő hírszerzési információkategóriára összpontosítsák; és minimálisra csökkentsék a hírszerzési vagy bűnüldözési követelmények szempontjából nem releváns személyes adatok felülvizsgálatát.” Lásd pl. CIA, jelfelderítési tevékenységek, 5. o.; FBI, a 28. elnöki politikai irányelv politikái és eljárásai, 3. o. A jelfelderítés reformjáról szóló 2016. évi eredményjelentés szerint a hírszerzési szervezeti egységek (így az FBI, a CIA és a NSA) intézkedéseket hoztak, hogy új képzési politikák létrehozásával vagy a meglévők módosításával felhívják személyzetük figyelmét a PPD-28 követelményeire.

([91]) Az ODNI nyilatkozatai szerint e korlátozások attól függetlenül alkalmazandók, hogy az adatokat nagy mennyiségű vagy célzott adatgyűjtés keretében gyűjtötték, és hogy az érintett milyen állampolgárságú.

(85) Az Egyesült Államok kormánya elmagyarázta, hogy ez az ésszerűségi követelmény azt jelenti, hogy a hírszerzési szervezeti egységeknek nem kell majd „minden elméletileg lehetséges intézkedést" elfogadniuk, hanem „egyensúlyt kell teremteniük a magánélet és az alapvető szabadságjogok védelméhez fűződő érdek jogszerű védelmére irányuló erőfeszítéseik és a jelfelderítési tevékenységek gyakorlati szükségletei között". ([92]) E tekintetben a nem amerikai állampolgárokat az amerikai személyekkel azonosan fogják kezelni a legfőbb ügyész által jóváhagyott eljárásokban ([93]).

(86) E szabályok szerint az adatmegőrzés általában maximum öt évre korlátozódik, kivéve, ha konkrét jogszabályi előírás vagy a nemzeti hírszerzés igazgatójának az adatvédelmi aggályok gondos értékelése után – az ODNI polgári szabadságjogi tisztviselője, valamint az ügynökség adatvédelmi és polgári szabadságjogi tisztviselője álláspontjának figyelembevételével – tett, kifejezett határozata szerint a további adatmegőrzés a nemzetbiztonság érdekében áll ([94]). A terjesztés azokra az esetekre korlátozódik, amikor az információk relevánsak az adatgyűjtés alapjául szolgáló cél szempontjából, tehát eleget tesznek az engedélyezett külföldi hírszerzési vagy bűnüldözési követelménynek ([95]).

(87) Az Egyesült Államok kormánya által adott biztosítékok szerint a személyes adatok nem terjeszthetők kizárólag azért, mivel az érintett személy nem amerikai állampolgár, továbbá „nem minősülnek különösen terjeszthetőnek vagy tartósan megőrizhetőnek a külföldi személy rutinszerű tevékenységeire vonatkozó jelfelderítési adatok egyedül amiatt, mert külföldiről van szó, kivéve, ha ezek az adatok egyébként felhasználhatóak egy engedélyezett külföldi hírszerzési követelmény céljaira." ([96])

(88) Mindezek alapján a Bizottság arra a következtetésre jutott, hogy az Egyesült Államokban léteznek olyan szabályok, amelyeknek az a célja, hogy a szóban forgó törvényes cél eléréséhez feltétlenül szükséges mértékűre korlátozzanak bármely nemzetbiztonsági célú beavatkozást azon személyek alapvető jogaiba, akiknek a személyes adatait az EU–USA adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbították.

(89) Amint a fenti elemzés mutatja, az Egyesült Államok joga biztosítja, hogy megfigyelési intézkedéseket kizárólag külföldi hírszerzési információk szerzése – ami jogos politikai célkitűzés ([97]) – érdekében, és a lehető

([92]) Lásd az ODNI nyilatkozatait (VI. melléklet).

([93]) Lásd: PPD-28. 4(a)(i). szak. és 12333. elnöki rendelet 2.3. szak.

([94]) Lásd a PPD-28 4(a)(i). szak.; ODNI-nyilatkozatok (VI. melléklet), 7. o. Például a FISA 702. szakasza alapján gyűjtött személyes adatok esetében az NSA-nak a FISC által jóváhagyott adatminimalizálási eljárásai azt a szabályt irányozzák elő, hogy a PRISM metaadatok és alulértékelt tartalom nem őrizhető meg öt évnél tovább, az UPSTREAM adatok esetében pedig az adatmegőrzés legfeljebb két év. Az NSA ezeket a tárolási korlátozásokat automata adatfeldolgozás révén teljesíti, amely a megfelelő megőrzési időszak végén törli a gyűjtött adatokat. Lásd: NSA, A FISA 702. szakasza szerinti adatminimalizálási eljárások, 7. szak. és 6(a)(1). szak.; NSA CLPO, A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014. április 16. Ehhez hasonlóan a FISA 501. szakasza (az USA PATRIOT törvény korábbi 215. szakasza) alapján az adatmegőrzés öt évre korlátozódik, kivéve, ha a személyes adatok külföldi hírszerzési információk megfelelően jóváhagyott terjesztésének részét képezik vagy az Igazságügyi Minisztérium írásban arról tájékoztatja az NSA-t, hogy a nyilvántartott adatok egy folyamatban lévő vagy előreláthető peres ügyben adatmegőrzési kötelezettség hatálya alá tartoznak. Lásd NSA CLPO, Átláthatósági jelentés: Az USA FREEDOM törvény Cégnyilvántartási adatok FISA végrehajtás, 2016. január 15.

([95]) Konkrétan a FISA 501. szakasza (az USA PATRIOT törvény korábbi 215. szakasza) esetén a személyes adatok terjesztése kizárólag terrorelhárítási célból vagy bűncselekmény bizonyítékaként történhet: a FISA 702. szakasza esetén kizárólag akkor, ha van érvényes külföldi hírszerzési vagy bűnüldözés cél. Vö.: NSA CLPO, A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014. április 16.; Átláthatósági jelentés: Az USA FREEDOM törvény Cégnyilvántartási adatok FISA végrehajtás, 2016. január 15. Lásd továbbá: Az NSA 12333. sz. elnöki rendeleten alapuló polgári szabadságjogi és adatvédelmi tevékenysége a célzott SIGINT tevékenység tekintetében, 2014. október 7.

([96]) Az ODNI nyilatkozatai (VI. melléklet), 7. o. (hivatkozással a hírszerzési szervezetekről szóló 203. irányelvre (ICD)).

([97]) A Bíróság egyértelművé tette, hogy a nemzetbiztonság jogos politikai célkitűzés. Lásd: *Schrems-ügy,* 88. pont. Lásd továbbá a *Digital Rights Ireland és társai* ügyben hozott ítélet 42–44. és 51. pontját, amelyekben a Bíróság úgy ítélte meg, hogy a súlyos bűnözés, különösen a szervezett bűnözés és a terrorizmus elleni küzdelem nagymértékben függ a modern nyomozati technikák alkalmazásától. Ezenfelül, szemben a bűnügyi nyomozással, amely általában a múltbeli cselekménnyel kapcsolatos felelősség és bűnösség visszamenőleges meghatározására irányul, a hírszerzési tevékenység gyakran a nemzetbiztonságot érő fenyegetések elhárítására összpontosít, mielőtt a kár bekövetkezne. Ezért az ilyen nyomozásoknak gyakran a lehetséges elkövetők („célszemélyek") szélesebb körére és tágabb földrajzi térségre kell kiterjedniük. Vö.: EJEB *Weber és Saravia kontra Németország* ügy, határozat: 2006. június 29., Kereset sz.: 54934/00., 105–118. pont (az úgynevezett „stratégiai figyelemmel kísérésről").

legcélzottabban alkalmazzanak. Mindenekelőtt a nagy mennyiségű adatgyűjtés csak kivételesen engedélyezett abban az esetben, amikor a célzott adatgyűjtés nem megvalósítható, és további biztosítékok kísérik, amelyek a gyűjtött adatok mennyiségének és a későbbi hozzáféréseknek (amelyeknek célzottnak kell lenniük és csak konkrét célokból engedélyezhetők) a minimalizálására irányulnak.

(90) A Bizottság értékelése szerint ez megerősíti a Bíróság által a *Schrems-ügyben* meghatározott normát, amely szerint a Charta 7. és 8. cikkében garantált alapvető jogokba való beavatkozással járó jogszabályoknak „minimális követelményeket" ([98]) kell előírniuk, valamint „nem a feltétlenül szükségesre korlátozódik az olyan szabályozás, amely általános jelleggel lehetővé teszi minden olyan személy összes személyes adatának tárolását, akiknek az adatait az Unióból az Egyesült Államokba továbbították, anélkül hogy a kitűzött cél alapján bármilyen különbségtételt, korlátozást vagy kivételt alkalmazna, és anélkül, hogy olyan objektív kritériumot írna elő, amely lehetővé tenné a hatóságok adatokhoz való hozzáférésének és azok későbbi felhasználásának meghatározott célokra történő, szigorúan behatárolt, valamint az ezen adatokhoz való hozzáférés és az azok felhasználása által okozott beavatkozás igazolására alkalmas korlátozását." ([99]) Nem kerül sor valamennyi személy adatainak korlátozás nélküli gyűjtésére és tárolására, sem pedig korlátlan hozzáférésre. Továbbá a Bizottsághoz eljuttatott nyilatkozatok – köztük az a biztosíték, miszerint az Egyesült Államok jelfelderítési tevékenysége csak egy töredékét érinti az interneten zajló kommunikációnak – kizárják, hogy „általános jelleggel" ([100]) hozzáférnének az elektronikus kommunikáció tartalmához.

3.1.2. Hatékony jogvédelem

(91) A Bizottság megvizsgálta az Egyesült Államokban meglévő felügyeleti mechanizmusokat az Egyesült Államok hírszerző hatóságainak az Egyesült Államokba továbbított személyes adatokba való beavatkozása tekintetében, valamint az egyéni jogorvoslatot igénylő uniós érintettek rendelkezésére álló lehetőségeket.

Felügyelet

(92) Az Egyesült Államok hírszerzési szervezetei a három hatalmi ág különféle felülvizsgálati és felügyeleti mechanizmusainak hatálya alá tartoznak. Ilyenek a végrehajtó hatalom belső és külső szervei, több kongresszusi bizottság, valamint a bírósági felügyelet; utóbbi kifejezetten a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény alapján végzett tevékenységek vonatkozásában.

(93) Először is az Egyesült Államok hatóságainak hírszerző tevékenysége a végrehajtó hatalmi ágon belüli kiterjedt felügyelet hatálya alá tartozik.

(94) A PPD-28 4(a)(iv) szakasza szerint a hírszerzési szervezeti egységek eljárásainak „megfelelő intézkedéseket kell felölelniük a személyes adatok védelemére vonatkozó biztosítékok végrehajtása feletti felügyelet elősegítése érdekében"; ezen intézkedéseik közé kell tartoznia az időszakos ellenőrzésnek ([101]).

([98]) *Schrems-ügy*, 91. pont, a további hivatkozásokkal.
([99]) *Schrems-ügy*, 93. pont.
([100]) Vö. *Schrems-ügy*, 94. pont.
([101]) ODNI, Mindenki személyes adatainak megóvása: Állapotjelentés a 28. elnöki politikai irányelv szerinti eljárások kidolgozásáról és végrehajtásáról, 7. o. Lásd pl. CIA, jelfelderítési tevékenységek, 6. o. (Megfelelés); FBI, a 28. elnöki politikai irányelv politikái és eljárásai, III (A)(4), (B)(4) szak.; NSA, PPD-28 4. szakasz Eljárások, 2015. január 12., 8.1, 8.6(c) szak.

(95) Ezzel kapcsolatosan több felügyeleti réteget hoztak létre, ideértve a polgári szabadságjogi vagy adatvédelmi tisztségviselőket, a főellenőröket, az ODNI Polgári Szabadságjogi és Adatvédelmi Hivatalát, az adatvédelmi és állampolgári jogi felügyeleti bizottságot (PCLOB) és az Elnöki Hírszerzési Felügyeleti Testületet. Az említett felügyeleti feladatokat az összes ügynökség megfeleléssel foglalkozó személyzete támogatja ([102]).

(96) Amint az Egyesült Államok kormánya kifejtette ([103]), felügyeleti feladatkörrel megbízott *polgári szabadságjogi és adatvédelmi tisztségviselők* dolgoznak a különböző, hírszerzési felelősségi körrel rendelkező minisztériumokban és a hírszerző ügynökségeknél ([104]). Bár az említett 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 (és egyes esetekben, például az ODNI esetében, hatáskörük a panaszok kivizsgálására is kiterjedhet ([105])). A minisztérium/ügynökség vezetője pedig gondoskodik arról, hogy a tisztségviselő hozzájusson valamennyi információhoz, és betekinthessen a feladatai ellátásához szükséges minden anyagba. A polgári szabadságjogi és adatvédelmi 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 ([106]). A nemzeti adatvédelmi hatóságok értékelése szerint a polgári szabadságjogi és adatvédelmi tisztségviselők által gyakorolt belső felügyelet „elég szilárdnak" tekinthető, még ha álláspontjuk szerint nem is teljesíti a függetlenség szükséges szintjét ([107]).

(97) Ezenfelül a hírszerzés minden szervezeti egysége saját *főellenőrrel* rendelkezik, akinek a feladata többek között a külföldi hírszerzési tevékenység felügyelete ([108]). Így többek között az ODNI keretében működő főellenőri hivatal 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 ([109]). A főellenőrök független jogállású ([110]) szervezeti egységek, amelyek a megfelelő ügynökség által végzett, nemzetbiztonsági célú programokkal és műveletekkel – így a törvénysértésekkel és visszaélésekkel – kapcsolatos ellenőrzések és vizsgálatok elvégzésért felelősek ([111]).

([102]) Például az NSA a Megfelelési Igazgatóságán több mint 300 megfeleléssel foglalkozó munkatársat alkalmaz. Lásd az ODNI nyilatkozatait (VI. melléklet), 7. o.

([103]) Lásd: ombudsmani mechanizmus (III. melléklet) 6(b) (i)–(iii) szak.

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

([105]) Az Egyesült Államok kormánya szerint, ha az ODNI Polgári Szabadságjogi és Adatvédelmi Hivatalához panasz érkezik, a hivatal a többi hírszerzési szervezeti egységgel is egyeztet arról, hogy a továbbiakban hogyan fogják kezelni a panaszt a hírszerzési szervezetekben. Lásd: ombudsmani mechanizmus (III. melléklet), 6(b) (ii) szak.

([106]) Lásd: 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről (elfogadás: 2016. április 13.), 41. o.

([108]) ODNI-nyilatkozatok (VI. melléklet), 7. o. Lásd: NSA, PPD-28 4. szakasz Eljárások, 2015. január 12., 8.1; CIA, jelfelderítési tevékenységek, 7. o. (Feladatkörök).

([109]) Ezt a főellenőrt (amelynek hivatalát 2010 októberében hozták létre) az elnök nevezi ki a Szenátus jóváhagyásával, és csak az elnök mentheti fel beosztásából, nem pedig a nemzeti hírszerzés igazgatója.

([110]) Az említett 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 Védelmi Minisztérium főellenőre); 8E. §. (az Igazságügyi Minisztérium főellenőre), 8G. §. (2)(A),(B) (az NSA főellenőre); 50. U.S.C. § 403q (b) (a CIA főellenőre); A 2010-es költségvetési évre vonatkozó hírszerzési engedélyezési törvény, 405(f) szak., (a hírszerzési szervezet főellenőre). A nemzeti adatvédelmi hatóságok értékelése szerint a főellenőrök *„valószínűleg megfelelnek az Európai Unió Bírósága és az Emberi Jogok Európai Bírósága (EJEB) meghatározása szerinti szervezeti függetlenségnek, legalábbis amikortól az új kinevezési eljárás mindegyikükre vonatkozik*." Lásd: a 29. cikk szerinti munkacsoport 01/2016. sz. véleménye az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről (elfogadás: 2016. április 13.) 40. o.

([111]) Lásd az ODNI nyilatkozatait (VI. melléklet), 7. o. Lásd továbbá a Pub. L. 113-126. o. 2014. július 7. által módosított, a főellenőrről szóló 1978. évi törvényt.

Jogosultak betekinteni 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 ([112]). Bár a főellenőrök csupán korrekciós intézkedésekre vonatkozó, jogilag nem kötelező ajánlásokat adhatnak ki, jelentéseiket – többek között a nyomonkövetési intézkedésekről (vagy azok hiányáról) szóló jelentéseiket – nyilvánosságra hozzák, és emellett elküldik a Kongresszusnak, amely ezek alapján gyakorolhatja felügyeleti funkcióját ([113]).

(98) Továbbá az *adatvédelmi és polgári szabadságjogi felügyelő tanács* (PCLOB) – a végrehajtó hatalmi ágba tartozó, kétpárti független hivatal ([114]), amelynek öttagú igazgatóságát ([115]) az elnök nevezi ki hatéves hivatali időre a Szenátus jóváhagyásával – rendelkezik hatáskörrel a terrorelhárítási politika és annak végrehajtása terén az adatvédelem és a polgári szabadságjogok védelme érdekében. A tanács a hírszerzés 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. Megkapja több szövetségi minisztérium/ügynökség polgári szabadságjogi és adatvédelmi tisztviselőinek ([116]) jelentéseit, ajánlásokat adhat ki számukra, és rendszeresen beszámol a kongresszusi bizottságoknak és az elnöknek ([117]). A PCLOB feladata továbbá, hogy megbízatásának keretei között a PPD-28 végrehajtását értékelő jelentést készítsen.

(99) A fenti felügyeleti mechanizmusokat végezetül az elnöki hírszerzési tanácsadó testületen belül létrehozott *hírszerzési felügyeleti testület* egészíti ki, amely azt felügyeli, hogy az Egyesült Államok hírszerző hatóságai betartják-e az Alkotmányt és az összes alkalmazandó szabályt.

(100) A felügyelet elősegítése érdekében arra ösztönzik a hírszerzési szervezeti egységeket, hogy alakítsanak ki olyan információs rendszereket, amelyek lehetővé teszik a személyes adatok lekérdezésének vagy egyéb keresésének figyelemmel kísérését, rögzítését és felülvizsgálatát ([118]). A felügyeleti és megfelelési testületek időszakonként ellenőrzik a nemzeti hírszerzési egységek gyakorlatait a jelfelderítésben szereplő személyes adatok védelme tekintetében, és azt, hogy betartják-e ezeket az eljárásokat ([119]).

(101) Emellett az említett felügyeleti funkciók ellátását a megfelelés hiányával kapcsolatos, széles körű jelentéstételi kötelezettségek segítik elő. Az ügynökségi eljárásoknak mindenekelőtt gondoskodniuk kell arról, hogy amennyiben állampolgárságtól függetlenül bármely személy jelfelderítés útján gyűjtött személyes adatait érintő, jelentős megfelelési probléma merül fel, az ilyen problémát haladéktalanul jelentsék a hírszerzési egység vezetőjének, aki pedig értesíti a nemzeti hírszerzési igazgatót, aki a PPD-28 alapján megállapítja, hogy szükség van-e korrekciós intézkedésekre ([120]). Ezenfelül az 12333. elnöki rendelet értelmében az összes hírszerzési szervezet köteles beszámolni a Hírszerzési Felügyeleti Testületnek a megfelelés hiányával kapcsolatos eseményekről ([121]). Az említett mechanizmusok biztosítják, hogy a problémával a hírszerzés legmagasabb szintjén

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

([113]) Lásd az ODNI nyilatkozatait (VI. melléklet), 7. o. Lásd a főellenőrről szóló 1978. évi törvény 4. §-ának (5) bekezdését és 5.§-át. A 2010-es költségvetési évre vonatkozó hírszerzési engedélyezési törvény, Pub. L. 111-259. o., 2010. július 10., 405(b)(3),(4) szak. szerint a hírszerzési szervezet főellenőre folyamatosan tájékoztatja a DNI-t és a Kongresszust a korrekciós intézkedések szükségességéről és azok előrehaladásáról.

([114]) A nemzeti adatvédelmi hatóságok értékelése szerint a PCLOB a múltban „igazolta független hatáskörét". Lásd: a 29. cikk szerinti munkacsoport 01/2016. sz. véleménye az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről (elfogadás: 2016. április 13.) 42. o.

([115]) Ezenfelül a PCLOB mintegy 20 fő állandó munkatársat alkalmaz. Lásd: https://www.pclob.gov/about-us/staff.html.

([116]) 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.

([117]) Lásd: 42 U.S.C. § 2000ee. Lásd továbbá: ombudsmani mechanizmus (III. melléklet), 6(b) (ii)szak. A PCLOB többek között köteles jelentést tenni arról, ha egy végrehajtó hatalmi ügynökség nem követi az ajánlását.

([118]) ODNI, Mindenki személyes adatainak megóvása: Állapotjelentés a 28. elnöki politikai irányelv szerinti eljárások kidolgozásáról és végrehajtásáról, 7–8. o.

([119]) Uo. 8. o. Lásd továbbá az ODNI nyilatkozatait (VI. melléklet), 9. o.

([120]) ODNI, Mindenki személyes adatainak megóvása: Állapotjelentés a 28. elnöki politikai irányelv szerinti eljárások kidolgozásáról és végrehajtásáról, 7. o. Lásd: NSA, PPD-28 4. szakasz Eljárások, 2015. január 12., 7.3, 8.7(c),(d) szak.; FBI, a 28. elnöki politikai irányelv politikái és eljárásai, III.(A)(4), (B)(4) szak.; CIA, jelfelderítési tevékenységek, 6. o. (Megfelelés) és 8. o. (Feladatkörök).

([121]) Lásd az 12333. sz. elnöki rendelet 1.6(c). szak.

foglalkozzanak. Ha az eset nem amerikai állampolgárt érint, a nemzeti hírszerzési igazgató – a külügyminiszterrel, valamint a bejelentő szervezeti egység vagy ügynökség vezetőjével konzultálva – megállapítja, hogy a források és módszerek, valamint az amerikai személyi állomány védelmével összhangban lépéseket kell-e tenni az érintett külföldi kormány értesítésére ([122]).

(102) Másrészt a végrehajtó hatalmon belüli, említett felülvizsgálati mechanizmusok mellett az Egyesült Államok Kongresszusa, konkrétan a *Képviselőház és a Szenátus hírszerzési és igazságügyi bizottságai* rendelkezik felügyeleti feladatkörökkel az Egyesült Államok külföldi hírszerzési tevékenységei, többek között az amerikai jelfelderítés tekintetében. 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, előrelátható hírszerzési tevékenységet." ([123]) Továbbá „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." ([124]) E bizottságok tagjai hozzáférnek a minősített adatokhoz, valamint a hírszerzési módszerekhez és programokhoz ([125]).

(103) Az utóbbi törvények kibővítették és pontosították a beszámolási kötelezettségeket a hírszerzési szervezeti egységek, az érintett főellenőrök és a legfőbb ügyész tekintetében egyaránt. Például a FISA előírja, hogy a legfőbb ügyész „maradéktalanul tájékoztatja" a Szenátus és a Képviselőház hírszerzési és igazságügyi bizottságait a FISA bizonyos szakaszain alapuló kormányzati tevékenységekről ([126]). Kötelezi továbbá a kormányt, hogy juttassa el a kongresszusi bizottságokhoz „a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság, illetve a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróság valamennyi olyan határozatának, végzésének vagy véleményének másolatát, amely kiterjed" a FISA-rendelkezések jelentős „kiegészítésére vagy értelmezésére". Mindenekelőtt ami a FISA 702. szakasza alapján történő megfigyelést illeti, a 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 megfelelés hiányával kapcsolatos bármely esemény leírása ([127]) – kísérnek, valamint a legfőbb ügyész és a DNI külön féléves jelentése, amely dokumentálja a célzottá tételre és az adatminimalizációra vonatkozó eljárások betartását, ideértve azon eljárások követését is, amelyek célja annak biztosítása, hogy az adatgyűjtés érvényes hírszerzési célokra irányuljon ([128]). A Kongresszus számára jelentést tesznek a főellenőrök is, akik jogosultak annak értékelésére, hogy az ügynökségek betartják-e a célzottá tételre és az adatminimalizációra vonatkozó eljárásokat és a legfőbb ügyész iránymutatásait.

(104) A 2015. évi USA FREEDOM törvény értelmében az Egyesült Államok kormányának évente közölnie kell 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 ([129]). A törvény emellett további nyilvános jelentéstételt ír elő az amerikai és nem amerikai személyek tekintetében kiadott nemzetbiztonsági

([122]) PPD-28 4(a)(iv). szak.
([123]) Lásd 501(a)(1) szak. (50 U.S.C. § 413(a)(1)). Ez a rendelkezés általános követelményeket tartalmaz a nemzetbiztonság területére vonatkozó kongresszusi felügyelet tekintetében.
([124]) Lásd 501(b) szak. (50 U.S.C. § 413(b)).
([125]) Vö. 501(d) szak. (50 U.S.C. § 413(d)).
([126]) Lásd: 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Lásd: 50 U.S.C. § 1881f.
([128]) Lásd: 50 U.S.C. § 1881a(l)(1).
([129]) Lásd: 2015. évi USA FREEDOM törvény, Pub. L. 114-23. sz., 602(a) szak. Ezenfelül a 402. szakasz szerint „a nemzeti hírszerzési igazgató a legfőbb ügyésszel konzultálva elvégzi a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság, illetve a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó 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."

levelek (NSL) számáról (ugyanakkor lehetővé téve a FISA-végzések és tanúsítványok, valamint NSL-kérelmek címzettjeinek, hogy bizonyos feltételek mellett átláthatósági jelentéseket bocsássanak ki) ([130]).

(105) Harmadrészt az Egyesült Államok hatóságainak a FISA-n alapuló hírszerzési tevékenységei esetében lehetőség van a *FISA-Bíróság* (FISC) ([131]) felülvizsgálatára, és egyes esetekben az intézkedések e bíróság általi előzetes engedélyezésére. A FISC független törvényszék ([132]), amelynek határozatai megtámadhatók a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróság (FISCR) ([133]) előtt, és végső soron az Egyesült Államok Legfelsőbb Bíróságán ([134]). Előzetes engedélyezés esetén a kérelmező hatóságoknak (az FBI, az NSA, a CIA stb.) kérelemtervezetet kell benyújtaniuk az Igazságügyi Minisztérium Nemzetbiztonsági Főosztályának jogászaihoz, akik ellenőrzik azt, és szükség esetén további információkat kérnek ([135]). A legfőbb ügyésznek, a legfőbb ügyész helyettesének vagy a nemzetbiztonsági legfőbb ügyész helyettesének ([136]) a kérelem véglegesítése után jóvá kell hagynia a kérelmet. Az Igazságügyi Minisztérium ezt követően a FISC elé terjeszti a kérelmet, amely megvizsgálja azt és előzetes döntést hoz az eljárás módjáról ([137]). Amennyiben meghallgatást tartanak, a FISC jogosult tanúvallomást felvenni, többek között akár szakértői tanácsadást igénybe venni ([138]).

(106) A FISC (és a FISCR) munkáját öt személyből álló állandó szakértői testület segíti, akik nemzetbiztonsági ügyekben, valamint a polgári szabadságjogok terén rendelkeznek szaktudással ([139]). 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 ([140]). 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 ([141]).

([130]) USA FREEDOM törvény, 602(a), 603(a) szak.

([131]) Bizonyos megfigyelési típusok esetében ennek alternatívájaként az Egyesült Államok főbírája által nyilvánosan kijelölt amerikai szövetségi bíró rendelkezhet hatáskörrel a kérelmek elbírálására és a végzések kiadására.

([132]) A FISC az Egyesült Államok főbírája által kinevezett tizenegy bíróból 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: FISA 103. szak. (50 U.S.C. 1803 (a)); PCLOB, a 215. szakaszra vonatkozó jelentés, 174–187. o. A bírákat tapasztalt bírósági tisztségviselők segítik. Ők alkotják a bíróság jogi személyzetét, amely jogi elemzést készít az adatgyűjtési kérelmekről. Lásd: adatvédelmi és állampolgári jogi felügyeleti bizottság (PCLOB), a 215. szakaszra vonatkozó jelentés, 178. o.; Reggie B. Walton, a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó amerikai bíróság elnöklő bírójának levele Patrick J. Leahy-hez, az Egyesült Államok Szenátusa igazságügyi bizottságának elnökéhez (2013. július 29.) (Walton-levél) 2–3. o.

([133]) 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: FISA 103. szak. (50 U.S.C. § 1803 (b)).

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

([135]) Például a megfigyelés alatt álló személyre vonatkozó további tényszerű részletekről, a megfigyelési módszerekkel kapcsolatos technikai információkról vagy arra vonatkozó biztosítékokról, hogy hogyan használják fel és terjesztik a megszerzett információkat. Lásd: PCLOB, a 215. szakaszra vonatkozó jelentés, 177. o.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) A FISC jóváhagyhatja a kérelmet, további információt kérhet, megállapíthatja a meghallgatás szükségességét vagy jelezheti a kérelem esetleges megtagadását. A szóban forgó előzetes döntés alapján a kormány megfogalmazza végleges kérelmét. Az utóbbi lényeges változtatásokat tartalmazhat az eredeti kérelemhez képest a bíróság előzetes észrevételei alapján. Bár a FISC nagy százalékban jóváhagyja az előzetes kérelmeket, ezek jelentős hányada – a 2013. július és szeptember közötti időszakban jóváhagyott kérelmek 24 %-a – lényeges változtatásokat tartalmaz az eredeti kérelemhez képest. Lásd: PCLOB, a 215. szakaszra vonatkozó jelentés, 179. o.; Walton-levél, 3. o.

([138]) PCLOB, a 215. szakaszra vonatkozó jelentés, 179. o. 619. lábjegyzet.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Ez az új jogszabály a PCLOB arra vonatkozó ajánlásait hajtja végre, hogy adatvédelmi és polgári szabadságjogi szakértőkből álló állományt hozzanak létre, akik elláthatják az *amicus curiae* szerepét annak érdekében, hogy az adatvédelmet és polgári szabadságjogokat előmozdító jogi érveket nyújtsanak a bíróság számára. Lásd: PCLOB, a 215. szakaszra vonatkozó jelentés, 183–187. o.

([140]) 50 U.S.C. § 1803 (i)(2)(A). Az ODNI-tól származó információk szerint már sor került ilyen kijelölésekre. Lásd: Jelfelderítési reform, 2016. évi eredményjelentés.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) A FISC eltérő felügyeletet gyakorol az EU–USA adatvédelmi pajzs keretében történő adattovábbítások szempontjából leginkább fontos, a megfigyelésre vonatkozó, FISA szerint két jogi felhatalmazás tekintetében.

(108) A FISA 501. cikke alapján ([142]), amely „bármely tárgyi bizonyíték" (többek között könyvek, nyilvántartások, iratok, dokumentumok és egyéb tárgyak) beszerzését lehetővé teszi, a FISC-hez benyújtott kérelemnek tartalmaznia kell a tényekre vonatkozó nyilatkozatot, amely bemutatja, hogy alapos okkal feltételezhető, hogy a keresett tárgyi bizonyíték fontos az amerikai személyt nem érintő külföldi hírszerzési információ beszerzése vagy a nemzetközi terrorizmussal vagy titkos hírszerzési tevékenységekkel szembeni védekezés céljából folytatott, (a fenyegetésértékeléstől eltérő) engedélyezett nyomozás szempontjából. Továbbá a kérelemnek tartalmaznia kell az összegyűjtött hírszerzési információk megőrzésére és terjesztésére vonatkozó, a legfőbb ügyész által elfogadott adatminimalizációs eljárások felsorolását. ([143])

(109) Ezzel ellentétben a FISA 702. szakasza ([144]) alapján a FISC nem egyéni megfigyelési intézkedéseket, hanem megfigyelési programokat (mint a PRISM, UPSTREAM), engedélyez a legfőbb ügyész és a nemzeti hírszerzési igazgató által készített éves tanúsítványok alapján. A FISA 702. szakasza külföldi hírszerzési információk szerzése céljából lehetővé teszi olyan személyek célba vételét, akikről megalapozottan feltételezhető, hogy az Egyesült Államokon kívül tartózkodnak ([145]). Az ilyen célmegjelölést az NSA az alábbi két lépésben végzi: 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. Másodsorban, miután azonosították a szóban forgó, egyénileg megjelölt személyeket, és az NSA-n ([146]) belüli, kiterjedt felülvizsgálati mechanizmus jóváhagyta a célmegjelölést, „rádolgoznak" a célszemély által használt kommunikációs eszközöket (például e-mail címeket) azonosító, kiválasztási tényezőkre (vagyis kidolgozzák és alkalmazzák azokat) ([147]). Amint jeleztük, a FISC által jóváhagyott tanúsítványok nem tartalmaznak információkat a célba vett egyes egyének tekintetében, hanem a külföldi hírszerzési információk kategóriáit határozzák meg ([148]). Bár a FISC nem értékeli – a valószínű ok vagy bármely más standard alapján –, hogy az egyéneket megfelelően veszik-e célba a külföldi hírszerzési információk megszerzéséhez, ([149]) a bíróság felügyelete kiterjed annak a feltételnek az ellenőrzésére, hogy „az adatszerzés jelentős célja külföldi hírszerzési információk megszerzése" ([150]). Ugyanis a FISA 702. szakasza alapján az NSA kizárólag akkor gyűjtheti az Egyesült Államokon kívüli, nem amerikai személyek kommunikációját, ha megalapozottan feltételezhető, hogy az adott kommunikációs eszközt külföldi hírszerzési információk közlésére használják (pl. a nemzetközi terrorizmussal, nukleáris proliferációval vagy ellenséges kibertevékenységgel kapcsolatosan). Ennek megállapítása bírósági felülvizsgálat hatálya alá tartozik ([151]). A tanúsítványoknak a célzottá tételre és az adatminimalizációra vonatkozó eljárásokat is biztosítaniuk kell ([152]). A legfőbb ügyész és a nemzeti hírszerzés igazgatója ellenőrzi a megfelelést és az

([142]) 50 U.S.C. § 1861
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) PCLOB, a 702. szakaszra vonatkozó jelentés, 46. o.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). A PCLOB szerint ezek a kategóriák mostanáig főként a nemzetközi terrorizmusra és olyan kérdésekre vonatkoztak, mint például a tömegpusztító fegyverek megszerzése. A PCLOB 702. szakaszra vonatkozó jelentése, 25. o.
([149]) PCLOB, a 702. szakaszra vonatkozó jelentés, 27. o.
([150]) 50 U.S.C. § 1881a.
([151]) „Szabadság és biztonság a változó világban", a Hírszerzéssel és Kommunikációs Technológiákkal foglalkozó Elnöki Felülvizsgálati Csoport jelentése és ajánlásai, 2013. december 12., 152. o.
([152]) 50 U.S.C.1881a (i).

ügynökségek kötelesek bármely megfelelés hiányára utaló eseményt bejelenteni a FISC-nek ([153]) (valamint a Kongresszusnak és az Elnöki Hírszerzési Felügyeleti Testületnek), amely ennek alapján módosíthatja az engedélyezést ([154]).

(110) Továbbá a FISC-felügyelet hatékonyságának fokozása érdekében az Egyesült Államok kormánya beleegyezett azon PCLOB-ajánlás végrehajtásába, miszerint el kell juttatni a FISC-hez a 702. cikk szerinti, célszemélyek kijelölésére vonatkozó határozatok dokumentációját – a feladatköröket kijelölő dokumentumok véletlenszerű mintájával együtt –, hogy a bíróság megvizsgálhassa, miként teljesül a gyakorlatban a külföldi hírszerzési célkitűzés követelménye ([155]). Az Egyesült Államok kormánya ugyanakkor beleegyezett és intézkedéseket hozott annak érdekében, hogy felülvizsgálja az NSA célszemélyek kijelölésével kapcsolatos eljárásait annak érdekében, hogy javítsák a célszemélyek kijelölésére vonatkozó határozatokat indokoló külföldi hírszerzési információk dokumentálását ([156]).

Egyéni jogorvoslatok

(111) Az Egyesült Államok joga alapján számos lehetőség áll az uniós érintettek rendelkezésére, ha aggályaik vannak azzal kapcsolatban, hogy az Egyesült Államok hírszerzési szervezetei kezelték-e (gyűjtötték, hozzáfértek azokhoz stb.) a személyes adataikat, és amennyiben igen, betartották-e az Egyesült Államok jogában alkalmazandó korlátozásokat. Mindezek lényegében az alábbi három területre vonatkoznak: a FISA szerinti beavatkozások; a kormányzati tisztviselők jogellenes, szándékos hozzáférése a személyes adatokhoz; valamint az információkhoz való hozzájutás az információhoz való szabad hozzáférésről szóló törvény (FOIA) ([157]) alapján.

(112) Először is a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény több olyan jogorvoslatot biztosít a jogellenes elektronikus megfigyelés megtámadására, amelyek a nem amerikai személyek számára is rendelkezésre állnak ([158]). Ez 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 ([159]); hogy magánszemélyi minőségükben pénzbeli kártérítés iránti keresetet indítsanak az Egyesült Államok kormányzati tisztviselőivel szemben (hivatali visszaélés) ([160]); 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 ([161]).

(113) Másrészt az Egyesült Államok kormánya a Bizottság számára hivatkozott számos további jogorvoslati lehetőségre, amelyeket az uniós érintettek felhasználhatnak ahhoz, hogy jogorvoslatot igényeljenek a kormányzati tisztviselőkkel szemben a személyes adatokhoz való jogellenes kormányzati hozzáférés vagy azok jogellenes felhasználása

([153]) A FISC eljárási szabályzatának 13(b) szabálya előírja, hogy a kormánynak haladéktalanul írásbeli értesítést kell adni a Bíróság számára annak felfedezését követően, hogy a Bíróság által kiadott engedélyt vagy jóváhagyást olyan módon hajtották végre, hogy ez nem felel meg a Bíróság engedélyének vagy jóváhagyásának vagy az alkalmazandó jognak. Előírja továbbá, hogy a kormánynak írásban értesítenie kell a FISC-et a megfelelés hiánya szempontjából releváns tényekről és körülményekről. Miután az összes lényeges tény ismertté vált és valamennyi engedély nélküli adatgyűjteményt megsemmisítettek, a kormány általában benyújtja a 13(a) szabály szerinti végleges értesítést. Lásd: Walton-levél, 10. o.

([154]) 50 U.S.C. § 1881 (l). Lásd még PCLOB, a 702. szakaszra vonatkozó jelentés, 66–76. o. NSA CLPO, A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakaszának az NSA általi végrehajtása, 2014.4.16. A végrehajtó hatalmi ágon belüli belső és külső felügyelet hatálya egyaránt kiterjed a FISA 702. szakaszán alapuló, hírszerzési célú személyesadat-gyűjtésre. A belső felügyelet többek között felöleli azokat a megfelelési programokat, amelyek célja a célzottá tételre és adatminimalizációra vonatkozó eljárások betartásának értékelése és felügyelete; a megfelelés hiányára utaló eseményekre vonatkozó belső és külső jelentéstétel az ODNI, az Igazságügyi Minisztérium, a Kongresszus és a FISC számára; valamint az ugyanazon szerveknek küldött éves felülvizsgálatok. Ami a külső felügyeletet illeti, az főként az ODNI, az Igazságügyi Minisztérium és a főellenőrök által a célzottá tételre és az adatminimalizációra vonatkozóan végzett felügyeletekből állnak, e szervek pedig a Kongresszusnak és a FISC-nek számolnak be, többek között a megfelelés hiányára utaló eseményekről. A megfeleléssel kapcsolatos jelentős eseményeket haladéktalanul jelenteni kell a FISC-nek, a többiről a negyedéves jelentésben kell beszámolni. Lásd: PCLOB, a 702. szakaszra vonatkozó jelentés, 66-77. o.

([155]) PCLOB, Ajánlás-értékelési jelentés, 2015. január 29., 20. o.

([156]) PCLOB, Ajánlás-értékelési jelentés, 2015. január 29., 16. o.

([157]) A minősített adatokkal kapcsolatos eljárásokról szóló törvény 10. szakasza ezenfelül előírja, hogy bármely olyan büntetőeljárás során, amelyben az Egyesült Államoknak meg kell állapítania, hogy az anyag minősített adatnak minősül (pl. mivel nemzetbiztonsági okokból védelmet igényel a jogosulatlan nyilvánosságra hozatallal szemben), az Egyesült Államok értesíti a vádlottat, hogy az anyagok mely részei tekintetében várható indokoltan minősített adatokat tartalmazó bűncselekményi elem megállapítása.

([158]) Lásd az alábbiak tekintetében az ODNI nyilatkozatait (VI. melléklet), 16. o.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

miatt, ideértve az elérni kívánt nemzetbiztonsági célokat (vagyis a számítógépes csalásról és visszaélésről szóló törvény ([162]), az elektronikus kommunikáció adatvédelméről szóló törvény ([163]), valamint a pénzügyi adatok védelméről szóló törvény ([164])). A 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 ([165]). Általánosabb jogorvoslati lehetőséget kínál az államigazgatási eljárásról szóló törvény (5 U.S. C. § 702), 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. 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" ([166]).

(114) Az Egyesült Államok kormánya végezetül rámutatott, hogy a FOIA olyan eszköz, amely alapján nem amerikai személyek hozzáférést igényelhetnek a meglévő szövetségi hivatali nyilvántartásokhoz, többek között azokhoz, amelyek egyének személyes adatait tartalmazzák ([167]). Hangsúlyának köszönhetően a FOIA nem nyújt lehetőséget egyéni jogorvoslatra önmagában véve a személyes adatokba való beavatkozással szemben, bár elvben lehetőséget biztosíthat az egyének számára, hogy hozzáférést kapjanak a nemzeti hírszerző ügynökségek birtokában lévő, releváns adatokhoz. Még e tekintetben is korlátozottnak látszanak a lehetőségek, ugyanis az ügynökségek visszatarthatnak olyan információkat, amelyek a felsorolt kivételek közé tartoznak, többek között megtagadhatják a minősített nemzetbiztonsági adatokba és a bűnügyi nyomozásokkal kapcsolatos információkba való betekintést ([168]). Mindemellett, ha a nemzeti hírszerző ügynökségek ilyen kivételeket alkalmaznak, az egyének közigazgatási és bírósági jogorvoslatot igényelve egyaránt megtámadhatják ezt.

(115) Jóllehet az egyéneknek – köztük az uniós érintetteknek – tehát számos jogorvoslati lehetőség áll a rendelkezésére, ha nemzetbiztonsági célú, jogellenes (elektronikus) megfigyelést folytatnak velük szemben, az is egyértelmű, hogy e jogorvoslati lehetőségek nem terjednek ki legalább néhány olyan jogalapra (pl. az 12333. elnöki rendeletre), amelyet az Egyesült Államok hírszerzési hatóságai igénybe vehetnek. Ezenfelül, még ha elvben léteznek is bírósági jogorvoslati lehetőségek a nem amerikai személyek számára, például a FISA alapján végzett megfigyelés esetében, a rendelkezésre álló kereseti jogcímek korlátozottak ([169]), és az egyének (köztük az amerikai személyek) által indított kereseteket elfogadhatatlannak nyilvánítják, amennyiben nem tudnak olyan „perképességet" ([170]) igazolni, amely korlátozza a rendes bíróságokhoz fordulást ([171]).

(116) Annak érdekében, hogy további jogorvoslati lehetőséget biztosítson valamennyi uniós érintett számára, az Egyesült Államok kormánya úgy döntött, hogy új ombudsmani mechanizmust hoz létre, az Egyesült Államok külügyminiszterének a Bizottsághoz címzett, e határozat III. mellékletében foglalt levélben kifejtettek szerint. Ez a mechanizmus lényegesen túllép az eredeti koncepción, amely arra épül, hogy a PPD-28 alapján magas szintű koordinátort (miniszterhelyettesi szinten) neveznek ki a Külügyminisztériumban a külföldi kormányok kapcsolattartó pontjaként, akinél azok felvethetik az Egyesült Államok jelfelderítési tevékenységeivel kapcsolatos aggályaikat.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) 12 U.S.C. § 3417.
([165]) ODNI-nyilatkozatok (VI. melléklet), 17. o.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Hasonló törvények vannak hatályban tagállami szinten.
([168]) 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).
([169]) Lásd az ODNI nyilatkozatait (VI. melléklet), 16. o. A szolgáltatott magyarázatok szerint a rendelkezésre álló kereseti jogcímek megkövetelik a *kár* megvalósulását (18 U.S.C. § 2712; 50 U.S.C. § 1810) vagy annak igazolását, hogy *az Egyesült Államokban zajló bírósági vagy közigazgatási eljárások folyamán a kormány fel kívánja használni vagy nyilvánosságra szándékozik hozni azokat az információkat*, amelyeket az érintett személy elektronikus megfigyelésével szereztek vagy amelyek abból származnak (50 U.S.C. § 1806). A Bíróság azonban ismételten hangsúlyozta, hogy a magánélet tiszteletben tartásához való alapvető jogba történő beavatkozás fennállásának megállapítása érdekében kevésbé fontos, hogy az érintett személyeknek ez a beavatkozás okozott-e esetleges kellemetlenséget vagy sem. Lásd:*Schrems-ügy,* 89. pont, a további hivatkozásokkal.
([170]) Ez az elfogadhatósági kritérium láthatólag az Egyesült Államok Alkotmányának III. cikkébe foglalt, „ügyek és jogviták" követelményéből ered.
([171]) Lásd: *Clapper kontra Amnesty Int'l USA* ügy, 133 S.Ct. 1138, 1144 (2013). Ami a nemzetbiztonsági levelek (NSL) alkalmazását illeti, USA FREEDOM törvény (502(f)–503. szakasz) úgy rendelkezik, hogy rendszeresen felül kell vizsgálni a közzététel megtagadására vonatkozó követelményeket, továbbá az NSL *címzettjeit* értesíteni kell arról, ha nem állnak fenn a közlés megtagadásának követelményét alátámasztó tények (lásd az ODNI nyilatkozatait (VI. melléklet), 13. o.). Ez azonban nem biztosítja, hogy az uniós érintetteket tájékoztassák arról, hogy nyomozást folytattak velük szemben.

(117) Mindenekelőtt az Egyesült Államok kormányának kötelezettségvállalása szerint az ombudsmani mechanizmus biztosítani fogja, hogy az egyéni panaszokat megfelelően kivizsgálják és kezeljék, valamint hogy az egyének független megerősítést kapjanak arról, hogy betartják az Egyesült Államok törvényeit, vagy e törvények megsértése esetén orvosolják a megfelelés hiányát ([172]). A mechanizmus felöleli az „adatvédelmi pajzs ombudsmanját", vagyis a miniszterhelyettest és a további személyzetet, valamint egyéb, a hírszerzés különböző szervezeti egységeinek felügyeletére hatáskörrel rendelkező olyan szervekre, amelyek együttműködését igénybe veheti az adatvédelmi pajzs ombudsmanja a panaszok kezelése során. Először is, amennyiben egy egyéni kérelem a megfigyelésnek az Egyesült Államok jogával való összeegyeztethetőségére vonatkozik, az adatvédelmi pajzs ombudsmanja nyomozati jogkörrel rendelkező független szervekre (például a főellenőrökre vagy a PCLOB-ra) támaszkodhat majd. Az egyes esetekben a külügyminiszter gondoskodik arról, hogy az ombudsman rendelkezésére álljanak az eszközök ahhoz, hogy az egyéni kérelemre adott válasza az összes szükséges információ alapuljon.

(118) Az ombudsmani mechanizmus összetett struktúrája révén garantálja a független felügyeletet és az egyéni jogorvoslatot. Továbbá a többi felügyeleti szervvel folytatott együttműködés biztosítja a szükséges szakértelemhez való hozzájutást. Végezetül a mechanizmus, amely kötelezővé teszi az adatvédelmi pajzs ombudsmanja számára a megfelelés megerősítését vagy bármely megfelelési hiány orvoslását, az Egyesült Államok egész kormányzatának azon elkötelezettségét tükrözi, hogy foglalkozzanak az uniós egyénektől érkező panaszokkal és rendezzék azokat.

(119) Először is, egy tisztán kormányközi mechanizmustól eltérően az adatvédelmi pajzs ombudsmanja átveszi és megválaszolja az egyéni panaszokat. E panaszok elküldetők a nemzeti biztonsági szolgálatok és/vagy a hatóságok általi személyesadat-kezelés felügyeletére hatáskörrel rendelkező tagállami felügyeleti hatóságoknak, amelyek benyújtják azokat egy központosított uniós szervnek, amely eljuttatja a panaszokat az adatvédelmi pajzs ombudsmanjának ([173]). Ez valóban hasznos lesz az uniós egyéneknek, akik az „otthonukhoz közeli" nemzeti hatóságokhoz fordulhatnak a saját nyelvükön. E hatóság feladat lesz, hogy támogatást nyújtson az egyéneknek ahhoz, hogy olyan kérelmet nyújtsanak be az adatvédelmi pajzs ombudsmanjának, amely tartalmazza az alapvető információkat és így „hiánytalannak" tekinthető. Az egyéneknek nem kell bizonyítaniuk, hogy az Egyesült Államok kormánya jelfelderítési tevékenységek keretében valóban hozzáfért a személyes adataikhoz.

(120) Másrészt az Egyesült Államok kormánya annak biztosítására kötelezi magát, hogy az adatvédelmi pajzs ombudsmanja feladatainak ellátása során számíthat az Egyesült Államok jogában meglévő más felügyeleti és megfelelőség-felülvizsgálati mechanizmusok együttműködésére. Ez időnként a nemzeti hírszerzési hatóságok bevonásával jár, különösen amikor a kérelem az információkhoz való szabad hozzáférésről szóló törvény szerinti dokumentumok egyikéhez való hozzáférés igényléseként értelmezhető. Más esetekben, különösen, ha a kérelem a megfigyelésnek az Egyesült Államok jogával való összeegyeztethetőségére vonatkozik, ez az együttműködés kiterjedhet az alapos vizsgálatok lefolytatására (különösen az összes releváns dokumentumhoz való hozzáférés, valamint az információ-igénylési és nyilatkozati jogkör révén) és a megfelelés hiányának kezelésére feladat- és hatáskörrel rendelkező független felügyeleti szervek (pl. a főellenőrök) bevonására ([174]). Továbbá az adatvédelmi pajzs ombudsmanja a PCLOB elé utalhatja az ügyeket mérlegelés céljából ([175]). Ha az említett felügyeleti szervek egyike megállapította megfelelés hiányát, a hírszerzés érintett szervezetének (pl. hírszerző ügynökségnek) orvosolnia kell a megfelelés hiányát, mivel csak ez teszi lehetővé, hogy az ombudsman „pozitív" választ adjon (vagyis hogy minden megfelelési problémát orvosoltak) annak a személynek, akivel szemben az Egyesült Államok

([172]) Abban az esetben, ha a panaszos hozzáférést szeretne az Egyesült Államok hatóságainak birtokában lévő dokumentumokhoz, az információkhoz való szabad hozzáférésről szóló törvényben meghatározott szabályok és eljárások alkalmazandók. Ez arra a lehetőségre is kiterjed, hogy a FOIA-ban meghatározott feltételek szerint bírósági jogorvoslatot igényeljenek (független felügyelet helyett) abban az esetben, ha a kérelmet elutasították.

([173]) Az ombudsmani mechanizmus (III. melléklet) 4(f) szakasza szerint az adatvédelmi pajzs ombudsmanja közvetlenül kommunikál majd az uniós egyén panaszkezelő szervével, amely pedig a kérelmet benyújtó egyénnel való kommunikációért felel. Ha a közvetlen kommunikáció részét képezi azoknak a „mögöttes eljárásoknak", amelyek biztosíthatják a kért intézkedést (pl. FOIA hozzáférési kérelem, lásd az 5. szakaszt), e kommunikáció a vonatkozó eljárásoknak megfelelően történik.

([174]) Lásd: ombudsmani mechanizmus (III. melléklet), 2(a) szak. Lásd továbbá a 0-0 preambulumbekezdést.

([175]) Lásd: ombudsmani mechanizmus (III. melléklet), 2(c) szak. Az Egyesült Államok kormánya által adott magyarázatok szerint a PCLOB folyamatosan felülvizsgálja majd a terrorelhárításért felelős amerikai hatóságok politikáit és eljárásait, valamint azok végrehajtását annak megállapítása érdekében, hogy azok intézkedései „megfelelően garantálják az adatvédelmet és a polgári szabadságjogok védelmét, és összhangban állnak az adatvédelemre és a polgári szabadságjogok védelmére irányadó jogszabályokkal, szabályzatokkal és politikákkal". A PCLOB továbbá „adatvédelmi tisztségviselőktől és polgári szabadságjogi tisztségviselőktől jelentéseket és más információkat kap, azokat felülvizsgálja, és adott esetben ajánlásokat tesz a tevékenységeik tekintetében."

kormánya kötelezettséget vállalt. Ezenfelül az adatvédelmi pajzs ombudsmanja az együttműködés keretében tájékoztatást fog kapni a vizsgálat eredményéről, valamint az ombudsman eszközökkel fog rendelkezni ahhoz, hogy megkapja a válasza elkészítéséhez szükséges valamennyi információt.

(121) Végezetül az adatvédelmi pajzs ombudsmanja független az Egyesült Államok hírszerzésétől, és így nem kaphat attól utasításokat ([176]). Ez különösen fontos, mivel az ombudsmannak kell megerősítenie, hogy i. a panaszt megfelelően kivizsgálták, valamint ii. betartották a vonatkozó amerikai jogot – többek között különösen a VI. mellékletben ismertetett korlátozásokat és biztosítékokat –, vagy a megfelelés hiánya esetén orvosolták ezt a jogsértést. Annak érdekében, hogy független megerősítést tudjon nyújtani, az adatvédelmi pajzs ombudsmanjának meg kell kapnia a vizsgálattal kapcsolatos, szükséges információkat annak vizsgálata céljából, hogy pontos választ adtak-e a panaszra. Ezenfelül a külügyminiszter vállalta, hogy a miniszterhelyettes pártatlanul, és a nyújtandó válasz megváltoztatására alkalmas, helytelen befolyásolásától mentesen látja majd el feladatait az adatvédelmi pajzs ombudsmanjaként.

(122) Ez a mechanizmus összességében véve biztosítja az egyéni panaszok alapos kivizsgálását és rendezését, valamint – legalábbis a megfigyelés területén – a szükséges szakértelemmel és vizsgálati hatáskörrel rendelkező független felügyeleti szervek, továbbá egy ombudsman bevonását, aki helytelen befolyásolástól, különösen politikai befolyástól mentesen láthatja el a feladatait. Továbbá az egyének anélkül terjeszthetnek elő panaszokat, hogy igazolniuk kellene, vagy akár arra utaló jeleket kellene bemutatniuk, hogy megfigyelést folytattak velük szemben ([177]). Az említett jellemzőkre tekintettel a Bizottság megbizonyosodott arról, hogy megfelelő és hatékony garanciák léteznek a visszaéléssel szemben.

(123) Mindezek alapján a Bizottság arra a következtetésre jutott, hogy az Egyesült Államok hatékony jogi védelmet nyújt hírszerző hatóságainak azon személyek alapvető jogaiba történő beavatkozásaival szemben, akiknek az adatait az EU–USA adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbítják.

(124) A Bizottság ezzel kapcsolatosan tudomásul veszi a Bíróság *Schrems-ügyben* hozott ítéletét, amely szerint „az olyan szabályozás, amely nem biztosít a jogalany számára semmilyen jogorvoslati lehetőséget abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse, nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét, amelyet a Charta 47. cikke mond ki." ([178]) A Bizottság értékelése megerősítette, hogy az Egyesült Államokban biztosítanak ilyen jogorvoslati lehetőségeket, többek között az ombudsmani mechanizmus bevezetésével. Az ombudsmani mechanizmus vizsgálati hatáskörrel rendelkező független felügyeletet nyújt. E mechanizmus hatékonyságát ismételten meg fogjuk vizsgálni annak keretében, hogy a Bizottság folyamatosan figyelemmel kíséri az adatvédelmi pajzsot, többek között az ombudsmant is érintő éves közös felülvizsgálat révén.

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

(125) Ami az EU-USA adatvédelmi pajzs alapján továbbított személyes adatokba való bűnüldözési célú beavatkozást illeti, az Egyesült Államok kormánya (az Igazságügyi Minisztériumon keresztül) biztosítékot nyújtott azon alkalmazandó korlátozásokra és biztosítékokra vonatkozóan, amelyek tekintetében a Bizottság vizsgálata igazolja a megfelelő szintű védelmet.

([176]) Lásd: *Roman Zakharov kontra Oroszország* ügy, 2015. december 4-i ítélet, (nagytanács), kereset sz. 47143/06., 275. pont („jóllehet főszabály szerint kívánatos, hogy bíróságot bízzanak meg a felügyeleti ellenőrzéssel, a nem bírósági szervek felügyelete összeegyeztethetőnek tekinthető az Egyezménnyel, amennyiben a felügyeleti szerv független a megfigyelést végző hatóságoktól, valamint elegendő és hatékony felügyeleti jogkörrel rendelkezik").

([177]) Lásd: *Kennedy kontra az Egyesült Királyság* ügy, 2010. május 18-i ítélet, Kereset sz. 26839/05., 167. pont.

([178]) *Schrems-ügy*, 95. pont. Amint az ítélet 91. és 96. pontja egyértelművé teszi, a 95. pont az uniós jogrendszerben garantált védelem szintjére vonatkozik, amellyel a harmadik ország védelmi szintjének „lényegében azonosnak" kell lennie. Az ítélet 73. és 74. pontja értelmében ez nem teszi szükségessé, hogy a védelem szintjének vagy a harmadik országban alkalmazott eszközöknek megegyezőnek kell lenniük, noha az alkalmazandó eszközöknek a gyakorlatban hatékonynak kell bizonyulniuk.

(126) E tájékoztatás szerint az Egyesült Államok Alkotmányának negyedik módosítása ([179]) értelmében a bűnüldöző hatóságok általi kutatáshoz és lefoglaláshoz főszabály szerint ([180])„valószínű indokon" alapuló bírósági parancs szükséges. Néhány konkrétan meghatározott és kivételes esetben, amikor a parancs követelménye nem alkalmazandó ([181]), a bűnüldözés az „ésszerűségi" vizsgálat alá tartozik ([182]). Azt, hogy egy kutatás vagy lefoglalás ésszerű-e „egyrészt annak értékelése határozza meg, hogy milyen mértékben avatkozik be az egyén magánéletébe, másrészt pedig, hogy milyen mértékben szükséges a törvényes kormányzati érdekek elősegítéséhez." ([183]) Általánosabban, a negyedik alkotmánykiegészítés garantálja a magánéletet és a méltóságot, valamint védelmet nyújt a kormányzati tisztségviselők önkényes és tolakodó cselekményeivel szemben ([184]). E fogalmak felölelik az uniós jog szerinti szükségesség és arányosság elképzelését. Ha a bűnüldözésnek már nincs szüksége arra, hogy bizonyítékként használja fel a lefoglalt tárgyakat, vissza kell azokat szolgáltatnia ([185]).

(127) Bár a negyedik alkotmánykiegészítésbe foglalt jog nem terjed ki azokra a nem amerikai személyekre, akik nem az Egyesült Államokban laknak, az utóbbiak mindazonáltal közvetetten hozzájutnak annak védelmi normáihoz, mivel a személyes adatok amerikai vállalatok birtokában vannak, és ennek következtében a bűnüldöző hatóságoknak mindenesetre bírósági felhatalmazást kell igényelniük (vagy legalább tiszteletben kell tartaniuk az ésszerűség követelményét) ([186]). További védelmet biztosítanak a különleges állami hatóságok és az Igazságügyi Minisztérium iránymutatásai, amelyek a szükségességgel és az arányossággal azonos okokból korlátozzák az adatokhoz való bűnüldözési célú hozzáférést (pl. előírva, hogy az FBI a rendelkezésére álló, legkisebb beavatkozást lehetővé tevő nyomozati módszereket alkalmazza, szem előtt tartva azoknak a magánéletre és a polgári szabadságjogokra gyakorolt hatását) ([187]). Az Egyesült Államok kormánya által tett nyilatkozatok szerint, azonos vagy magasabb szintű védelmi normák vonatkoznak a állami szintű bűnügyi nyomozásokra (a tagállamok joga alapján végzett nyomozások tekintetében) ([188]).

(128) Jóllehet a bíróság vagy vádesküdtszék (a bíróság bírákból vagy szövetségi bírákból álló nyomozati ága) általi előzetes bírósági engedély nem minden esetben szükséges ([189]), a bizonyítási cselekményben való közreműködésre kötelező közigazgatási határozatok konkrét ügyekre korlátozódnak, és független bírósági felülvizsgálat alá tartoznak, legalábbis, amennyiben a kormány bírósági jogérvényesítést igényel ([190]).

([179]) A negyedik alkotmánykiegészítés szerint: „a népnek az a joga, hogy személye, háza, iratai és ingóságai tekintetében indokolatlan kutatások és letartóztatások ellen védve legyen, nem sérthető meg és elfogató parancsok nem adhatók ki, csak valószínű, eskü vagy ünnepélyes fogadalom által támogatott indokokból és részletesen leírva a kutatandó helyet és a letartóztatandó személyt vagy lefoglalandó tárgyat." Csak a (szövetségi) bírók adhatnak ki kutatási parancsot. Az elektronikusan tárolt adatok másolására vonatkozó szövetségi parancsokra vonatkozó további szabályokat a szövetségi büntetőeljárási szabályok 41. szabálya állapítja meg.

([180]) A parancs nélküli kutatásokra a Legfelsőbb Bíróság ismételten „kivételesként" utalt. Lásd pl. *Johnson kontra Egyesült Államok* ügy, 333 U. S. 10, 14 (1948); *McDonald kontra Egyesült Államok* ügy, 335 U.S. 451, 453 (1948); *Camara kontra városi bíróság* ügy, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp. kontra Egyesült Államok* ügy, 429 U.S. 338, 352-53, 355 (1977). A Legfelsőbb Bíróság szintén rendszeresen hangsúlyozta, hogy „e területnek az a legalapvetőbb alkotmányos szabálya, hogy a bírósági eljáráson kívül, bíró vagy szövetségi bíró előzetes jóváhagyása nélkül végzett kutatások a negyedik alkotmánykiegészítés – alapján – néhány konkrétan meghatározott és jól körülhatárolt kivételtől eltekintve – önmagában véve ésszerűtlenek". Lásd pl. *Coolidge kontra New Hampshire* ügy, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp. kontra Egyesült Államok* ügy, 429 U.S. 338, 352-53, 358 (1977).

([181]) *City of Ontario, Cal. kontra Quon* ügy, 130 S. Ct. 2619, 2630 (2010).

([182]) PCLOB, a 215. szakaszra vonatkozó jelentés, 107. o., amely utal a *Maryland kontra King* ügyre, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB, a 215. szakaszra vonatkozó jelentés, 107. o., amely utal a *Samson kontra California* ügyre, 547 U.S. 843, 848 (2006).

([184]) *City of Ontario, Cal. kontra Quon* ügy, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Lásd pl. *Egyesült Államok kontra Wilson* ügy, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Vö. *Roman Zakharov kontra Oroszország* ügy, 2015.12.4.-i ítélet (nagytanács), kereset sz.: 47143/06., 269. pont, amely szerint „az a követelmény, hogy adatszerzési engedélyt kell bemutatni a kommunikációs szolgáltatónak, mielőtt hozzáférést biztosítanának az adott személy kommunikációjához, a bűnüldöző hatóságok visszaélésével szembeni egyik legfontosabb biztosíték, amely biztosítja, hogy minden adatszerzés esetén beszerezzék a megfelelő engedélyt."

([187]) Az Igazságügyi Minisztérium nyilatkozatai (VII. melléklet), 4. o. további hivatkozásokkal.

([188]) Az Igazságügyi Minisztérium nyilatkozatai (VII. melléklet), 2. lábjegyzet.

([189]) A Bizottsághoz beérkezett információk szerint, és eltekintve azoktól a területektől, amelyek valószínűleg nem relevánsak az EU–USA adatvédelmi pajzs alapján végzett adattovábbítások szempontjából (pl. az egészségügyi ellátási csalások, gyermekbántalmazás vagy ellenőrzött anyagok ügyében folytatott nyomozások), ez főként az elektronikus kommunikáció adatvédelméről szóló törvény hatálya alá tartozó bizonyos hatóságokat érint, konkrétan az alapvető előfizetői, munkamenet- és számlázási információk (18 U.S.C. § 2703(c) (1), (2), pl. cím, a szolgáltatás típusa/hossza) és a 180 napnál régebbi e-mailek tartamára irányuló igénylések (18 U.S.C. § 2703(a), (b)) esetében. Az utóbbi esetben azonban értesíteni kell az érintett egyént, akinek így lehetősége van arra, hogy bíróság előtt megtámadja az igénylést. Lásd továbbá az Igazságügyi Minisztérium áttekintését, Számítógépek átkutatása és lefoglalása és elektronikus bizonyítékok beszerzése a bűnügyi nyomozások során, 3. fejezet: A tárolt kommunikációról szóló törvény, 115–138. o.

([190]) Az Egyesült Államok kormányának nyilatkozatai szerint a bizonyítási cselekményben való közreműködésre kötelező közigazgatási határozatok címzettjei megtámadhatják azokat a bíróságon azzal az indokkal, hogy azok nem ésszerűek, vagy túlzott a hatókörük, elnyomóak vagy terhesek. Lásd az Igazságügyi Minisztérium nyilatkozatait (VII. melléklet), 2. o.

(129) Ugyanez vonatkozik a közérdekű célokra használt közigazgatási idézésekre. Ezenfelül az Egyesült Államok Kormányának nyilatkozatai szerint hasonló érdemi korlátozások vonatkoznak arra, hogy az ügynökségek kizárólag azokhoz az adatokhoz igényelhetnek hozzáférést, amelyek lényegesek a felelősségi- és hatáskörükbe tartozó ügyek szempontjából, valamint tiszteletben kell tartaniuk az ésszerűség normáját.

(130) Továbbá az amerikai jog számos bírósági jogorvoslati lehetőséget biztosít az egyéneknek a hatóságokkal vagy azok tisztviselőivel szemben, amennyiben ezek a hatóságok személyes adatokat kezelnek. 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.

(131) Általában véve az államigazgatási eljárásról szóló törvény bírósági felülvizsgálatra vonatkozó rendelkezései szerint ([191])„egy hivatal tevékenysége miatt jogellenesen kárt szenvedő, vagy egy hivatal tevékenysége révén hátrányos helyzetbe kerülő vagy sérelmet szenvedő személyek” jogosultak bírósági jogorvoslatot ([192]) igényelni. 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” ([193]).

(132) Közelebbről az elektronikus kommunikáció adatvédelméről szóló törvény II. címe ([194]) 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 ([195]). 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.

(133) Továbbá az információkhoz való szabad hozzáférésről szóló törvény (FOIA, 5 U.S.C. § 552) értelmében mindenkinek joga van betekintést nyerni a szövetségi ügynökségek nyilvántartásaiba, valamint a közigazgatási jogorvoslatok kimerítése esetén e jogot a bíróságon érvényesíteni, kivéve amennyiben valamely mentesség vagy különleges bűnüldözési kizárás védelmet nyújt az ilyen nyilvántartásoknak a nyilvánosságra hozatalával szemben ([196]).

([191]) 5 U.S.C. § 702.

([192]) 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.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701-2712.

([195]) 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.

([196]) Az említett kizárások azonban korlátozottak. Például a 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 ésszerűen 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)).

(134) Ezenfelül több más törvény biztosítja az egyéneknek azt a jogot, hogy keresetet indítsanak az Egyesült Államok hatósága vagy tisztviselője ellen a személyes adataik kezelése tekintetében; így például a lehallgatásról szóló törvény ([197]), a számítógépes csalásról és visszaélésről szóló törvény ([198]), a kártérítési követelésekről szóló szövetségi törvény ([199]), a pénzügyi adatok védelméről szóló törvény ([200]), valamint a méltányos hitelminősítésről szóló törvény ([201]).

(135) A Bizottság ezért arra a következtetésre jutott, hogy az Egyesült Államokban léteznek olyan szabályok, amelyeknek az a célja, hogy a szóban forgó törvényes cél eléréséhez feltétlenül szükséges mértékűre korlátozzanak bármely bűnüldözési ([202]) vagy egyéb közérdekű célokból történő beavatkozást azon személyek alapvető jogaiba, akiknek a személyes adatait az EU–USA adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbítják, valamint hatékony jogvédelmet biztosítsanak az ilyen beavatkozással szemben.

4. MEGFELELŐ SZINTŰ VÉDELEM AZ EU–USA ADATVÉDELMI PAJZS ALAPJÁN

(136) A fenti megállapítások alapján a Bizottság úgy ítéli meg, hogy az Egyesült Államok megfelelő szintű védelmet biztosít az EU–USA adatvédelmi pajzs keretében az Unióból az öntanúsított egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében.

(137) A Bizottság mindenekelőtt úgy véli, hogy az Egyesült Államok Kereskedelmi Minisztériuma által kibocsátott elvek összességében véve a személyes adatok védelmének olyan szintjét biztosítják, amely lényegében azonos a 95/46/EK irányelvben meghatározott alapelvek révén garantálttal.

(138) Továbbá az elvek tényleges alkalmazását szavatolják az átláthatósági kötelezettségek, valamint az, hogy az adatvédelmi pajzsot az Egyesült Államok Kereskedelmi Minisztériuma igazgatja.

(139) A Bizottság ezenfelül úgy ítéli meg, hogy az adatvédelmi pajzs által előírt felügyeleti és jogorvoslati mechanizmusok összességében véve lehetővé teszik, hogy a gyakorlatban azonosítsák és szankcionálják azt, ha az adatvédelmi pajzsban részt vevő szervezetek megsértik az elveket, továbbá hogy jogorvoslatok biztosítsanak az érintetteknek ahhoz, hogy betekinthessenek a rájuk vonatkozó személyes adatokba, és esetleg helyesbítsék vagy töröljék ezeket az adatokat.

(140) Végezetül az Egyesült Államok jogrendszerével kapcsolatban rendelkezésre álló információk – többek között az Egyesült Államok kormányának nyilatkozatai és kötelezettségvállalásai – alapján a Bizottság úgy ítéli meg, hogy az Egyesült Államok hatóságainak nemzetbiztonsági, bűnüldözési vagy egyéb közérdekű célokból azon személyek alapvető jogaiba történő beavatkozása, akiknek az adatait az adatvédelmi pajzs keretében az Unióból az Egyesült Államokba továbbították, valamint ebből következően az öntanúsított vállalatokra az elvek elfogadása tekintetében meghatározott korlátozások a szóban forgó törvényes cél eléréséhez feltétlenül szükséges mértékűre fognak korlátozódni, továbbá hogy hatékony jogvédelem létezik az ilyen beavatkozással szemben.

([197]) 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 címekre vonatkozó és egyéb 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).

([198]) 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.

([199]) 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."

([200]) 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.

([201]) 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).

([202]) A Bíróság elismerte, hogy a bűnüldözés jogos politikai célkitűzés. Lásd a C-293/12. és C-594/12. sz., *Digital Rights Ireland és társai* egyesített ügyekben hozott ítélet (EU:C:2014:238) 42. pontját. Lásd továbbá az EJEE 8. cikkének (2) bekezdését, valamint az Emberi Jogok Európai Bírósága *Weber és Saravia kontra Németország* ügyben (kereset sz.: 54934/00.) hozott ítéletének 104. pontját.

(141) A Bizottság arra a következtetésre jutott, hogy ez megfelel a 95/46/EK irányelv 25. cikkébe foglalt, az Európai Unió Alapjogi Chartája alapján értelmezett normáknak, a Bíróság által különösen a *Schrems-ügyben* hozott ítéletben kifejtettek szerint.

5. AZ ADATVÉDELMI HATÓSÁGOK FELLÉPÉSE ÉS A BIZOTTSÁGNAK NYÚJTOTT TÁJÉKOZTATÁS

(142) A *Schrems-ügyben* hozott ítéletben a Bíróság egyértelművé tette, hogy a Bizottság nem rendelkezik hatáskörrel arra, hogy korlátozza az adatvédelmi hatóságokat a 95/46/EK irányelv 28. cikkéből eredően megillető jogkört (ideértve az adattovábbítás felfüggesztésére vonatkozó jogkört), amennyiben egy adott személy e rendelkezés alapján indított keresetében kétségbe vonja a Bizottság megfelelőségi határozatának összeegyeztethetőségét a magánélethez és az adatvédelemhez fűződő alapvető jog védelmével ([203]).

(143) Az adatvédelmi pajzs működésének hatékony figyelemmel kísérése érdekében a tagállamoknak tájékoztatniuk a Bizottságot az adatvédelmi hatóságok által hozott releváns intézkedésekről.

(144) A Bíróság úgy ítélte meg továbbá, hogy a 95/46/EK irányelv 25. cikke (6) bekezdésének második albekezdése szerint a tagállamok és szerveik kötelesek megtenni az ahhoz szükséges intézkedéseket, hogy teljesítsék az uniós intézmények jogi aktusait, mivel az utóbbiak főszabály szerint 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. Következtetésképpen a Bizottságnak a 95/46/EK irányelv 25. cikkének (6) bekezdése alapján elfogadott megfelelőségi határozata kötelező a címzett tagállamok valamennyi szervére, így a független felügyeleti hatóságokra nézve is ([204]). Ha e hatósághoz olyan panasz érkezik, amely kétségbe vonja a Bizottság megfelelőségi határozatának a magánélethez és az adatvédelemhez fűződő alapvető jog védelmével való összhangját, valamint úgy véli, hogy a kifogások megalapozottak, a nemzeti jognak jogorvoslatot kell biztosítania ahhoz, hogy e kifogásokat a nemzeti bíróság elé terjesszék, amelynek kétség esetén fel kell függesztenie az eljárást és előzetes döntéshozatal iránti kérelemmel kell a Bírósághoz fordulnia ([205]).

6. A MEGFELELŐSÉGI MEGÁLLAPÍTÁS IDŐSZAKOS FELÜLVIZSGÁLATA

(145) Tekintettel arra, hogy az Egyesült Államok jogrendszerében biztosított védelem szintje megváltozhat, a Bizottság e határozatának elfogadását követően időszakonként ellenőrzi, hogy az EU–USA adatvédelmi pajzs keretében az Egyesült Államok által biztosított védelem megfelelő szintjére vonatkozó megállapítás továbbra is ténybelileg és jogilag igazolt-e. Ezen vizsgálat mindenképpen szükséges azokban az esetekben, amikor a Bizottság által kapott bármely információ alapján indokolt kétségek merülhetnek fel e tekintetben ([206]).

(146) A Bizottság ezért továbbra is folyamatosan nyomon követi az EU–USA adatvédelmi pajzzsal létrehozott, személyes adatok továbbítására szolgáló átfogó keretet, valamint azt, hogy az Egyesült Államok hatóságai eleget tesznek-e az e határozathoz csatolt nyilatkozatoknak és kötelezettségvállalásoknak. Ezen eljárás elősegítése érdekében az Egyesült Államok kötelezettséget vállalat arra, hogy tájékoztatja a Bizottságot az USA jogában bekövetkező lényeges fejleményekről, amennyiben azok relevánsak az adatvédelmi pajzs szempontjából az adatvédelem, valamint a hatóságok személyes adatokhoz való hozzáférésére vonatkozó korlátozások és biztosítékok terén. Továbbá e határozat vonatkozásában éves közös felülvizsgálatra kerül sor, amely az EU–USA adatvédelmi pajzs működésének minden elemét lefedi, ideértve az elvek alóli nemzetbiztonsági és bűnüldözési kivételek működését is. Ezenfelül az általános adatvédelmi rendelet hatálybalépését követően a Bizottság megvizsgálja majd az adatvédelmi pajzs által biztosított védelem szintjét, ugyanis az uniós jog jogi fejleményei szintén befolyásolhatják a megfelelőségre vonatkozó megállapítást.

(147) Az I., II. és VI. mellékletben említett éves közös felülvizsgálat elvégzése érdekében a Bizottság találkozni fog a Kereskedelmi Minisztériummal és az FTC-vel, amelyeket megfelelő esetben elkísérnek az adatvédelmi pajzs rendelkezéseinek végrehajtásában részt vevő egyéb szervezeti egységek és ügynökségek, valamint a nemzetbiztonsággal összefüggő ügyekben az ODNI képviselői, az egyéb hírszerzési szervezeti egységek és az ombudsman. E találkozón részt vehetnek az uniós adatvédelmi hatóságok, valamint a 29. cikk szerinti munkacsoport képviselői.

([203]) *Schrems-ügy*, 40. és azt követő pontok, 101–103. pont.
([204]) *Schrems-ügy*, 51., 52. és 62. pont.
([205]) *Schrems-ügy*, 65. pont.
([206]) *Schrems-ügy*, 76. pont.

(148) Az éves közös felülvizsgálat keretében a Bizottság felkéri majd a Kereskedelmi Minisztériumot, hogy nyújtson átfogó tájékoztatást az EU–USA adatvédelmi pajzs működésének valamennyi fontos eleméről, többek között az adatvédelmi hatóságoktól a Kereskedelmi Minisztériumhoz érkező utalásokról, valamint a hivatalból végzett megfelelőségi felülvizsgálatok eredményeiről. A Bizottság magyarázatokat igényel továbbá az EU–USA adatvédelmi pajzzsal és annak működésével kapcsolatban, bármely rendelkezésre álló információ – többek között az USA FREEDOM törvény alapján engedélyezett átláthatósági jelentések, az USA nemzeti hírszerzési hatóságai, az adatvédelmi hatóságok, és adatvédelmi csoportok nyilvános jelentései, média-beszámolók vagy bármely egyéb lehetséges forrás – alapján felmerülő kérdésekről és ügyekről. Ezenfelül a Bizottság e tekintetben ellátandó feladatainak megkönnyítése érdekében a tagállamoknak tájékoztatniuk kell a Bizottságot azokról az esetekről, amikor az elvek egyesült államokbeli betartásának biztosításáért felelős szervek intézkedései nem szavatolják a megfelelést, és bármely arra utaló körülményről, hogy az Egyesült Államok nemzetbiztonságért, vagy a bűncselekmények megelőzéséért felderítéséért és üldözéséért felelős hatóságai nem biztosítják a szükséges védelmet.

(149) Az éves közös felülvizsgálat alapján a Bizottság az Európai Parlamentnek és a Tanácsnak benyújtandó nyilvános jelentést készít.

7. A MEGFELELŐSÉGI HATÁROZAT FELFÜGGESZTÉSE

(150) Amennyiben az ellenőrzések vagy bármely egyéb rendelkezésre álló információ alapján a Bizottság arra a következtetésre jut, hogy az adatvédelmi pajzs által kínált védelem szintje már nem tekinthető az Unióéval lényegében azonosnak, vagy egyértelmű jelei mutatkoznak annak, hogy az Egyesült Államokban már nem biztosítható az elvek hatékony betartása, vagy az Egyesült Államok nemzetbiztonságért, vagy a bűncselekmények megelőzéséért, nyomozásáért, felderítéséért és üldözéséért felelős hatóságainak intézkedései nem biztosítják a szükséges védelmet, a Bizottság tájékoztatja erről a Kereskedelmi Minisztériumot és azt kérelmezi, hogy meghatározott, ésszerű határidőn belül hozzák meg a megfelelő intézkedéseket az elvek esetleges nem teljesítésének gyors kezelésére. Ha a meghatározott határidő letelte után az Egyesült Államok hatóságai nem igazolják kielégítően, hogy az EU–USA adatvédelmi pajzs továbbra is garantálja a tényleges megfelelést és a megfelelő szintű védelmet, a Bizottság megindítja az e határozat részbeni vagy teljes felfüggesztéséhez vagy hatályon kívül helyezéséhez vezető eljárást ([207]). Ennek alternatívájaként a Bizottság javaslatot tehet e határozat például oly módon történő módosítására, hogy csupán a további feltételeknek megfelelő adattovábbításokra korlátozza a megfelelőségre vonatkozó megállapítás hatályát.

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

a) arra utaló jelek, hogy az Egyesült Államok hatóságai nem tesznek eleget az e határozathoz csatolt nyilatkozatoknak és kötelezettségvállalásoknak, többek között az Egyesült Államok hatóságainak az EU–USA adatvédelmi pajzs alapján továbbított személyes adatokhoz való nemzetbiztonsági, bűnüldözési és egyéb közérdekű célokból történő hozzáférésére vonatkozó feltételek és korlátozások tekintetében;

b) az uniós érintettek panaszai hatékony kezelésének elmulasztása; ezzel összefüggésben a Bizottság az összes olyan körülményt figyelembe fogja venni, amely hatást gyakorol az uniós érintettek jogai érvényesítésének lehetőségére, ideértve különösen az öntanúsított egyesült államokbeli vállalatok önkéntes kötelezettségvállalását az adatvédelmi hatóságokkal való együttműködésre és azok ajánlásainak követésére; vagy

c) az, hogy az adatvédelmi pajzs ombudsmanja nem ad időben megfelelő választ az uniós érintettektől érkező kérelmekre.

(152) A Bizottság fontolóra veszi továbbá az e határozat módosításához, felfüggesztéséhez vagy hatályon kívül helyezéséhez vezető eljárás megindítását, ha az EU–USA adatvédelmi pajzs működésének éves közös felülvizsgálata keretében vagy egyéb alkalommal a Kereskedelmi Minisztérium vagy az adatvédelmi pajzs végrehajtásában érintett egyéb szervezeti egységek és ügynökségek vagy a nemzetbiztonsággal összefüggő ügyekben a hírszerzési szervezeti egységek képviselői és az ombudsman nem szolgáltatják az elvek teljesítésének, a panaszkezelési eljárások hatékonyságának vagy az Egyesült Államok nemzeti hírszerzési hatóságainak intézkedései következtében

([207]) Az általános adatvédelmi rendelet alkalmazásának időpontjától a Bizottság élni fog azzal a jogkörével, hogy kellően indokolt, rendkívül sürgős esetben az e határozatot felfüggesztő végrehajtási aktust fogadjon el, amely a megfelelő komitológiai bizottságnak való előzetes benyújtás nélkül, haladéktalanul alkalmazandó, és hat hónapot meg nem haladó időszakig marad hatályban.

– különösen amiatt, hogy a személyes adatok gyűjtése és/vagy az azokhoz való hozzáférés nem korlátozódik a feltétlenül szükséges és arányos mértékre – az előírt védelmi szint csökkenésének értékeléséhez szükséges információkat vagy pontosításokat. A Bizottság ezzel összefüggésben figyelembe veszi majd, hogy a releváns információk milyen mértékben szerezhetők be más forrásokból, többek között az öntanúsított amerikai vállalatoknak az USA FREEDOM törvény alapján engedélyezett jelentéseiből.

(153) A 95/46/EK irányelv 29. cikke alapján létrehozott, az egyéneknek a személyes adatok feldolgozása tekintetében való védelmével foglalkozó munkacsoport közzétette véleményét az EU–USA adatvédelmi pajzs által biztosított védelem szintjéről, ([208]) amit figyelembe vettünk e határozat elkészítése során.

(154) Az Európai Parlament állásfoglalást fogadott el a transzatlanti adatáramlásokról ([209]).

(155) Az e határozatban előírt intézkedések összhangban állnak a 95/46/EK irányelv 31. cikke (1) bekezdése szerint felállított bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

(1) A 95/46/EK irányelv 25. cikke (2) bekezdésének alkalmazásában az Egyesült Államok megfelelő szintű védelmet biztosít az EU–USA adatvédelmi pajzs keretében az Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében.

(2) Az EU–USA adatvédelmi pajzsot az Egyesült Államok Kereskedelmi minisztériuma által 2016. július 7-én kibocsátott, a II. mellékletben ismertetett elvek, valamint az I. és a III–VII. mellékletben felsorolt dokumentumokban foglalt hivatalos nyilatkozatok és kötelezettségvállalások alkotják.

(3) Az (1) bekezdés alkalmazásában a személyes adatok az EU–USA adatvédelmi pajzs keretében kerülnek továbbításra, amennyiben az Unióból egy olyan egyesült államokbeli szervezethez továbbítják azokat, amelyet – a II. mellékletben ismertetett elvek I. és III. szakaszának megfelelően – felvettek az „adatvédelmi pajzsban részt vevő szervezetek listájára", amelyet az Egyesült Államok Kereskedelmi Minisztériuma vezet és a nyilvánosság számára hozzáférhetővé tesz.

2. cikk

E határozat nem érinti a 95/46/EK irányelvnek a 25. cikk (1) bekezdésétől eltérő azon rendelkezéseinek, különösen (4) cikkének alkalmazását, amelyek a személyes adatok tagállamokon belüli kezelésére vonatkoznak.

3. cikk

Ha a tagállamok hatáskörrel rendelkező hatóságait a 95/46/EK irányelv 28. cikkének (3) bekezdése alapján megillető jogkör gyakorlása egy olyan egyesült államokbeli szervezethez irányuló adatáramlás felfüggesztéséhez vagy végleges tilalmához vezet, amelyet a II. mellékletben ismertetett elvek I. és III. szakaszának megfelelően az egyének személyes adataik kezelése tekintetében történő védelme érdekében felvettek az adatvédelmi pajzsban részt vevő szervezetek listájára, az érintett tagállam haladéktalanul tájékoztatja erről a Bizottságot.

4. cikk

(1) A Bizottság folyamatosan figyelemmel kíséri az EU–USA adatvédelmi pajzs működését annak vizsgálata céljából, hogy az Egyesült Államok továbbra is megfelelő védelmet biztosít-e az annak alapján az Unióból az egyesült államokbeli szervezetekhez továbbított személyes adatok tekintetében.

([208]) 01/2016. sz. vélemény az EU–USA adatvédelmi pajzs megfelelőségéről szólói határozattervezetről, elfogadás: 2016. április 13.
([209]) Az Európai Parlament 2016. május 26-i állásfoglalása a transzatlanti adatáramlásokról (2016/2727(RSP))

(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 kormányzati 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 feltétlenül szükséges mértéket és/vagy nem létezik hatékony jogvédelem az ilyen beavatkozásokkal szemben.

(4) A Bizottság az ezen határozatról a tagállamoknak küldött értesítés időpontjától számított egy éven belül és azt követően évente értékeli az 1. cikk (1) bekezdésébe foglalt megállapítást az összes rendelkezésre álló információ alapján, ideértve az I., II. és VI. mellékletben említett éves közös felülvizsgálat részeként kapott információkat.

(5) A Bizottság jelentést tesz bármely vonatkozó megállapításról a 95/46/EK irányelv 31. cikke alapján létrehozott bizottságnak.

(6) A Bizottság a 95/46/EK irányelv 31. cikkének (2) bekezdésében említett eljárásnak megfelelően intézkedéstervezeteket nyújt be e határozat felfüggesztése, módosítása, visszavonása vagy hatályának korlátozása céljából többek között akkor, ha az alábbiakra utaló jelek mutatkoznak:

— az Egyesült Államok hatóságai nem tesznek eleget az e határozathoz csatolt nyilatkozatoknak és kötelezettségvállalásoknak, többek között az Egyesült Államok hatóságainak az EU–USA adatvédelmi pajzs alapján továbbított személyes adatokhoz való nemzetbiztonsági, bűnüldözési és egyéb közérdekű célokból történő hozzáférésére vonatkozó feltételek és korlátozások tekintetében,

— az uniós érintettek panaszai hatékony kezelésének rendszeres elmulasztása, vagy

— az, hogy az adatvédelmi pajzs ombudsmanja rendszeresen nem ad időben megfelelő választ – a III. melléklet 4. szakasza e) pontjának előírásai szerint – az uniós érintettektől érkező kérelmekre.

A Bizottság ilyen intézkedéstervezeteket terjeszt elő továbbá, ha az EU–USA adatvédelmi pajzs működésének biztosításában részt vevő egyesült államokbeli szervek együttműködésének hiánya megakadályozza a Bizottságot annak megállapításában, hogy érinti-e bármely tényező az 1. cikk (1) bekezdésében foglalt megállapítást.

5. cikk

A tagállamok megtesznek minden, az e határozatnak való megfeleléshez szükséges intézkedést.

6. cikk

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2016. július 12-én.

a Bizottság nevében

Věra JOUROVÁ

a Bizottság tagja

I. MELLÉKLET

Penny Pritzker amerikai kereskedelmi miniszter levele

2016. július 7.

Věra Jourová
a jogérvényesülésért, a fogyasztópolitikáért és a nemek közötti esélyegyenlőségért felelős biztos
Európai Bizottság
Rue de la Loi/Westraat 200
1049 Bruxelles/Brussel
Belgium

Tisztelt Jourová biztos asszony!

Az Egyesült Államok nevében ezennel örömmel adom át az EU-USA adatvédelmi pajzs anyagainak csomagját, amely a munkacsoportjaink közötti gyümölcsöző tárgyalások eredménye. Ez a csomag a Bizottság számára nyilvános forrásokból elérhető más anyagokkal együtt nagyon szilárd alapot biztosít az Európai Bizottság részére a megfelelőség újonnan történő megállapításához ([1]).

Mindketten büszkék lehetünk a keretrendszeren végzett javításokra. Az adatvédelmi pajzs az atlanti térség mindkét oldalán erős konszenzusos támogatást élvező elveken alapul, és mi megerősítettük azok érvényességét. Együttműködésünk révén valódi lehetőségünk nyílt az adatvédelem javítására az egész világon.

Az adatvédelmi csomag tartalmazza az adatvédelmi pajzs elveit, valamint a programot igazgató Kereskedelmi Minisztérium Nemzetközi Kereskedelmi Igazgatósága (ITA) által írt, 1. mellékletként csatolt levelet, amelyben leírjuk a minisztériumunk által annak biztosítása érdekében tett kötelezettségvállalásokat, hogy az adatvédelmi pajzs hatékonyan működjön. A csomag tartalmazza még a 2. mellékletet is, amely részletezi a Kereskedelmi Minisztériumnak az adatvédelmi pajzs keretében elérhető új választott bírósági modellre vonatkozó további kötelezettségvállalásait.

Arra utasítottam a munkatársaimat, hogy minden szükséges erőforrást sürgősen és teljes körűen állítsanak az adatvédelmi pajzs keretrendszer megvalósításának szolgálatába, illetve fordítsák ezeket az erőforrásokat annak biztosítására, hogy az 1. és 2. mellékletben leírt kötelezettségvállalások időben teljesüljenek.

Az adatvédelmi pajzs csomag tartalmaz még az Egyesült Államok hatóságai által készített más dokumentumokat is, nevezetesen az alábbiakat:

— a Szövetségi Kereskedelmi Bizottság (FTC) levele, amely leírja az adatvédelmi pajzs általa történő végrehajtását,

— a Közlekedési Minisztérium levele, amely leírja az adatvédelmi pajzs általa történő végrehajtását,

— a nemzeti hírszerzés igazgatójának irodája (ODNI) által készített két levél az USA nemzetbiztonsági hatóságaira vonatkozó biztosítékokról és korlátozásokról,

— a Külügyminisztérium levele és az azt kísérő tájékoztatás, amely leírja a Külügyminisztérium kötelezettségvállalását egy új adatvédelmi pajzs ombudsman kinevezésére, akinek a feladata az Egyesült Államok jelfelderítési gyakorlataira vonatkozó megkeresések benyújtása, valamint

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

Biztosíthatom arról, hogy az Egyesült Államok komolyan veszi ezeket a kötelezettségvállalásokat.

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

A megfelelőség megállapításáról szóló végső jóváhagyás után 30 napon belül a teljes adatvédelmi pajzs csomagot továbbítjuk a *Szövetségi Közlönynek* közzétételre.

Várakozással tekintünk az Önökkel történő együttműködésre az adatvédelmi pajzs megvalósítása, valamint e folyamat következő szakaszának megkezdése során.

Üdvözlettel:

Penny Pritzker

1. melléklet

Ken Hyatt megbízott nemzetközi kereskedelmi miniszterhelyettes levele

Tisztelt Věra Jourová
A jogérvényesülésért, a fogyasztópolitikáért és a nemek közötti esélyegyenlőségért felelős biztos
Európai Bizottság
Rue de la Loi/Westraat 200
1049 Bruxelles/Brussel
Belgium

Tisztelt Jourová biztos asszony!

A Nemzetközi Kereskedelmi Igazgatóság nevében örömmel mutatom be a személyes adatok magasabb szintű védelmét, amelyet az EU-USA adatvédelmi pajzs keretrendszer (a továbbiakban: „adatvédelmi pajzs" vagy „keretrendszer") biztosít, valamint a Kereskedelmi Minisztérium (a továbbiakban: „Minisztérium") által annak biztosítása érdekében tett kötelezettségvállalásokat, hogy az adatvédelmi pajzs hatékonyan működjön. Ennek a történelmi megállapodásnak a véglegesítése jelentős eredmény az adatvédelem szempontjából és a vállalkozások számára egyaránt az atlanti térség mindkét oldalán. Biztonságot nyújt az EU polgárok számára az adataik védelme és annak tekintetében, hogy bármely probléma esetén jogorvoslat áll rendelkezésükre. Bizonyosságot nyújt, amely azzal segíti az atlanti térség gazdasági növekedését, hogy biztosítja, hogy európai és amerikai vállalkozások ezrei folytathassák a határainkon átívelő beruházásaikat és üzleti tevékenységüket. Az adatvédelmi pajzs Önökkel, az Európai Bizottságban („Bizottság") dolgozó kollégáinkkal folytatott több mint két éves kemény munka és együttműködés eredménye. Várakozással tekintünk a Bizottsággal végzett munka folytatására annak biztosítása érdekében, hogy az adatvédelmi pajzs a várakozások szerint működjön.

Együttműködtünk a Bizottsággal az adatvédelmi pajzs kidolgozásában azért, hogy az Egyesült Államokban létrehozott szervezetek teljesítsék az uniós jogszabályok adatvédelemre vonatkozó megfelelőségi követelményeit. Az új keretrendszer az egyének és a vállalkozások számára is számos jelentős előnyt nyújt. Először is az uniós polgárok adatait jelentős adatvédelmi rendelkezésekkel védi. Előírja a részt vevő egyesült államokbeli szervezetek számára, hogy megfelelő adatvédelmi szabályzatot dolgozzanak ki, nyilvános kötelezettségvállalást tegyenek az adatvédelmi pajzs elveinek való megfelelés tekintetében azért, hogy a kötelezettségvállalás az amerikai jog alapján érvényesíthető legyen, évente újra tanúsítsák a megfelelésüket a Minisztérium számára, ingyenes független vitarendezési lehetőséget biztosítsanak az uniós polgárok részére, valamint az Egyesült Államok Szövetségi Kereskedelmi Bizottsága („FTC"), Közlekedési Minisztériuma („DOT"), illetve más jogérvényesítési hatóságok hatálya alá tartozzanak. Másodszor, az adatvédelmi pajzs lehetővé teszi az Egyesült Államokban működő vállalatok, valamint európai vállalatok egyesült államokbeli leányvállalatainak ezrei számára, hogy személyes adatokat kapjanak az Európai Unióból a transzatlanti kereskedelmet támogató adatáramlás elősegítése érdekében. A transzatlanti gazdasági kapcsolatok már most a legnagyobb volumenűek a világon, a globális gazdasági teljesítmény felét teszik ki, és közel egybillió dollár értékű áru és szolgáltatás kereskedelmét jelentik, amely több millió álláshelyet támogat az atlanti térség mindkét oldalán. A transzatlanti adatáramlásra támaszkodó vállalkozások valamennyi ipari ágazatot képviselik, köztük vannak a legnagyobb Fortune 500 listán szereplő cégek, valamint sok kis- és középvállalkozás (kkv). A transzatlanti adatáramlás lehetővé teszi az egyesült államokbeli szervezetek számára az áruk, szolgáltatások és munkalehetőségek európai polgárok számára történő nyújtásához szükséges adatok kezelését. Az adatvédelmi pajzs támogatja a közös adatvédelmi elveket, a jogi eljárásaink közötti eltérések áthidalását, miközben elősegíti Európa és az Egyesült Államok kereskedelmi és gazdasági célkitűzéseit.

A vállalatok önkéntesen dönthetnek ugyan arról, hogy önmaguk tanúsítják az új keretrendszer betartását, de ha egyszer egy vállalat nyilvánosan kötelezettséget vállalt az adatvédelmi pajzs alkalmazására, a kötelezettségvállalása érvényesíthető az Egyesült Államok joga alapján – a Szövetségi Kereskedelmi Bizottság vagy a Közlekedési Minisztérium által attól függően, hogy melyiknek van hatásköre az adatvédelmi pajzs alkalmazását vállaló szervezet felett.

Az adatvédelem erősödése az adatvédelmi pajzs elvei alapján

A létrehozott adatvédelmi pajzs erősíti az adatok védelmét az alábbiak révén:

— a tájékoztatási elvben előírja további információk nyújtását egyének számára, beleértve a szervezet nyilatkozatát az adatvédelmi pajzsban történő részvételről, nyilatkozat tételét az egyén személyes adatokhoz való hozzáférési jogáról, valamint az illetékes független vitarendezési szerv meghatározását,

— erősíti az adatvédelmi pajzsban részt vevő szervezet által egy harmadik fél adatkezelő számára átadott személyes adatok védelmét azáltal, hogy előírja a feleknek szerződés kötését, amely rendelkezik arról, hogy az ilyen adatok csak korlátozott és meghatározott célokra dolgozhatók fel, amelyek összhangban vannak az egyén által adott hozzájárulással, valamint azt, hogy a címzett az elvekkel azonos szintű védelmet biztosít,

— erősíti az adatvédelmi pajzsban részt vevő szervezet által egy harmadik szereplő számára átadott személyes adatok védelmét, beleértve az alábbiak előírását az adatvédelmi pajzsban részt vevő szervezet számára: indokolt és megfelelő lépések tétele annak biztosítása érdekében, hogy az adott szereplő hatékonyan kezelje a személyes adatokat, amelyeket a szervezet elvek szerinti kötelezettségeivel összhangban továbbítottak; kérésre indokolt és megfelelő lépések tétele a jogosulatlan adatkezelés megszüntetése és az eredeti állapot helyreállítása érdekében; valamint az adott szereplővel kötött szerződése megfelelő adatvédelmi rendelkezései összefoglalásának vagy egy reprezentatív példányának az átadása kérésre a Minisztérium számára,

— rendelkezés arról, hogy az adatvédelmi pajzsban részt vevő szervezet felelős az általa az adatvédelmi pajzs keretében kapott és ezt követően a nevében tevékenykedő harmadik fél megbízottnak átadott személyes adatok kezeléséért, valamint arról, hogy az adatvédelmi pajzsban részt vevő szervezet marad a felelős az elvek alapján, amennyiben a megbízottja a szóban forgó személyes adatokat olyan módon kezeli, amely nincs összhangban az elvekkel – kivéve, ha a szervezet bizonyítja, hogy nem felelős a károkozást előidéző eseményért,

— annak egyértelmű rögzítése, hogy az adatvédelmi pajzsban részt vevő szervezetnek a személyes adatokat a kezelés szempontjából lényeges adatokra kell korlátoznia,

— annak megkövetelése a szervezettől, hogy évente tanúsítsa a Minisztérium felé azon kötelezettségvállalását, hogy alkalmazza az elveket az adatvédelmi pajzsban történő részvétele során általa kapott adatokra, amennyiben kilép az adatvédelmi pajzsból és úgy dönt, hogy megőrzi ezeket az adatokat,

— annak előírása, hogy független jogorvoslati mechanizmusokat biztosítsanak ingyenesen az egyének számára,

— annak előírása a szervezetek és a kiválasztott független jogorvoslati mechanizmusok számára, hogy azonnal válaszoljanak a Minisztériumnak az adatvédelmi pajzzsal kapcsolatos információkra vonatkozó megkereséseire és kéréseire,

— annak előírása a szervezetek számára, hogy gyorsan válaszoljanak az EU tagállamok hatóságai által a Minisztériumon keresztül az elvek betartására vonatkozóan benyújtott panaszokra, és

— annak előírása az adatvédelmi pajzsban részt vevő szervezet számára, hogy tegye közzé az FTC számára benyújtott megfelelési vagy értékelési jelentés adatvédelmi pajzsra vonatkozó részét, amennyiben az FTC vagy egy bíróság meg nem felelés miatt eljárást indít vele szemben.

Az adatvédelmi pajzs program Kereskedelmi Minisztérium általi igazgatása és felügyelete

A Minisztérium megerősíti az elkötelezettségét, hogy fenntart és közzétesz egy hiteles listát azokról az egyesült államokbeli szervezetekről, amelyek önmaguk tanúsították a megfelelésüket a Minisztérium felé, és kötelezettséget vállaltak az elvek betartására (az „adatvédelmi pajzsban részt vevő szervezetek listáj"). A Minisztérium az adatvédelmi pajzs listát naprakésszé teszi azon szervezetek törlésével, amelyek önkéntesen kilépnek, nem teljesítik az éves ismételt tanúsítást a Minisztérium eljárásainak megfelelően vagy megállapítják róluk, hogy ismételten nem teljesítik az elveket. Ezenkívül a Minisztérium fenntart és közzétesz egy hiteles listát azokról az egyesült államokbeli szervezetekről, amelyek előzőleg önmaguk tanúsították a megfelelésüket a Minisztérium felé, majd törölték őket az adatvédelmi pajzs listáról, beleértve azokat, amelyeket azért töröltek, mert ismételten nem tartották be az elveket. A Minisztérium minden szervezet esetében megadja a törlés okát.

Ezenkívül a Minisztérium kötelezettséget vállal az adatvédelmi pajzs igazgatásának és felügyeletének az erősítésére. A Minisztérium konkrétan az alábbiakat teszi:

További információk nyújtása az adatvédelmi pajzs honlapon

— az adatvédelmi pajzsban részt vevő szervezetek listájának, valamint azon szervezetek nyilvántartásának a vezetése, amelyek előzőleg önmaguk tanúsították az elvek betartását, de már nem élvezik az adatvédelmi pajzs előnyeit,

— jól látható helyen elhelyezett tájékoztatás arról, hogy az adatvédelmi pajzs listáról törölt egyik szervezet sem élvezi már az adatvédelmi pajzs előnyeit, viszont továbbra is kötelesek alkalmazni az elveket az általuk az adatvédelmi pajzsban történt részvétel során kapott személyes adatokra, ameddig megőrzik azokat az adatokat, valamint

— link biztosítása az adatvédelmi pajzzsal kapcsolatos FTC esetek listájához, amely az FTC honlapján található.

Öntanúsításra vonatkozó követelmények ellenőrzése

— a szervezet öntanúsításának (vagy éves ismételt tanúsításának) a véglegesítése és a szervezet adatvédelmi pajzs listára történő felvétele előtt annak ellenőrzése, hogy a szervezet:

  — megadta az előírt szervezeti elérhetőségeket,

  — leírta a szervezet Unióból kapott személyes adatokkal kapcsolatos tevékenységeit,

  — megadta, hogy milyen személyes adatokra vonatkozik az öntanúsítás,

  — ha a szervezetnek van nyilvános honlapja, akkor megadta a honlap címét, ahol az adatvédelmi szabályzat elérhető és a megadott honlapon az adatvédelmi szabályzat elérhető, vagy ha a szervezet nem rendelkezik nyilvános honlappal, akkor megadta, hol tekinthető meg az adatvédelmi szabályzat a nyilvánosság számára,

  — a vonatkozó adatvédelmi szabályzata nyilatkozatot tartalmaz arra vonatkozóan, hogy betartja az elveket, és ha az adatvédelmi szabályzat online elérhető, a Minisztérium adatvédelmi pajzs honlapjára mutató hiperlinket,

  — meghatározta 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),

  — ha a szervezet úgy dönt, hogy a jogorvoslati, végrehajtási és felelősségi elv (a)(i) és (a)(iii) bekezdéseiben meghatározott követelményeket teljesíti azáltal, hogy vállalja az együttműködést a megfelelő uniós adatvédelmi hatóságokkal, jelezte a szándékát az adatvédelmi hatóságokkal való együttműködésre az adatvédelmi pajzs keretében benyújtott panaszok kivizsgálása és megoldása terén, konkrétan azt, hogy válaszol a megkeresésekre az érintettek által közvetlenül a nemzeti adatvédelmi hatóságokhoz benyújtott panaszok esetén,

  — megadta azokat az adatvédelmi programokat, amelyekben a szervezet részt vesz,

  — megadta az elveknek való megfelelés biztosítása ellenőrzésének a módszerét (*pl.* belső, harmadik fél általi),

  — mind az öntanúsításban, mint az adatvédelmi szabályzatában megadta azt a független jogorvoslati mechanizmust, amely rendelkezésre áll a panaszok kivizsgálására és megoldására,

  — a vonatkozó adatvédelmi szabályzatában – ha az online is elérhető – a megoldatlan panaszok kivizsgálására rendelkezésre álló független jogorvoslati mechanizmus honlapjára vagy panasz-benyújtási formanyomtatványára mutató hiperlink is szerepel, valamint

  — ha a szervezet jelezte a szándékát, hogy az EU által átadott, munkaviszony keretében használt humánerőforrás-adatokat kíván fogadni, kinyilvánította kötelezettségvállalását, hogy együttműködik az adatvédelmi hatóságokkal és betartja azok előírásait az ilyen adatokkal kapcsolatos tevékenységére vonatkozó panaszok kezelése terén, átadta a Minisztérium számára a humánerőforrás-adatok védelmére vonatkozó politikájának egy példányát és megadta, hogy az érintett alkalmazottai hol tekinthetik meg az adatvédelmi szabályzatot.

— független jogorvoslati mechanizmusokat alkalmaznak annak ellenőrzésére, hogy a szervezetek az öntanúsításukban megadott vonatkozó mechanizmusokban ténylegesen regisztráltak, amennyiben ilyen regisztráció elő van írva.

Az adatvédelmi pajzs listáról törölt szervezetek ellenőrzésének kiterjesztése

— az adatvédelmi pajzs listáról „ismétlődő nemteljesítés” miatt törölt szervezetek értesítése arról, hogy nem jogosultak megőrizni az adatvédelmi pajzs keretében kapott információkat, valamint

— kérdőívek küldése azon szervezeteknek, amelyek öntanúsítása lejár vagy amelyek önkéntesen kiléptek az adatvédelmi pajzsból, annak ellenőrzése céljából, hogy a szervezet visszatér, törlik vagy folytatja az elvek alkalmazását azokra a személyes adatokra, amelyeket az adatvédelmi pajzsban történt részvétele során kapott, és a személyes adatok megőrzése esetén annak ellenőrzése, hogy a szervezeten belül ki lesz a folyamatos kapcsolattartó az adatvédelmi pajzzsal kapcsolatos kérdésekben.

Hamis részvételi nyilatkozatok keresése és kezelése

— az adatvédelmi pajzsban történő részvételre vonatkozó hamis nyilatkozatok megállapítása érdekében azon szervezetek adatvédelmi szabályzatainak a felülvizsgálata, amelyek előzőleg részt vettek az adatvédelmi pajzs programban, de törölték őket az adatvédelmi pajzs listáról,

— folyamatosan, amennyiben a szervezet: a) visszalép az adatvédelmi pajzsból, b) nem tanúsítja ismételten az elvek teljesítését, vagy c) törlik az adatvédelmi pajzs résztvevői közül mégpedig „ismétlődő nemteljesítés" miatt, vállalja, hogy *hivatalból* ellenőrzi, hogy a szervezet törölte a vonatkozó közzétett adatvédelmi szabályzatból a hivatkozást az adatvédelmi pajzsra, amely arra utal, hogy a szervezet továbbra is aktívan részt vesz az adatvédelmi pajzsban és jogosult annak előnyeire. 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 jogérvényesítésre, amennyiben továbbra is azt állítja, hogy tanúsította az adatvédelmi pajzs teljesítését. Ha a szervezet nem törli a hivatkozásokat és nem végez öntanúsítást az adatvédelmi pajzs követelményeinek teljesítéséről, a Minisztérium *hivatalból* továbbítja az ügyet az FTC, a DOT vagy más megfelelő jogérvényesítési hivatal számára, vagy intézkedik az adatvédelmi pajzs tanúsítási jel végrehajtásáról,

— egyéb intézkedéseket tesz az adatvédelmi pajzsban történő részvételre vonatkozó hamis nyilatkozatoknak és az adatvédelmi pajzs tanúsítási jel rosszhiszemű használatának a megállapítása érdekében, beleértve az interneten történő kutatást annak megállapítása érdekében, hogy az adatvédelmi pajzs tanúsító védjegyet hol teszik ki, és hol szerepel hivatkozás az adatvédelmi pajzsra a szervezet adatvédelmi szabályzatában,

— azonnal foglalkozik azokkal a kérdésekkel, amelyeket a részvételre vonatkozó hamis nyilatkozatok és a tanúsító védjeggyel történő visszaélés *hivatalból* történő vizsgálata során határoztunk meg, beleértve azon szervezetek figyelmeztetését, amelyek a fentiek szerint hamisan állítják, hogy részt vesznek az adatvédelmi pajzs programban,

— egyéb megfelelő korrekciós intézkedések tétele, beleértve olyan jogorvoslat alkalmazását, amelyre a Minisztériumnak jogosultsága van, és az ügy továbbítása az FTC, a DOT vagy más megfelelő jogérvényesítő hatóság számára, és

— a részvételre vonatkozó hamis nyilatkozatokkal kapcsolatosan általunk kapott panaszok azonnali vizsgálata és kezelése.

A Minisztérium vizsgálja a szervezetek adatvédelmi szabályzatát az adatvédelmi pajzsban történő részvételre vonatkozó hamis nyilatkozatok hatékony megállapítása és kezelése érdekében. A Minisztérium konkrétan vizsgálja azoknak a szervezeteknek az adatvédelmi szabályzatát, amelyeknek az öntanúsítása lejárt, mivel nem tanúsították ismételten az elvek teljesítését. A Minisztérium az ilyen vizsgálatot annak ellenőrzése érdekében végzi, hogy az ilyen szervezetek törölték a nyilvánosan közzétett adatvédelmi szabályzatukból a hivatkozásokat, amelyek arra utalnak, hogy a szervezet továbbra is aktívan részt vesz az adatvédelmi pajzsban. Az ilyen típusú vizsgálatokkal meghatározzuk azokat a szervezeteket, amelyek nem törölték az ilyen hivatkozásokat, és levelet küldünk ezeknek a szervezeteknek a Minisztérium Főtanácsadói Hivatalából, amely figyelmezteti az adott szervezetet az esetleges jogérvényesítési intézkedésre, amennyiben nem törli a hivatkozásokat. A Minisztérium nyomonkövetési intézkedéseket tesz annak biztosítása érdekében, hogy a szervezetek vagy törlik a helytelen hivatkozásokat, vagy ismételten tanúsítják az elvek teljesítését. Ezenkívül, a Minisztérium intézkedéseket tesz az adatvédelmi pajzsban történő részvételre vonatkozó hamis nyilatkozatokat tett olyan szervezetek meghatározása érdekében, amelyek soha nem vettek részt az adatvédelmi pajzs programban, és hasonló korrekciós intézkedéseket tesz az ilyen szervezetekkel kapcsolatban.

A program rendszeres, *hivatalból* történő megfelelőség-felülvizsgálata és értékelése

— folyamatosan figyeli a tényleges megfelelést, beleértve részletes kérdőívek küldését a részt vevő szervezeteknek, azoknak a kérdéseknek a meghatározását, amelyek garantálhatják a további nyomonkövetési intézkedéseket. Ilyen megfelelőség-felülvizsgálatokat különösen akkor végeznek, ha: a) a Minisztérium konkrét lényegi panaszt kap az elvek szervezet általi teljesítésével kapcsolatban, b) a szervezet nem reagál megfelelő módon a Minisztérium adatvédelmi pajzsra vonatkozó információkkal kapcsolatos megkeresésére, vagy c) hitelt érdemlő bizonyíték van arra, hogy a szervezet nem teljesíti az adatvédelmi pajzs keretében tett kötelezettségvállalásait. A Minisztérium adott esetben tanácskozik az illetékes adatvédelmi hatóságokkal az ilyen megfelelőség-felülvizsgálatokról, és

— rendszeresen értékeli az adatvédelmi pajzs program igazgatását és felügyeletét annak biztosítása érdekében, hogy a felügyeleti intézkedésekkel megfelelően kezelik a felmerülő új kérdéseket.

A Minisztérium növelte az adatvédelmi pajzs program igazgatására és felügyeletére szánt erőforrásokat, a program igazgatásáért és felügyeletéért felelős személyzet létszámának megduplázását is beleértve. Továbbra is megfelelő erőforrásokat szánunk az ilyen intézkedésekre a program hatékony felügyeletének és igazgatásának a biztosítása érdekében.

Az adatvédelmi pajzs honlap célközönségre szabása

A Minisztérium az adatvédelmi pajzs honlapját három célközönségre szabja: uniós polgárok, uniós vállalkozások és egyesült államokbeli vállalkozások. A közvetlenül uniós polgárokat és uniós vállalkozásokat célzó anyagok bevonása számos módon megkönnyíti az átláthatóságot. Az uniós polgárok számára egyértelműen kifejti: (1) az adatvédelmi pajzs által az uniós polgároknak nyújtott jogokat; (2) az uniós polgárok számára elérhető jogorvoslati mechanizmusokat, ha úgy gondolják, hogy egy szervezet megsértette az elvek betartására vonatkozó kötelezettségvállalását; és (3) a szervezet adatvédelmi pajzsra vonatkozó öntanúsításával kapcsolatos információk elérésének módját. Az uniós vállalkozások számára megkönnyíti az alábbiak ellenőrzését: (1) a szervezet számára biztosítottak-e az adatvédelmi pajzs előnyei; (2) a szervezet adatvédelmi pajzs öntanúsításában szereplő információk típusa; (3) a benne szereplő információkra vonatkozó adatvédelmi szabályzat; és (4) a szervezet által az elvek teljesítésének ellenőrzésére alkalmazott módszer.

Az együttműködés fokozása az adatvédelmi hatóságokkal

Az adatvédelmi hatóságokkal folytatott együttműködés lehetőségeinek a növelése érdekében a Minisztérium kijelölt kapcsolattartót nevez ki a Minisztériumban, aki kapcsolattartóként jár el az adatvédelmi hatóságok felé. Azokban az esetekben, amikor egy adatvédelmi hatóság úgy gondolja, hogy egy szervezet nem teljesíti az elveket, beleértve azt az esetet, amikor egy uniós polgár panaszt nyújtott be, az adatvédelmi hatóság kapcsolatba léphet a Minisztérium kijelölt kapcsolattartójával a szervezet további felülvizsgálatra történő bejelentése érdekében. A kapcsolattartó azokra a szervezetekre vonatkozóan is kap bejelentést, amelyek hamisan állítják, hogy részt vesznek az adatvédelmi pajzsban, habár soha nem végeztek öntanúsítást az elvek teljesítésére vonatkozóan. A kapcsolattartó segít az adatvédelmi hatóságoknak adott szervezet öntanúsítására vagy a programban történt előző részvételére vonatkozó információk keresésében, és a kapcsolattartó válaszol az adatvédelmi hatóságnak az adott adatvédelmi pajzs követelmények megvalósításával kapcsolatos megkeresésére. Másodszor, a Minisztérium anyagokat biztosít az adatvédelmi hatóságoknak az adatvédelmi pajzsra vonatkozóan, amelyeket megjeleníthetnek a saját honlapjukon az átláthatóság növelése érdekében az uniós polgárok és uniós vállalkozások számára. Az adatvédelmi pajzs és a jogok és feladatok ezáltal biztosított jobb ismerete elősegíti a felmerülő problémák meghatározását azok megfelelő kezelése érdekében.

Nemteljesítéssel kapcsolatos panaszok megoldásának elősegítése

A Minisztérium a kijelölt kapcsolattartón keresztül kapja meg az adatvédelmi hatóság által a Minisztériumhoz bejelentett arra vonatkozó panaszokat, hogy az adatvédelmi pajzsban részt vevő valamely szervezet nem teljesíti az elveket. A Minisztérium megtesz minden tőle telhetőt az adatvédelmi pajzsban részt vevő szervezet panasza megoldásának elősegítése érdekében. A panasz kézhezvételétől számított 90 napon belül a Minisztérium tájékoztatást ad az adatvédelmi hatóságnak az aktuális helyzetről. Az ilyen panaszok benyújtásának megkönnyítése érdekében a Minisztérium egy szabvány formanyomtatványt hoz létre az adatvédelmi hatóságok számára, amelyet a Minisztérium kijelölt kapcsolattartójához kell benyújtani. A kijelölt kapcsolattartó nyomon követi az adatvédelmi hatóságoknak a Minisztériumhoz küldött bejelentéseit, és a Minisztérium az alább leírt éves felülvizsgálat során az adott évben általa kapott panaszok összegzéséről szóló jelentést ad ki.

Választott bírósági eljárások alkalmazása és választott bírák kiválasztása a Bizottsággal egyeztetve

A Minisztérium teljesíti az I. melléklet szerinti kötelezettségvállalásait, és közzéteszi az eljárásokat, miután megállapodásra jutottak.

Az adatvédelmi pajzs működésének közös felülvizsgálati mechanizmusa

A Kereskedelmi Minisztérium, az FTC vagy adott esetben egyéb hatóságok éves megbeszélést tartanak a Bizottság, az érintett adatvédelmi hatóságok és a 29. cikk szerinti munkacsoport megfelelő képviselőinek részvételével, ahol a Minisztérium tájékoztatást ad az adatvédelmi pajzs program aktuális helyzetéről. Az éves megbeszéléseken megvitatják az adatvédelmi pajzs működésére, megvalósítására, felügyeletére és végrehajtására vonatkozó aktuális kérdéseket, beleértve a Minisztérium által az adatvédelmi hatóságoktól kapott bejelentéseket, a *hivatalból* végzett megfelelőség-felülvizsgálat eredményeit, továbbá a vonatkozó jogszabály-módosításokat is megvitathatják. Az első éves felülvizsgálat és az azt követő felülvizsgálatok adott esetben kiterjednek az olyan egyéb témákról folytatott párbeszédre, mint az automatizált döntéshozatal területe, ideértve az EU és az Egyesült Államok megközelítése közötti hasonlóságokkal és különbségekkel kapcsolatos kérdéseket.

Jogszabályok naprakésszé tétele

A Minisztérium ésszerű erőfeszítéseket tesz arra, hogy tájékoztassa a Bizottságot az Egyesült Államok jogában bekövetkező lényeges fejleményekről, amennyiben azok relevánsak az adatvédelmi pajzs szempontjából az adatvédelem, valamint az Egyesült Államok hatóságainak a személyes adatokhoz való hozzáférésére és azt követő használatára vonatkozó korlátozások és biztosítékok terén.

Nemzetbiztonsági kivétel

Az adatvédelmi pajzs elveinek betartására vonatkozó, nemzetbiztonsági okokból fennálló korlátozások tekintetében a nemzeti hírszerzés igazgatója irodájának főtanácsadója, Robert Litt is küldött két levelet Justin Antonipillai és Ted Dean számára a Kereskedelmi Minisztériumba, amelyet Önök is megkaptak. Ezek a levelek részletesen tárgyalják többek között az Egyesült Államok által folytatott jelfelderítési tevékenységekre vonatkozó politikákat, biztosítékokat és korlátozásokat. Ezenkívül ezek a levelek leírják a Hírszerző Közösség által ezekkel a kérdésekkel kapcsolatban biztosított átláthatóságot. Amikor a Bizottság értékeli az adatvédelmi pajzs keretrendszert, az ezekben a levelekben adott tájékoztatás biztosítékot nyújt annak a következtetésnek a levonására, hogy az adatvédelmi pajzs megfelelően fog működni az abban meghatározott elveknek megfelelően. Úgy tudjuk, hogy Ön a jövőben – egyéb információk mellett – a Hírszerző Közösség által nyilvánosan kiadott információkat kaphat az adatvédelmi pajzs keretrendszer éves felülvizsgálatára vonatkozóan.

Az adatvédelmi pajzs elvei és a kísérőlevelek és anyagok – köztük a Minisztériumnak az adatvédelmi pajzs keretrendszer igazgatására és felügyeletére vonatkozó kötelezettségvállalásai – alapján azt várjuk, hogy a Bizottság úgy dönt, hogy az EU-USA adatvédelmi pajzs keretrendszer megfelelő védelmet biztosít az uniós jogszabályok értelmében, és az Európai Unióból jövő adattovábbítás folytatódik azon szervezetek felé, amelyek részt vesznek az adatvédelmi pajzsban.

Üdvözlettel:

Ken Hyatt

2. melléklet

Választott bírósági modell

I. MELLÉKLET

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

A. **Hatály**

Ez a választott bírósági lehetőség az egyének rendelkezésére áll annak meghatározására maradványkövetelések esetén, hogy az adatvédelmi pajzsban 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 ([1]) alóli kivételek esetében, vagy az adatvédelmi pajzs megfelelőségére vonatkozó állítások tekintetében.

B. **Rendelkezésre álló jogorvoslatok**

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

C. **Választott bíráskodás előtti követelmények**

Az ezzel a választott bírósági 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 az elvek III.11(d) pontja i. francia bekezdésében meghatározott határidőn belül; (2) az elvek szerinti független jogorvoslati mechanizmusok igénybevétele, amely az egyén számára ingyenes; és (3) a kérdés jelzése az adatvédelmi hatóságukon keresztül a Kereskedelmi Minisztériumnak, és lehetőséget biztosítani a Kereskedelmi Minisztérium számára, hogy mindent megtegyen a kérdés rendezésére a Kereskedelmi Minisztérium Nemzetközi Kereskedelmi Igazgatóságának a levelében meghatározott határidőn belül – az egyén számára ingyenesen.

Ez a választott bírósági lehetőség nem vehető igénybe, ha az elveknek az egyén által említett állítólagos megsértése tárgyában (1) korábban már lefolytattak kötelező erejű választott bírósági eljárást; (2) az egyén részvételével folyó bírósági perben jogerős döntést hoztak; vagy (3) a felek azt már korábban rendezték. Ezenkívül, ezzel a lehetőséggel nem lehet élni, ha egy uniós adatvédelmi hatóság (1) az elvek III.5. vagy III.9. pontja szerint hatáskörrel rendelkezik az adott kérdésben; 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 választott bírósági lehetőségnek az alkalmazását egy másik jogi személlyel szemben, amelyre nem vonatkozik az adatvédelmi hatóság hatásköre.

D. **Ítéletek kötelező ereje**

Az egyén döntése, hogy ezzel a választott bírósági lehetőséggel éljen, teljesen önkéntes. A választott bírósági ítélet a választott bírósági 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, hogy amennyiben a nem pénzbeli méltányos jóvátétel nem teljesen orvosolja az állítólagos jogsértést, akkor a választott bírósági eljárás egyén általi kezdeményezése nem zárja ki a kártérítés iránti követelést, amely egyébként bírósági úton elérhető.

([1]) Az elvek I.5. pontja.

E. **Felülvizsgálat és végrehajtás**

Az egyének és az adatvédelmi pajzsban részt vevő szervezetek a választott bíróság végzésének bírósági felülvizsgálatát és végrehajtását kérhetik a USA Szövetségi Választott bírósági Törvénye alapján ([1]). Minden ilyen ügyet azon szövetségi kerületi bíróság elé kell vinnie, amely az adatvédelmi pajzsban részt vevő szervezet székhelye szerint illetékes bíróság.

Ennek a választott bírósági lehetőségnek a célja egyéni viták rendezése, és a választott bírósági 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 választott bírói testület**

A felek választják ki a választott bírákat a választott bírák alább tárgyalt listájáról.

A vonatkozó jogszabályokkal összhangban az Egyesült Államok Kereskedelmi Minisztériuma és az Európai Bizottság listát állít össze legalább 20 választott bírával, akiket függetlenség, feddhetetlenség és tapasztalat alapján választanak ki. Erre a folyamatra az alábbiak vonatkoznak:

Választott bírák:

(1) a listán maradnak 3 évig, kivételes körülmények vagy okok hiányában, amely időszak további egy alkalommal, 3 évre meghosszabbítható;

(2) nem utasíthatja őket egyik fél vagy az adatvédelmi pajzsban 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; és

(3) engedéllyel kell rendelkezniük az Egyesült Államokban történő jogi praktizálásra, és szakértőknek kell lenniük az Egyesült Államok adatvédelmi törvénye szerint, továbbá tapasztalattal kell rendelkezniük az uniós adatvédelmi jog területén.

G. **Választott bírósági eljárások**

A vonatkozó jogszabályokkal összhangban a megfelelőségi határozat meghozatalától számított 6 hónapon belül a Kereskedelmi Minisztérium és az Európai Bizottság megállapodnak egy bevezetett egyesült államokbeli választott bírósági eljárás rendszerről (mint az AAA vagy JAMS), amely az adatvédelmi pajzzsal foglalkozó testület eljárásaira vonatkozik – az alábbi megfontolások figyelembevételével:

1. A szervezetnek küldött értesítéssel egyén kezdeményezhet kötelező erejű választott bírósági eljárást a fenti választott bírósági 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.

([1]) A szövetségi választott bírósági törvény („FAA") 2. fejezete úgy rendelkezik, hogy „egy akár szerződéses, akár másmilyen jogviszonyból eredő választott bírósági megállapodás vagy választott bírósági ítélet, amely kereskedelmi jellegű, beleértve egy [az FAA 2. pontjában] leírt tranzakciót, szerződést vagy megállapodást, a külföldi választott bírósági 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 választott bírósági eljárásban részt vevő bármelyik fél az e fejezet szerint hatáskörrel rendelkező bírósághoz fordulhat a választott bírósági 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 érvényesítésének 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 választott bírósági 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 tovább 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. §

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

3. Az FTC fellépése a választott bírósági 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 választott bírósági eljárásban – azzal, hogy egy uniós egyén kérésére az uniós adatvédelmi hatóságok segítséget nyújthatnak kizárólag az értesítés megfogalmazásában, de az uniós adatvédelmi hatóságok nem férhetnek hozzá az ilyen választott bírósági eljárások betekintésre szánt vagy más anyagaihoz.

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

7. A választott bíráknak benyújtott anyagokat bizalmasan kezelik, és csak a választott bírósági eljárással kapcsolatban használják fel.

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

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

H. **Költségek**

A választott bíráknak indokolt lépéseket kell tenniük a választott bírósági eljárás költségeinek minimalizálása érdekében.

A vonatkozó jogszabályokkal összhangban a Kereskedelmi Minisztérium előmozdítja egy alap létrehozását, amelybe az adatvédelmi pajzsban részt vevő szervezeteknek – a szervezet mérete alapján – éves hozzájárulást kell fizetniük, amely fedezi a választott bírósági költségeket, beleértve a választott bírák díjazását az Európai Bizottsággal megállapodott felső összeghatár („plafon”) erejéig. Az alapot egy harmadik fél kezeli, amely rendszeresen beszámol az alap működéséről. Az éves felülvizsgálatkor a Kereskedelmi Minisztérium és az Európai Bizottság áttekinti az alap működését, beleértve a hozzájárulások összegének vagy a maximális díjnak a kiigazítását, és megvizsgálják többek között a választott bírósági eljárások számát, valamint költségeit és időzítését – kölcsönösen megállapodva abban, hogy az adatvédelmi pajzsban részt vevő szervezetek számára a díj ne jelentsen túlzott pénzügyi terhet. Az ügyvédi költségekre ez a rendelkezés nem vonatkozik, és azok e rendelkezés szerinti alapból nem fedezhetők.

II. MELLÉKLET

AZ EU-USA ADATVÉDELMI PAJZS KERETRENDSZER ELVEI KIADTA AZ EGYESÜLT ÁLLAMOK KERESKEDELMI MINISZTÉRIUMA

I. ÁTTEKINTÉS

1. Bár az Egyesült Államok és az Európai Unió közös célja az adatvédelem fokozása, az Egyesült Államok az Európai Uniótól eltérően közelíti meg az adatvédelmet. Az Egyesült Államok ágazati megközelítést használ, amely a jogalkotási eszközök, az előírások és az önszabályozás kombinációján alapszik. Figyelembe véve ezeket az eltéréseket, valamint annak érdekében, hogy az egyesült államokbeli szervezetek számára a személyes adatok Európai Unióból az Egyesült Államokba történő továbbításához megbízható mechanizmust biztosítsunk, miközben garantáljuk, hogy az érintett uniós polgárok továbbra is élvezzék az európai jogszabályok által előírt hatékony biztosítékokat és védelmet a személyes adataik kezelésével kapcsolatban, amikor azokat nem uniós országokba továbbítják, a Kereskedelmi Minisztérium hatósági jogkörében a nemzetközi kereskedelem támogatása, elősegítése és fejlesztése céljából kiadja ezeket az adatvédelmi pajzs elveket, köztük a kiegészítő elveket (együttesen: „az elvek") (15 U.S.C. § 1512). Az elveket az ágazattal és a nyilvánossággal konzultálva a kereskedelem, illetve az Egyesült Államok és az Európai Unió közötti nemzetközi kereskedelem megkönnyítése érdekében dolgozták ki. Az elveket csak az Európai Unióból személyes adatokat fogadó egyesült államokbeli szervezetek használatára szánták az adatvédelmi pajzs minősítés elnyerése, és ezáltal az Európai Bizottság megfelelőségi határozatának előnyeiből való részesülés céljából ([1]). Az elvek nem érintik a tagállamokban a személyes adatok kezelésére alkalmazandó 95/46/EK irányelv („az irányelv") végrehajtására szolgáló nemzeti rendelkezéseket. Az elvek az Egyesült Államok joga alapján egyébként alkalmazandó adatvédelmi kötelezettségeket sem korlátozzák.

2. A személyes adatok Unióból történő továbbítása érdekében az adatvédelmi pajzs alkalmazásának céljából a szervezeteknek maguknak kell tanúsítaniuk az elvek teljesítését a Kereskedelmi Minisztérium (vagy annak megbízottja) („a Minisztérium") számára. A szervezet döntése, hogy ilyen módon csatlakozik az adatvédelmi pajzshoz, teljesen önkéntes ugyan, de a hatékony megfelelés kötelező: annak a szervezetnek, amely önmaga tanúsítja a Minisztérium felé a megfelelését, és nyilvánosan bejelenti kötelezettségvállalását az elvek teljesítésére, teljes mértékben be kell tartania az elveket. Az adatvédelmi pajzshoz történő csatlakozás érdekében a szervezetnek a) a Szövetségi Kereskedelmi Bizottság (az „FTC"), a Közlekedési Minisztérium vagy más hatósági szerv vizsgálati és végrehajtási hatáskörébe kell tartoznia, amely hatékonyan biztosítja az elvek teljesítését *(jövőbeli melléklet az Európai Unió által elismert további USA hatósági szerveket is felsorolhat)*; b) nyilvánosan ki kell jelenteniük a kötelezettségvállalásukat, hogy betartják az elveket; c) nyilvánosságra kell hozniuk az adatvédelmi szabályzatukat ezekkel az elvekkel összhangban; és d) teljes körűen meg kell valósítaniuk azt. Ha a szervezet nem felel meg, akkor a Szövetségi Kereskedelmi Bizottságról szóló törvény tisztességtelen és megtévesztő cselekedetek tilalmáról szóló 5. szakasza (15 U.S.C. § 45(a)) vagy az ilyen cselekedetek tilalmáról szóló más törvény vagy rendelet alapján peresíthető.

3. A Kereskedelmi Minisztérium fenntart és közzétesz egy hiteles listát azokról az egyesült államokbeli szervezetekről, amelyek öntanúsítást végeztek a Minisztérium felé, és kötelezettséget vállaltak az elvek betartására (az „adatvédelmi pajzsban részt vevő szervezetek listája"). Az adatvédelmi pajzs előnyei biztosítottak attól a naptól fogva, amikor a Minisztérium az adatvédelmi pajzs listára felveszi a szervezetet. A Minisztérium törli a szervezetet az adatvédelmi pajzs listáról, ha önkéntesen kilép az adatvédelmi pajzs rendszerből, vagy nem teljesíti az éves ismételt tanúsítását a Minisztérium felé. A szervezet törlése az adatvédelmi pajzs listáról azt jelenti, hogy többé nem élvezi az Európai Bizottság megfelelőségi határozatának előnyeit személyes adatok Unióból történő fogadása tekintetében. A szervezetnek továbbra is alkalmaznia kell az elveket az adatvédelmi pajzsban történő részvétele során általa kapott személyes adatok tekintetében, és évente meg kell erősítenie a Minisztérium számára a kötelezettségvállalását, hogy így tesz, ameddig a birtokában van az információ; ellenkező esetben a szervezetnek vissza kell adnia vagy törölnie kell az információt, vagy más engedélyezett módon „megfelelő" védelmet kell biztosítania az információ számára. A Minisztérium azokat a szervezeteket is törli az adatvédelmi pajzs listáról, amelyek ismételten nem teljesítették az elveket; ezek a szervezetek nem jogosultak az adatvédelmi pajzs előnyökre és vissza kell adniuk vagy törölniük kell a személyes adatokat, amelyeket az adatvédelmi pajzs keretében kaptak.

4. A Minisztérium fenntart és közzétesz egy hiteles listát is azokról az egyesült államokbeli szervezetekről, amelyek előzőleg öntanúsítást végeztek a Minisztérium felé, majd törölték őket az adatvédelmi pajzs listáról. A Minisztérium egyértelmű figyelmeztetést ad, hogy ezek a szervezetek nem résztvevői az adatvédelmi pajzsnak; hogy az adatvédelmi pajzs listáról történt törlés azt jelenti, hogy az ilyen szervezet nem állíthatja, hogy megfelel az adatvédelmi pajzsnak és kerülnie kell minden olyan állítást vagy félrevezető gyakorlatot, amely arra utal, hogy résztvevője az adatvédelmi pajzsnak; és hogy az ilyen szervezetek már nem jogosultak az Európai Bizottság megfelelőségi határozatának előnyeire, amelynek révén az ilyen szervezetek személyes adatokat kaphatnának az Európai Uniótól. Az a szervezet, amely továbbra is azt állítja, hogy részt vesz az adatvédelmi pajzsban, vagy az adatvédelmi

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

pajzs listáról történt törlése után az adatvédelmi pajzzsal kapcsolatos egyéb megtévesztő nyilatkozatot tesz, az FTC, a Közlekedési Minisztérium vagy más végrehajtási hatóság végrehajtási intézkedést foganatosíthat vele szemben.

5. Az elvek betartása az alábbiak szerint korlátozható: a) a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben; b) törvény, kormányrendelet vagy az ítélkezési gyakorlat által, amelyek az elvekkel ellentétes kötelezettségeket vagy kifejezett felhatalmazásokat hoznak létre, feltéve, hogy az ilyen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nemteljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik; vagy c) ha az irányelv vagy a tagállami jogszabályok hatálya kivételeket vagy eltéréseket tesz lehetővé, feltéve, hogy az ilyen kivételeket vagy eltéréseket összehasonlítható esetekben alkalmazzák. Az adatvédelem erősítésének céljával összhangban a szervezeteknek törekedniük kell az elvek teljes mértékű és átlátható megvalósítására, beleértve adatvédelmi szabályzatukban annak megjelölését, hogy az elvek alól a fenti b) pontban engedélyezett kivételeket hol alkalmazzák rendszeresen. 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 adatvédelmi pajzshoz történt csatlakozásuk után az adatvédelmi pajzs keretében továbbított valamennyi személyes adatra kötelesek alkalmazni az elveket. Az a szervezet, amely az adatvédelmi pajzs előnyeit ki akarja terjeszteni az Európai Unióból továbbított, a munkaviszonnyal összefüggésben felhasználandó, humán erőforrással kapcsolatos személyes információra, köteles ezt jelezni, amikor öntanúsítást végez a Minisztérium felé, és meg kell felelnie az öntanúsításról szóló kiegészítő elvben meghatározott követelményeknek.

7. Az értelmezési kérdések és az elveknek való megfelelés, valamint az adatvédelmi pajzsban részt vevő szervezetek adatvédelmi szabályzatainak 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" és „személyes információk": olyan azonosított vagy azonosítható egyénre vonatkozó adatok, amelyek az irányelv hatálya alá tartoznak, és amelyeket valamely egyesült államokbeli szervezet az Európai Unióból kapott, és valamilyen formában rögzítette őket.

   b. „Személyes adatok kezelése": 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.

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

9. Az elvek hatálybalépésének napja az a nap, amikor az Európai Bizottság megfelelőségi határozatát véglegesen jóváhagyják.

II. ALAPELVEK

1. **Tájékoztatás**

   a. A szervezetnek tájékoztatnia kell az egyéneket az alábbiakról:

      i. a részvétele az adatvédelmi pajzsban, és egy linket vagy internetcímet kell biztosítania az adatvédelmi pajzs listához,

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

iii. a kötelezettségvállalása, hogy alkalmazza az elveket valamennyi személyes adatra, amelyet az Európai Uniótól az adatvédelmi pajzs keretében 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, amelyek részére felfedi a személyes adatokat, és az adatok felfedésének célja,

vii. az egyének személyes adataikhoz való hozzáféréshez való joga,

viii. a szervezet által az egyének számára biztosított lehetőségek és eszközök a személyes adataik használatának vagy felfedésének korlátozására,

ix. a panaszok kezelésére és az egyének számára ingyenes jogorvoslat biztosítására kijelölt független vitarendező szerv, valamint annak meghatározása, hogy az: (1) az adatvédelmi hatóságok által létrehozott testület, (2) egy Európai Unióban székhellyel rendelkező alternatív vitarendezési szolgáltató, vagy (3) egy 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 választott bírósági határozatért folyamodjon,

xii. állami hatóságok jogszerű kérésére személyes adatok átadásának az előírása, beleértve a nemzetbiztonsági vagy bűnüldözési előírások teljesítését, és

xiii. a felelőssége harmadik fél részére történő adattovábbítás esetén.

b. Ezt a tájékoztatást világos és érthető megfogalmazásban kell megadni, az első alkalommal akkor, amikor az egyéneket felkérik arra, hogy a szervezet részére személyes információkat szolgáltasson, vagy azt követően a lehető legrövidebb időn belül, de minden esetben azt megelőzően, hogy a szervezet az ilyen információt más célra használná fel, mint amelyre 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 egyéneknek, hogy személyes adataikat 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 gyakorolására.

b. Az előző bekezdéstől eltérően nem szükséges választási lehetőséget biztosítani, amikor az adatközlés a feladato(ka)t a szervezet nevében és útmutatásai alapján 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, ha az információt i. harmadik fél számára átadják, vagy ii. a gyűjtés eredeti céljától, illetve az egyén által a választási lehetőségével élve a későbbiekben engedélyezett céltól eltérő célra használják fel. Ezenkívül a szervezetnek különleges adatként kell kezelnie minden olyan, harmadik féltől kapott információt, amelyet a harmadik fél érzékeny (különleges) adatként határoz meg és kezel.

3. **Elszámoltathatóság harmadik fél részére történő adattovábbításért**

a. Az információ adatkezelőként eljáró harmadik fél számára történő továbbításához a szervezeteknek alkalmazniuk kell az értesítés 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 célokra 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 felel meg ennek a kötelezettségnek. A szerződés úgy rendelkezik, hogy ilyen megállapítás esetén a harmadik fél adatkezelő megszünteti az adatkezelést vagy egyéb ésszerű és megfelelő lépéseket tesz a védelem helyreállítására..

b. A személyes adatok adatkezelőként eljáró harmadik fél számára történő továbbításához a szervezeteknek: i. az ilyen adatokat csak korlátozott és meghatározott célokra szabad átadniuk; ii. meg kell bizonyosodniuk arról, hogy a közvetítő köteles legalább olyan szintű adatvédelmet biztosítani, mint amit az elvek előírnak; iii. indokolt és megfelelő lépéseket kell tenniük annak biztosítására, hogy a közvetítő valóban a szervezet elvek szerinti kötelezettségeivel összhangban kezeli a továbbított személyes adatokat; iv. kötelezniük kell a megbízottat, hogy értesítse a szervezetet, ha megállapítja, hogy nem felel meg annak kötelezettségének, hogy az elvekben előírttal azonos szintű védelmet biztosítsa; v. kérésre – többek között iv. francia bekezdés szerinti esetben – indokolt és megfelelő lépéseket kell tenniük a jogosulatlan adatkezelés megszüntetése és az eredeti állapot helyreállítása érdekében; valamint 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 információt az elvesztéstől, a visszaéléstől és a jogtalan hozzáféréstől, a nyilvánosságra hozataltól, a megváltoztatástól és a megsemmisítéstől, megfelelően figyelembe véve a kezeléssel járó kockázatokat és a személyes adatok természetét.

5. **Adatok sértetlensége és célhoz kötöttség**

a. Az elvekkel összhangban a személyes adatoknak olyan információkra kell korlátozódniuk, amelyek a kezelés célja szempontjából relevánsak ([1]). 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 annyi ideig kell teljesítenie az elveket, amíg megőrzi az ilyen információkat.

b. Az adatok kizárólag addig őrizhetők meg az egyént azonosító vagy annak azonosítására alkalmas formában ([2]), amíg ez az adatkezelés az 5. pont a. alpontja szerinti célját szolgálja. Ez a kötelezettség nem akadályozza meg, hogy a szervezet hosszabb időszakokon keresztül kezeljen személyes adatokat, amennyiben a szóban forgó adatkezelés ésszerűen szolgálja a közérdekű archiválás, újságírás, irodalom és művészet, tudományos és történeti kutatás, és statisztikai elemzés céljait. Ilyen esetekben az érintett adatkezelés egyéb elvek és a keretrendszer egyéb rendelkezéseinek hatálya alá tartozik. A szervezeteknek ésszerű és megfelelő intézkedéseket kell hozniuk, 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 információk 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.

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

([2]) E tekintetben egy egyén akkor „azonosítható”, ha – tekintettel azokra az azonosítási eszközökre, amelyeknek az alkalmazása ésszerűen 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 ésszerűen azonosítani tudná az adott egyént, ha hozzáférne az adatokhoz.

7. **Jogorvoslat, végrehajtás és felelősség**

a. A hatékony adatvédelemnek magában kell foglalnia az elvek teljesítését biztosító erős mechanizmusokat, a jogorvoslati jogot az elvek nemteljesítése által érintett egyének számára, valamint a szervezetre vonatkozó következményeket, amikor az elveket nem követi. Az ilyen mechanizmusoknak minimumkövetelményként tartalmazniuk kell:

i. könnyen hozzáférhető független eljárási mechanizmusokat, amelyekkel minden egyes személy panaszait és vitáit az egyén számára ingyenesen és az elvekre hivatkozva meg lehet vizsgálni és gyorsan meg lehet oldani, 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 teljesítés biztosítása érdekében a szankcióknak kellőképpen szigorúaknak kell lenniük.

b. A szervezetek és a kiválasztott független jogorvoslati mechanizmusok azonnal válaszolnak a Minisztériumnak az adatvédelmi pajzzsal kapcsolatos megkereséseire és információkéréseire. Valamennyi szervezetnek gyorsan kell válaszolnia az EU 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.

c. A szervezetek kötelesek a panaszok választott bírósági rendezésére és az I. mellékletben meghatározott feltételek követésére, amennyiben egy egyén kötelező erejű választott bírósági határozatot kért – értesítést küldve az érintett szervezetnek, követve az I. mellékletben meghatározott eljárásokat, és betartva az ott meghatározott feltételeket.

d. Harmadik fél részére történő adattovábbítás esetén az adatvédelmi pajzsban részt vevő szervezet felelős az általa az adatvédelmi pajzs alapján kapott és ezt követően a nevében tevékenykedő harmadik fél megbízottnak átadott személyes adatok kezeléséért. Az adatvédelmi pajzsban részt vevő szervezet marad a felelős az elvek alapján, amennyiben a megbízottja az ilyen személyes adatokat nem az elveknek megfelelően kezeli, kivéve, ha a szervezet bizonyítja, hogy nem felelős a károkozást előidéző eseményért.

e. Ha az adatvédelmi pajzsban részt vevő szervezet nemteljesítés miatt az FTC vagy egy bíróság végzésének a hatálya alá kerül, a szervezetnek közzé kell tennie az FTC számára benyújtott megfelelési vagy értékelési jelentés adatvédelmi pajzsra vonatkozó minden részét, amennyiben az nem ellentétes a titoktartási előírásokkal. A Minisztérium egy kijelölt kapcsolattartó pontot létesített az adatvédelmi hatóságok számára az adatvédelmi pajzsban részt vevő szervezetek megfelelőségi problémáinak kezelésére. Az FTC 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 (önkéntes részvétel) beszerezni a különleges adatokra vonatkozóan, ha az adatkezelés:

i. az érintett vagy más személy létfontosságú érdekében áll;

ii. jogszerű követelések vagy a védelem kialakításához 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 szervezet tagjaira vagy olyan személyekre vonatkozik, akik a céljaival összefüggésben rendszeres kapcsolatban állnak az adott szervezettel, és az adatokat az érintettek beleegyezése nélkül nem adják át harmadik félnek;

v. a szervezetnek a munkajog területén fennálló kötelezettségei végrehajtása céljából szükséges; vagy

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

2. **Újságírói kivételek**

a) Tekintve az Egyesült Államokban a sajtószabadság alkotmányos védelmét és az irányelv szerinti mentességet az újságírói anyagra vonatkozóan, amennyiben az Egyesült Államok alkotmányának első kiegészítésében szereplő, a 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 televízióműsorhoz vagy újságírói anyag nyilvános közlésének más formájához összegyűjtött személyes adatokra – akár felhasználják azokat, akár nem –, valamint a korábban közzétett anyagban talált, médiaarchívumból terjesztett információkra az adatvédelmi pajzs elvek követelményei nem vonatkoznak.

3. **Mögöttes felelősség**

a) Az internetszolgáltatók, a távközlési szolgáltatók és más szervezetek nem felelősek az adatvédelmi pajzs elvek alapján, amikor más szervezet nevében csupán közlik, továbbítják, átirányítják vagy tárolják az információt. Amint maga az irányelv, az adatvédelmi pajzs sem hoz létre mögöttes felelősséget. Amennyiben a szervezet a harmadik fél által továbbított adatok tekintetében csupán továbbító csatornaként jár el, és nem határozza meg e személyes adatok kezelésének céljait és eszközeit, nem felelős.

4. **Átvilágítás és auditálás végzése**

a) A könyvvizsgálók és befektetési bankárok tevékenysége az egyén beleegyezése vagy tudta nélküli személyesadat-kezeléssel is járhat. Ezt lehetővé teszik az értesítésre, a választási lehetőségre és a hozzáférésre vonatkozó elvek az alább leírt körülmények között.

b) A nyilvánosan működő részvénytársaságok és a zártkörű részvénytársaságok – az adatvédelmi pajzsban részt vevő szervezeteket is beleértve – rendszeres auditáláson esnek át. Az ilyen auditálásokat – különösen az esetleges törvénysértést vizsgálókat – veszélyezteti, ha idő előtt közlik őket. Ugyanígy a lehetséges összeolvadásban vagy felvásárlásban érintett, adatvédelmi pajzsban részt vevő szervezetnek átvilágítást kell végez(tet)nie. 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 csak a törvényes vagy közérdekű követelményeknek való megfeleléshez szükséges mértékben és időtartamban kezelhetnek információt az egyén tudta nélkül, 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 összefüggő titoktartás szükségességét.

5. **Az adatvédelmi hatóságok szerepe**

a) A szervezetek az uniós adatvédelmi hatóságokkal folytatott együttműködésre vonatkozó kötelezettségvállalásukat az alábbiakban leírt módon valósítják meg. Az adatvédelmi pajzs alapján az EU-ból személyes adatokat fogadó egyesült államokbeli szervezeteknek kötelezettséget kell vállalniuk az adatvédelmi pajzs elveinek teljesítését biztosító hatékony mechanizmusok alkalmazására. Konkrétan a jogorvoslati, végrehajtási és felelősségi elvben meghatározottak szerint a részt vevő szervezeteknek az alábbiakat kell biztosítaniuk: (a) i. jogorvoslati lehetőség azon egyének számára, akikre az adatok vonatkoznak; (a) ii. nyomonkövetési eljárások annak ellenőrzésére, hogy az általuk az adatvédelmi gyakorlataikról készített tanúsítványok és állítások helytállóak-e; (a) iii. az elvek nemteljesítéséből eredő problémák orvoslására vonatkozó kötelezettségek és az ilyen szervezetekre vonatkozó következmények. A szervezet eleget tehet a jogorvoslati, végrehajtási és felelősségi elv (a) pontja i. és iii. francia bekezdésének, ha elfogadja az adatvédelmi hatóságokkal történő együttműködésre vonatkozóan itt meghatározott előírásokat.

b) A szervezet kötelezi magát az adatvédelmi hatóságokkal történő együttműködésre azáltal, hogy az adatvédelmi pajzs öntanúsítási beadványában bejelenti a Kereskedelmi Minisztériumnak (*lásd:* öntanúsításról szóló kiegészítő elv), hogy a szervezet:

i. elhatározza, hogy az adatvédelmi hatóságokkal történő együttműködés révén eleget tesz az adatvédelmi pajzs jogorvoslati, végrehajtási és felelősségi elv (a) pontja i. és iii. francia bekezdésében meghatározott követelménynek;

ii. együttműködik az adatvédelmi hatóságokkal az adatvédelmi pajzs alapján benyújtott panaszok kivizsgálásában és megoldásában; és

iii. betartja az adatvédelmi hatóságoktól kapott valamennyi ajánlást, amennyiben az adatvédelmi hatóságok úgy látják, hogy a szervezetnek különleges intézkedést kell hoznia az adatvédelmi pajzs elveinek 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 ajánlását az adatvédelmi hatóságok európai uniós szinten létrehozott nem hivatalos testülete kézbesíti, amely *többek között* segíti az összehangolt és összefüggő megközelítés biztosítását.

2. A testület ajánlást ad az Egyesült Államok egyénektől származó megoldatlan panaszokkal kapcsolatban érintett szervezeteinek az EU-ból az adatvédelmi pajzs alapján továbbított személyes információk kezelésére. Ez az ajánlás az adatvédelmi pajzs elvek helyes alkalmazását kívánja 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 adatvédelmi pajzs céljainak megfelelően elkötelezték magukat az adatvédelmi hatóságokkal történő együttműködés mellett, miközben ösztönzi és szükség esetén első fokon segíti az ilyen egyének számára a belső panaszkezelési eljárások igénybevételét, amelyeket a szervezet nyújtani tud.

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 elfogadja 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 jogviták megoldására ezt a lehetőséget választó szervezeteknek vállalniuk kell, hogy betartják az adatvédelmi hatóságok ajánlását. Ha a szervezet az átadástól 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 a Szövetségi Kereskedelmi Bizottság, a Közlekedési Minisztérium vagy az Egyesült Államok más szövetségi vagy állami testülete elé viszi, 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 Kereskedelmi Minisztériumot annak érdekében, hogy az adatvédelmi pajzs listát megfelelően módosíthassák. Az adatvédelmi hatóságokkal történő együttműködési kötelezettségvállalás bármilyen nemteljesítése, valamint az adatvédelmi pajzs elvek be nem tartása a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza vagy más hasonló törvény alapján megtévesztő gyakorlatként perelhető lesz.

d) Ha a szervezet az kívánja, hogy az adatvédelmi pajzs 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 adott esetben vállalniuk kell a szükséges fordítási költségeket, amelyek a testületnél a kérelmek elbírálásából vagy a szervezetekkel szemben felmerülő panaszokból adódnak. Az éves díj nem haladja meg az 500 USD-t, és kisebb vállalkozások esetében ennél kevesebb lesz.

6. **Öntanúsítás**

a) Az adatvédelmi pajzs előnyök attól a naptól fogva biztosítottak, hogy a Minisztérium – miután megállapította, hogy a beadvány hiánytalan – a szervezet öntanúsítási beadványát feltette az adatvédelmi pajzs listára.

b) Az adatvédelmi pajzsra vonatkozó öntanúsításhoz a szervezet az adatvédelmi pajzshoz csatlakozó szervezet nevében eljáró vállalkozás tisztségviselője által aláírt levelet küldhet a Minisztériumnak, amely legalább a következő adatokat tartalmazza:

i. a szervezet neve, levélcíme, e-mail címe, telefon- és telefaxszámai;

ii. a szervezet tevékenységeinek leírása, tekintettel az EU-ból kapott személyes adatokra; és

iii. a szervezet 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;

2. a bevezetés tényleges időpontja;

3. a panaszokat, hozzáférési kérelmeket és az adatvédelmi pajzzsal kapcsolatban felmerülő bármilyen kérdést kezelő kapcsolattartó iroda;

4. 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);

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

6. az ellenőrzés módszere (*pl.* házon belül, harmadik fél által) (*lásd* az ellenőrzésről szóló kiegészítő elvet); és

7. a független jogorvoslati mechanizmus, amely a megoldatlan panaszok kivizsgálására rendelkezésre áll.

c) Amennyiben a szervezet az adatvédelmi pajzs 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 öntanúsítási beadványában, és ki kell jelentenie az EU érintett hatóságával vagy hatóságaival való együttműködésre vonatkozó kötelezettségvállalását a humánerőforrás-adatokra és az adatvédelmi hatóságokra vonatkozó kiegészítő elvnek megfelelően, 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.

d) A Minisztérium adatvédelmi pajzs listát tart fenn azokról a szervezetekről, amelyek öntanúsítást tartalmazó beadványt nyújtottak be, ezáltal biztosítva az adatvédelmi pajzs előnyök hozzáférhetőségét, és az éves ismételt öntanúsítások és a vitarendezésről és végrehajtásról szóló kiegészítő elv szerint kapott értesítések alapján frissíti ezt a listát Az ilyen öntanúsításokat legalább évente kell benyújtani; ellenkező esetben a szervezetet törlik az adatvédelmi pajzs listáról, és az adatvédelmi pajzs előnyök már nem lesznek biztosítottak számára. Mind az adatvédelmi pajzs listát, mind a szervezetek öntanúsítási beadványait nyilvánosan közzéteszik. Minden olyan szervezetnek, amelyet a Minisztérium felvett az adatvédelmi pajzs listára, az erre vonatkozóan közzétett adatvédelem-politikai nyilatkozatában szintén ki kell jelentenie, hogy betartja az adatvédelmi pajzs elveket. Ha

a szervezet adatvédelmi szabályzata online elérhető, tartalmaznia kell a Minisztérium adatvédelmi pajzs honlapjára mutató hiperlinket, valamint a megoldatlan panaszok kivizsgálására rendelkezésre álló független jogorvoslati mechanizmus honlapjára vagy panaszbenyújtási formanyomtatványára mutató hiperlinket.

e) Az adatvédelmi elvek közvetlenül a tanúsítás után már alkalmazandók. Mivel az elvek harmadik felekkel folytatott kereskedelmi kapcsolatokat érintenek, az adatvédelmi pajzs keretrendszerben a keretrendszer hatálybalépését követő első két hónap során tanúsító szervezeteknek a harmadik felekkel fennálló kereskedelmi kapcsolataikat a lehető legrövidebb időn belül, de legkésőbb kilenc hónappal azt követően, hogy tanúsították az adatvédelmi pajzs megfelelésüket, összhangba kell hozniuk a harmadik fél részére történő adattovábbításokért való elszámoltathatóságra vonatkozó elvvel. Az átmeneti időszak során, amikor a szervezetek harmadik felek számára adatokat adnak át, i. alkalmazniuk kell az értesítési és választási lehetőség elveket, és ii. amennyiben személyes adatokat továbbítanak megbízottként működő harmadik felek számára, meg kell bizonyosodniuk arról, hogy a megbízott köteles legalább ugyanolyan szintű védelmet nyújtani, mint amelyet az elvek előírnak.

f) A szervezetnek alkalmaznia kell az elveket valamennyi személyes adatra, amelyet az Európai Unióból az adatvédelmi pajzs keretében kapott. Az adatvédelmi pajzs elvek betartására vonatkozó kötelezettségvállalást nem kötik időkorláthoz az azon idő alatt fogadott személyes adatok tekintetében, amíg a szervezet élvezi az adatvédelmi pajzs 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 elhagyja az adatvédelmi pajzsot. Annak a szervezetnek, amely kilép az adatvédelmi pajzsból, 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 információt számára (például olyan szerződés alkalmazásával, amely teljes körűen tükrözi a megfelelő általános szerződési feltételeket, amelyeket az Európai Bizottság elfogadott); ellenkező esetben a szervezetnek vissza kell küldenie vagy törölnie kell az információkat. Annak a szervezetnek, amely kilép az adatvédelmi pajzsból, törölnie kell a vonatkozó adatvédelmi szabályzatából az adatvédelmi pajzsra való hivatkozást, amely arra utal, hogy a szervezet továbbra is aktívan részt vesz az adatvédelmi pajzsban, és jogosult annak előnyeire.

g) Annak a szervezetnek, amely összeolvadás vagy felvásárlás eredményeként megszűnik önálló jogi személyként létezni, előzetesen értesítenie kell a Minisztériumot erről. Az értesítésben jeleznie kell azt is, hogy a felvásárló jogi személy vagy az összeolvadás eredményeként létrejött jogi személy i. továbbra is betartja az adatvédelmi pajzs elveket a felvásárlást vagy összeolvadást szabályozó törvény rendelkezése alapján; vagy ii. úgy dönt, hogy önmaga tanúsítja az adatvédelmi pajzs elvek betartását vagy helyettük más biztosítékokat vezet be, például írásos megállapodást, amely biztosítja az adatvédelmi pajzs elvek betartását. Amennyiben sem az i., sem a ii. francia bekezdés nem alkalmazandó, az adatvédelmi pajzs keretében megszerzett valamennyi személyes adatot haladéktalanul törölni kell.

h) Annak a szervezetnek, amely bármely okból kilép az adatvédelmi pajzsból, törölnie kell minden olyan állítást, amely arra utal, hogy a szervezet továbbra is részt vesz az adatvédelmi pajzsban, vagy jogosult az adatvédelmi pajzs előnyeire. Az EU-USA adatvédelmi pajzs tanúsító védjegyet, amennyiben használták, szintén törölni kell. Ha a szervezet hamisan tájékoztatja a közvéleményt az adatvédelmi pajzs elvek betartásával kapcsolatban, a szervezet az FTC 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 adatvédelmi pajzs szerinti adatvédelmi gyakorlatukról készítenek, megfelelnek-e a valóságnak, és megvalósításuk a tényállításokkal és az adatvédelmi pajzs 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) Az önértékelési megközelítés szerint az ilyen ellenőrzésnek jeleznie kell, hogy a szervezetnek az EU-ból fogadott személyes információkra vonatkozó, közzétett adatvédelmi szabályzata pontos, átfogó, jól látható módon bemutatott, teljes mértékben végrehajtott és hozzáférhető. Azt is jeleznie kell, hogy az adatvédelmi szabályzata megfelel az adatvédelmi pajzs elveinek; hogy az egyéneket tájékoztatják a panaszok kezelésére szolgáló bármilyen belső szabályzatról, valamint azokról a független mechanizmusokról, amelyeken keresztül panaszt tehetnek; hogy tartalmaz az alkalmazottak oktatására vonatkozó eljárást a végrehajtást illetően, valamint fegyelmi eljárásokat az adatvédelmi szabályzat követésének elmulasztása esetére; és hogy tartalmaz belső eljárásokat a fentiek teljesítésének időszakos tárgyilagos vizsgálatára. Az önértékelést hitelesítő nyilatkozatot

a vállalkozás egy tisztségviselőjének vagy a szervezet más meghatalmazottjának kell aláírnia legalább évente egyszer, és az egyének kérelmére, illetve vizsgálattal vagy a teljesítés elmulasztására vonatkozó panasszal összefüggésben hozzáférhetővé kell tennie.

d) Amennyiben a szervezet a külső megfelelőségi felülvizsgálatot választja, az ilyen felülvizsgálati eljárásnak be kell mutatnia, hogy a szervezetnek az EU-ból fogadott személyes adatokra vonatkozó adatvédelmi szabályzata összhangban van az adatvédelmi pajzs elvekkel, azoknak megfelel, valamint az egyéneket tájékoztatták azokról a mechanizmusokról, amelyeken keresztül panaszt tehetnek. A felülvizsgálat módszerei korlátlanul magukban foglalhatják az ellenőrzést, szúrópróbaszerű felülvizsgálatokat, „csapdák" használatát, vagy adott esetben technikai eszközök használatát. A külső megfelelőségi felülvizsgálat sikeres befejezését 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 egy vizsgálattal vagy a teljesítéssel kapcsolatos panasszal összefüggésben rendelkezésre kell bocsátani.

e) A szervezeteknek meg kell őrizniük az adatvédelmi pajzs adatvédelmi gyakorlatuk végrehajtásáról szóló nyilvántartásaikat, és kérésre, vizsgálattal vagy a teljesítés elmulasztására vonatkozó 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 adatvédelmi pajzs elvek alapján a hozzáférési jog az adatvédelem alapvető eleme. Különösen azt teszi lehetővé az egyének számára, hogy ellenőrizzék a róluk tárolt információ 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 ([1]);

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

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. 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 információ védelemre szorul, és könnyen elkülöníthető más, a hozzáférés iránti kérelem tárgyát képező személyes információtól, 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 kapcsolattartási 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 a hozzáférés biztosításának terhe vagy költsége nem állna arányban az adott esetben az egyén adatvédelmi jogának a kockázatával. A költség és a teher fontos tényezők, amelyeket figyelembe kell venni, de nem meghatározó tényezők annak megállapításában, hogy a hozzáférés biztosítása indokolt-e.

([1]) A szervezetnek válaszolnia kell az egyén arra vonatkozó kéréseire, hogy mi az adatfeldolgozás célja, melyek az érintett személyesadat-kategóriák, a címzettek vagy a címzettek kategóriái, akik felé az adatokat továbbítják.

ii. Ha például a személyes adatot olyan döntésekre használják, amelyek jelentős hatással vannak az egyénre (*pl.* fontos juttatások megtagadása vagy megadása, mint például biztosítás, jelzáloghitel vagy állás), akkor – e kiegészítő elvek más rendelkezéseivel összhangban – a szervezetnek akkor is fel kell fednie az információt, ha ez viszonylag bonyolult vagy költséges. Ha a kért információ 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 információkhoz.

c) Bizalmas kereskedelmi 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.

ii. Amennyiben a bizalmas kereskedelmi információ könnyen elkülöníthető más, hozzáférés iránti kérelem tárgyát képező személyes információktól, 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 az egyén számára történő megfelelő személyes adatok 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. Mivel 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 az irányelv szerint, a szervezet korlátozhatja az információhoz való hozzáférést, amennyiben a megismerése valószínűleg fontos közérdekek – például nemzetbiztonság, honvédelem, közbiztonság – védelmével ütközne. Ezen túlmenően, amennyiben a személyes információt 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 biztos irányítással összefüggő folyamatos ellenőrzéssel, felülvizsgálattal vagy szabályozó funkciókkal összefüggésben vagy a szervezet részvételével a jövőben vagy jelenleg folyamatban levő tárgyalások során szükséges titkosság hátrányos befolyásolása.

ii. A kivételre igényt tartó szervezetnek igazolnia kell annak alkalmazhatóságát, 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 szervezet 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 hozzáférés iránti kérelmek

A szervezetek ésszerű 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

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

i) Válaszadási határidő

A szervezetnek ésszerű időn belül, ésszerű 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 adatvédelmi pajzs adatköre

i. Amennyiben az EU-ban letelepedett szervezet (korábbi vagy jelenlegi) munkavállalóiról a munkaviszonnyal kapcsolatban gyűjtött személyes információkat továbbítja az adatvédelmi pajzsban részt vevő anya-, leányvállalatnak vagy hozzá nem tartozó szolgáltatónak az Egyesült Államokba, a továbbítás élvezi az adatvédelmi pajzs előnyeit. Ilyen esetekben az információ gyűjtése és a továbbítást megelőző kezelése annak az uniós országnak a nemzeti joga alá tartozik, ahol azt összegyűjtötték, és a továbbításra vonatkozó feltételeket és korlátozásokat azon jog szerint kell figyelembe venni.

ii. Az adatvédelmi pajzs 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) Az értesítési és választási lehetőség elvek alkalmazása

i. Bármely egyesült államokbeli szervezet, amely az adatvédelmi pajzs alapján az Európai Unióból munkavállalókra vonatkozó információt kapott, azt csak az értesítési és választási lehetőség elvvel összhangban fedheti fel harmadik fél számára vagy használhatja fel különböző célokra. Ha például egy szervezet a munkaviszonyon keresztül összegyűjtött személyes információt nem munkaviszonnyal összefüggő célokra – például marketingértesítésekre – szándékozik felhasználni, akkor az egyesült államokbeli szervezetnek az előírt választási lehetőséget kell biztosítania az érintett magánszemélyek számára, mielőtt így tenne, kivéve, ha azok már engedélyezték az információ 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 alkalmak korlátozására vagy az ilyen alkalmazottakkal szemben bármilyen megtorló intézkedés alkalmazására felhasználni.

ii. Meg kell jegyezni, hogy egyes, a néhány EU tagállamból történő továbbítás tekintetében általánosan alkalmazható feltételek kizárhatják az ilyen információ felhasználását más célokra, még az EU-n kívüli továbbítást követően is, és az ilyen feltételeket tiszteletben kell tartani.

iii. Ezen túlmenően, a munkaadóknak ésszerű erőfeszítéseket kell tenniük, hogy igazodjanak a munkavállalók adatvédelmi érdekeihez. Ez jelentheti például a személyes adatokhoz való hozzáférés korlátozását, bizonyos adatok névtelenítését, vagy kódok vagy álnevek hozzárendelését, ha az adott igazgatási 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 szervezetnek nem szükséges felajánlania az értesítést és a választási lehetőséget.

c) A hozzáférési elv alkalmazása

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 rendeleteknek kell megfelelniük, és biztosítaniuk kell, hogy az európai unióbeli alkalmazottak a saját országaik jogszabályaiban előírtaknak megfelelően hozzáférjenek az ilyen információhoz, az adatfeldolgozás és a tárolás helyszínétől függetlenül. Az adatvédelmi pajzs megköveteli, hogy az ilyen adatokat az Egyesült Államokban kezelő szervezet együttműködjön az ilyen hozzáférés biztosításában vagy közvetlenül, vagy az EU-beli munkaadón keresztül.

d) Végrehajtás

i. Amennyiben a személyes információt 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 az alkalmazott munkahelye szerint illetékes állami vagy nemzeti adatvédelmi vagy munkaügyi hatósághoz kell irányítani őket. Ez magában foglalja azokat az eseteket is, amikor a személyes dat vélelmezett helytelen kezelésének a felelőssége azé az egyesült államokbeli szervezeté, amely az információt a munkaadótól kapta, ilyenformán az adatvédelmi pajzs 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 teljesítésének.

ii. Az Egyesült Államokban az adatvédelmi pajzsban részt vevő szervezetnek, amely az Európai Unióból továbbított európai unióbeli humánerőforrás-adatokat használ fel a munkaviszonnyal összefüggésben, és amely az ilyen adattovábbításokat az adatvédelmi pajzs keretébe kívánja helyezni, ezért el kell köteleznie magát az EU illetékes hatóságai által elvégzett vizsgálatokban való együttműködésre, valamint azok ajánlásainak követésére az ilyen esetekben.

e) Az elszámoltathatóság harmadik fél részére történő adattovábbításért elv alkalmazása

Az adatvédelmi pajzsban részt vevő szervezet foglalkoztatással kapcsolatos, az adatvédelmi pajzs keretében 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 elszámoltathatóság harmadik fél részére történő adattovábbításért elv, amennyiben az adatvédelmi pajzsban részt vevő szervezet betartotta az értesítés és a választási lehetőség elvét.

10. **Harmadik fél részére történő adattovábbításra 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 adatkezelő adatvédelmi pajzsban való részvételére.

ii. Az Európai Unióban 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 adatkezelő részt vesz-e az adatvédelmi pajzsban. A szerződés célja annak biztosítása, hogy az adatot kezelő személy:

1. kizárólag az adatkezelő utasítása alapján jár el;

2. megfelelő technikai és szervezési intézkedéseket tesz a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, és tudatában van, hogy a harmadik fél részére történő adattovábbítás engedélyezett-e; valamint

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

iii. Mivel az adatvédelmi pajzsban részt vevők megfelelő védelmet biztosítanak, az adatvédelmi pajzsban részt vevőkkel pusztán adatkezelésre vonatkozóan kötött szerződések előzetes engedélyezésére nincs szükség (vagy az ilyen engedélyt az uniós tagállamok automatikusan megadják), ami egyébként az adatvédelmi pajzsban részt nem vevő vagy megfelelő védelmet másként nem biztosító adatátvevőkkel való szerződések esetében szükséges lenne.

b) Adattovábbítás vállalatok vagy jogi személyek ellenőrzött csoportján belül

Amikor személyes adatokat továbbítanak vállalatok vagy jogi személyek ellenőrzött csoportján belül, nem mindig szükséges szerződés az elszámoltathatóság harmadik fél részére történő adattovábbításért elv 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 védelmének a folytonosságát az adatvédelmi pajzs elvei szerint. Ilyen adattovábbítás esetén az adatvédelmi pajzsban részt vevő szervezet marad a felelős az adatvédelmi pajzs elveinek teljesítéséért.

c) Adatkezelők közötti adattovábbítás

Adatkezelők közötti adattovábbítás esetén a címzett adatkezelőnek egy adatvédelmi pajzsban részt vevő szervezetnek kell lennie, vagy rendelkeznie kell független jogorvoslati mechanizmussal. Az adatvédelmi pajzsban részt vevő szervezetnek szerződést kell kötnie a címzett harmadik fél adatkezelővel, amely ugyanolyan szintű védelemről rendelkezik, mint amilyen az adatvédelmi pajzs keretében rendelkezésre áll, ide nem értve azt az előírást, hogy a harmadik fél adatkezelő egy adatvédelmi pajzsban 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 adatvédelmi pajzs végrehajtására vonatkozó követelményeket. Az elv a) pontja ii. francia bekezdése szerinti követelményeknek való megfelelést a hitelesítésről szóló kiegészítő elv határozza meg. Ez a kiegészítő elv az a) pont i. és iii. francia bekezdésével 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 adatvédelmi programok teljesítése, amelyek az adatvédelmi pajzs elveket belefoglalják szabályaikba, és a jogorvoslati, végrehajtási és felelősségi elvben leírt típusú, hatékony végrehajtási mechanizmusokat tartalmaznak; ii. alkalmazkodás a törvényi vagy szabályozó felügyeleti hatóságokhoz, amelyek rendelkeznek az egyedi panaszok kezeléséről és a jogviták rendezéséről; vagy iii. kötelezettségvállalás az Európai Unióban lévő adatvédelmi hatóságokkal vagy meghatalmazott képviselőikkel való együttműködésre.

b) E felsorolás szándéka a szemléltetés, nem a korlátozás. A magánszektor a végrehajtás biztosítására további mechanizmusokat is tervezhet, 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 arra vonatkozó követelményeken túl alkalmazandók, hogy az önszabályozó törekvéseknek a Szövetségi Kereskedelmi Bizottságról szóló törvény tisztességtelen vagy megtévesztő cselekményeket tiltó 5. cikke vagy más olyan jogszabály vagy rendelkezés alapján végrehajthatóknak kell lenniük, amely tiltja az ilyen cselekményeket.

c) Az adatvédelmi pajzs 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 adatvédelmi pajzsról. Ezenkívül valamennyi szervezetnek gyorsan kell válaszolnia az adatvédelmi hatóságok által a Minisztériumon keresztül az elvek betartására vonatkozóan benyújtott panaszokra. A válaszban szerepelni 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. A fogyasztókat arra kell ösztönözni, hogy szükség esetén még azelőtt nyújtsanak be panaszt az adott szervezettel kapcsolatban, hogy független jogorvoslati mechanizmust vennének igénybe. A szervezeteknek a panasz kézhezvételétől számított 45 napon belül válaszolniuk kell a fogyasztónak. A jogorvoslati mechanizmus függetlensége olyan ténykérdés, amely különösen elfogulatlansággal, átlátható összetétellel és finanszírozással, valamint hitelesített nyomon követő nyilvántartással mutatható be. A jogorvoslati, végrehajtási és felelősségi elvben megkövetelteknek megfelelően, a magánszemélyek számára rendelkezésre álló jogorvoslatnak könnyen hozzáférhetőnek és az egyének számára ingyenesnek kell lennie. A jogvitát eldöntő szerveknek a magánszemélyektől 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 szervezet részéről, de az ilyen követelményeknek átláthatóaknak és igazoltaknak 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 törvényes panaszok kivizsgálására vonatkozó kötelezettségvállalást. Ezen túlmenően, a jogorvoslati mechanizmusoknak az egyének számára a panasz benyújtásakor teljes és könnyen elérhető információt kell szolgáltatniuk a jogvitákat eldöntő eljárás működéséről. Az ilyen információnak értesítést kell tartalmaznia a mechanizmus adatvédelmi gyakorlatairól, összhangban az adatvédelmi pajzs elvekkel. Szintén együtt kell működniük az eszközök – mint például formanyomtatványok a panaszokhoz – kidolgozásában, a panaszrendezési eljárás megkönnyítése érdekében.

ii. A független jogorvoslati mechanizmusok nyilvános honlapján tájékoztatást kell nyújtani az adatvédelmi pajzs elveiről és az adott mechanizmus által az adatvédelmi pajzs keretében nyújtott szolgáltatásokról. E tájékoztatásnak tartalmaznia kell: (1) az adatvédelmi pajzs elvei független jogorvoslati mechanizmusokra vonatkozó követelményeivel kapcsolatos információkat vagy egy arra mutató linket; (2) a Minisztérium adatvédelmi pajzs honlapjára mutató linket; (3) annak leírását, hogy az adatvédelmi pajzs keretében nyújtott vitarendezési szolgáltatásaik ingyenesek az egyének számára; (4) annak leírását, hogyan lehet egy adatvédelmi pajzzsal kapcsolatos panaszt benyújtani; (5) az adatvédelmi pajzzsal kapcsolatos panaszok kezelésének a határidejét; valamint (6) a lehetséges jogorvoslatok körének leírását.

iii. A független jogorvoslati mechanizmusoknak éves jelentést kell közzétenniük, amely összesített statisztikákat tartalmaz a vitarendezési szolgáltatásaikra vonatkozóan. Az éves jelentésnek a következőket kell tartalmaznia: (1) az adatvédelmi pajzzsal kapcsolatosan kapott panaszok összesített számát az adott év során; (2) a kapott panaszok típusát; (3) a vitarendezés minőségére vonatkozó mutatókat, pl. a panaszok kezelésére fordított időtartam; és (4) a kapott panaszok kimenetelét, mégpedig a jogorvoslatok vagy a kiszabott szankciók számát és típusát.

iv. Az I. mellékletben meghatározottak szerint választott bírósági lehetőség áll az egyének számára rendelkezésre annak meghatározására maradványkövetelés esetén, hogy az adatvédelmi pajzsban részt vevő szervezet megsértette-e az elvek szerinti kötelezettségeit az adott egyénnel kapcsolatban, és az ilyen jogsértés teljesen vagy részlegesen orvoslás nélkül marad-e. Ez a lehetőség csak ezekre a célokra áll rendelkezésre. Ez a lehetőség például nem áll rendelkezésre az elvek ([1]) kivételei esetében vagy az adatvédelmi pajzs megfelelőségére vonatkozó állítás tekintetében. E választott bírósági lehetőség keretében az adatvédelmi pajzzsal foglalkozó testület (amely a felek megállapodása szerint egy–három választott bíróból áll) egyénspecifikus, nem pénzbeli méltányos jogorvoslatot (pl. az egyén kérdéses adataihoz való hozzáférés, azok korrekciója, törlése vagy visszaadása) is kiszabhat, amely csak az adott egyén tekintetében hivatott orvosolni az elvek megsértését. Az egyének és az adatvédelmi pajzsban részt vevő szervezetek a választott bíróság határozatának bírósági felülvizsgálatát és végrehajtását kérhetik a USA Szövetségi Választott bírósági Törvénye alapján.

([1]) Az elvek I.5. pontja

e) Jogorvoslatok és szankciók

A jogvitákat eldöntő 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 szüntessék be. A szankcióknak kellőképpen szigorúaknak kell lenniük ahhoz, hogy biztosítsák az elvek szervezet általi betartását. A változó szigorúságú szankciók skálája a jogvitát eldöntő szervek számára lehetővé teszi a nemteljesítés különböző fokozatainak megfelelő választ. A szankcióknak magukban kell foglalniuk a nemteljesítésre vonatkozó megállapítások közzétételét és bizonyos körülmények között az adatok törlésére vonatkozó követelményt ([1]). Más szankciók magukban foglalhatják a pecsét felfüggesztését és eltávolítását, az egyének ellentételezését a nemteljesítés következtében felmerült veszteségekért és a felfüggesztő végzéseket. A magánfelek jogvitáit eldöntő szerveknek és az önszabályozó testületeknek értesíteniük kell a megfelelő joghatósággal rendelkező kormányzati szervet vagy adott esetben a bíróságokat az adatvédelmi pajzsban részt vevő szervezetek szabályszegéséről, továbbá tájékoztatniuk kell erről a Minisztériumot is.

f) Az FTC fellépése

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 meghagyással, vagy panasz benyújtásával valamelyik szövetségi kerületi bírósághoz, amelynek az eredménye siker esetén az ugyanilyen tartalmú szövetségi bírósági végzés lehet. Ide tartozik az adatvédelmi pajzs elvei teljesítésének vagy az adatvédelmi pajzsban való részvételnek a hamis állítása olyan szervezetek részéről, amelyek vagy már nem szerepelnek az adatvédelmi pajzs listán, vagy soha nem nyújtottak be öntanúsítást a Minisztériumhoz. Az FTC az adott magatartás beszüntetésére kötelező meghagyás 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 adatvédelmi pajzs elvekhez való csatlakozást meghatározó más döntésekről.

g) Ismétlődő nemteljesítés

i. Ha egy szervezet ismétlődően nem teljesíti az elveket, tovább már nem jogosult az adatvédelmi pajzs előnyeire. Az elveket ismétlődően nem teljesítő szervezeteket a Minisztérium törli az adatvédelmi pajzs listáról, és vissza kell adniuk vagy törölniük kell azokat a személyes adatokat, amelyeket az adatvédelmi pajzs keretében 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 megállapítja, hogy a szervezet gyakran nem teljesíti az elveket, olyan mértékben, hogy a teljesítésre vonatkozó állítása már nem hihető. Ezekben az esetekben a szervezetnek haladéktalanul értesítenie kell a Minisztériumot az ilyen tényekről. Ellenkező esetben a szervezet a hamis nyilatkozatokról szóló törvény (18 U. S. C. § 1001) alapján perelhető. Egy szervezet visszalépése egy magánszektorbeli adatvédelmi önszabályozó programból vagy független vitarendezési mechanizmusból nem menti fel a kötelezettsége alól, hogy megfeleljen az elveknek, és a megfelelés ismétlődő nemteljesítését jelenti.

iii. A Minisztérium törli a szervezetet az adatvédelmi pajzs listáról, amennyiben értesítést kap az ismétlődő nemteljesítésről függetlenül attól, hogy az értesítést magától a szervezettől, egy adatvédelmi önszabályozó szervtől vagy más független vitarendező szervtől vagy egy kormányzati szervtől kapta-e, de csak azután, hogy először 30 napos határidővel felszólítást küld erre vonatkozóan, és lehetőséget biztosít a nemteljesítő szervezet számára a válaszadásra. Ennek megfelelően a Minisztérium által fenntartott adatvédelmi pajzsban

([1]) A jogvitákat eldöntő szervek saját belátásuk szerint ítélhetik meg azokat a körülményeket, amelyek esetén ezeket a szankciókat alkalmazzák. Az érintett adatok érzékenysége figyelembe veendő tényező annak eldöntésében, hogy szükség lehet-e az adatok törlésére, mint ahogyan az is, hogy a szervezet az adatvédelmi pajzs elveinek durva áthágásával gyűjtött-e össze, használt-e fel vagy hozott-e nyilvánosságra információt.

részt vevő szervezetek listája egyértelműen mutatja, mely szervezetek élvezik és mely szervezetek nem élvezik már az adatvédelmi pajzs előnyeit.

iv. Az adatvédelmi pajzs újraminősítés céljából egy önszabályozó szervben való részvételért folyamodó szervezetnek az adatvédelmi pajzsban való előző részvételéről teljes körűen tájékoztatnia kell az adott szervet.

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

a) A választási lehetőség elv célja alapvetően annak biztosítása, hogy a személyes információt olyan módon használják, illetve fedjék fel, amely összhangban van az egyén elvárásaival és választásaival. Ennek megfelelően az egyénnek lehetősége kell hogy legyen bármikor kizárni azt, hogy a személyes információt közvetlen üzletszerzési célra használják fel, a szervezet által megállapított ésszerű határokon belül, azaz például időt adva a szervezetnek a kívülmaradás érvénybe léptetésére. A szervezet ezenkívül megkövetelheti a kívülmaradást kérő egyéntől az azonosság megállapításához elegendő információ szolgáltatását. Az Egyesült Államokban az egyének ezzel a választási lehetőséggel egy központi „kívülmaradási" program révén élhetnek: ilyen pl. a Direct Marketing Association Mail Preference Service Közvetlen (Üzletszerzést Folytató Vállalkozások Szövetségének Csomagküldő Szolgálata) programja. Olyan szervezeteknek, amelyek részt vesznek a Direct Marketing Association Mail Preference Service szolgáltatásában, elő kell segíteniük a „kívülmaradási" lehetőség rendelkezésre állását olyan fogyasztók számára, akik nem kívánnak kereskedelmi információkhoz jutni. Az egyénnek minden esetben könnyen hozzáférhető és megfizethető mechanizmust kell biztosítani e lehetőség gyakorlására.

b) Hasonlóképpen, a szervezet felhasználhatja az információt bizonyos közvetlen értékesítési célokra, olyankor, amikor a gyakorlatban kivitelezhetetlen az egyén számára a kívülmaradási lehetőség megadása az információ 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 üzletszerzési értesítés 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 irányelv 26. cikke alapján a „személyes adatok olyan harmadik országba irányuló továbbítása, amely a 25. cikk (2) bekezdése értelmében nem biztosít megfelelő szintű védelmet", csak a következő feltételek mellett történhet: i. a továbbítás a fogyasztó által kért szolgáltatások biztosítása, vagy egy megállapodás, mint például a „törzsutasprogram" megállapodás feltételeinek teljesítése érdekében szükséges; vagy i.) a fogyasztó egyértelműen hozzájárulását adta. Az Egyesült Államokban az adatvédelmi pajzshoz tartozó szervezetek biztosítják a személyes adatok megfelelő védelmét, és ezért a fenti feltételek és az irányelv 26. cikkében megállapított más feltételek teljesítése nélkül fogadhatnak az EU-ból továbbított adatokat. Mivel az adatvédelmi pajzs a különleges információk tekintetében különleges szabályokat tartalmaz, az ilyen információkat (amelyek összegyűjtésére például a vásárlók fizikai segítségre vonatkozó igényeivel összefüggésben lehet szükség) az adatvédelmi pajzs résztvevői számára történő továbbítások magukban foglalhatják. Az információt továbbító szervezetnek azonban minden esetben tiszteletben kell tartania annak az uniós 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 adatvédelmi pajzs elveinek alkalmazása

A személyes adatok összegyűjtésére és bármilyen, az Egyesült Államokba történő továbbítást megelőző kezelésére a tagállami jogszabályokat kell alkalmazni. Amint az adatokat továbbították az Egyesült Államokba, az adatvédelmi pajzs 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 kidolgozott személyes adatok gyakran értékes szerepet játszanak a jövőbeni tudományos kutatásban. Amennyiben egy adott kutatásra összegyűjtött személyes adatokat az Egyesült Államok valamelyik adatvédelmi pajzsban levő 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 jövőbeni felhasználásairól: például időszakos nyomon követés, kapcsolódó tanulmányok vagy marketing.

ii. Magától értetődő, hogy az adatok összes jövőbeni felhasználása nem határozható meg pontosan, mivel az eredeti adatokba történő új betekintésből 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 jövőbeni, 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

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

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 lemondás. 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

A gyógyszeripari vagy orvostechnikai eszközt gyártó vállalatnak nem kell alkalmaznia az adatvédelmi pajzs elveit az értesítésre, a választási lehetőségre, az elszámoltathatóságra harmadik fél részére történő adattovábbításért, 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

A kutatási adatokat a kutatás vezetője egyedi módon és megváltoztathatatlanul kódolta 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 továbbítása az EU-ból az Egyesült Államokba nem képez az adatvédelmi pajzs elvek hatálya alá tartozó személyesadat-továbbítást.

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

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

b) Az értesítés, választási lehetőség és az elszámoltathatóság harmadik fél részére történő adattovábbításért elvét nem szükséges alkalmazni a nyilvános nyilvántartásban lévő információra mindaddig, amíg az nem kapcsolódik össze nem nyilvános nyilvántartásban lévő információval, valamint amennyiben a vonatkozó joghatóság által a betekintésre megállapított feltételeket tiszteletben tartják. Általában nem szükséges az értesítés, választási lehetőség és az elszámoltathatóság harmadik fél részére történő adattovábbításért elvét alkalmazni a nyilvánosan hozzáférhető információra, hacsak az európai átadó nem jelzi, hogy az ilyen információ olyan korlátozások alá tartozik, amelyek megkövetelik a szervezettől a fenti elvek alkalmazását a tervezett felhasználásokra. A szervezetek nem felelősek azért, hogy az információt hogyan használják fel azok, akik ahhoz nyilvánosságra hozott anyagokból jutnak hozzá.

c) Amennyiben egy szervezetről megállapították, hogy az elveket megsértve szándékosan hozott nyilvánosságra személyes információt annak érdekében, hogy ő vagy mások e kivételekből részesülhessenek, a továbbiakban nem jogosult az adatvédelmi pajzs előnyeire.

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

e) Ugyanúgy, mint a nyilvános archívumokban tárolt adatok esetében, nem szükséges a nagyközönség számára már elérhető információhoz való hozzáférés biztosítása, amíg azokat nem kapcsolják össze nyilvánosan nem elérhető információval. Azok a szervezetek, amelyek a nyilvánosan hozzáférhető információ 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 összeállította az adatokat.

16. **Közigazgatási szervek hozzáférési kérései**

a) A közigazgatási szervek személyes adatokhoz történő hozzáférésre vonatkozó jogszerű kérései átláthatóságának a biztosítása érdekében az adatvédelmi pajzsban 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) Az adatvédelmi pajzsban 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 adatvédelmi pajzs működéséről szóló közös éves áttekintés céljára az elveknek megfelelően.

c) Az értesítés elve (a) pontja xii. francia bekezdésének megfelelően az értesítés hiánya nem akadályozza vagy gátolja meg, hogy a szervezet választ adjon a jogszerű kérésekre.

I. melléklet

Választott Bírósági modell

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

A. **Hatály**

Ez a választott bírósági lehetőség az egyének rendelkezésére áll annak meghatározására maradványkövetelések esetén, hogy az adatvédelmi pajzsban 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 ([1]) alóli kivételek esetében, vagy az adatvédelmi pajzs megfelelőségére vonatkozó állítások tekintetében.

B. **Rendelkezésre álló jogorvoslatok**

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

C. **Választott bíráskodás előtti követelmények**

Az ezzel a választott bírósági 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 az elvek III.11(d) pontja i. francia bekezdésében meghatározott határidőn belül; (2) az elvek szerinti független jogorvoslati mechanizmusok igénybevétele, amely az egyén számára ingyenes; és (3) a kérdés jelzése az adatvédelmi hatóságukon keresztül a Kereskedelmi Minisztériumnak, és lehetőséget biztosítani a Kereskedelmi Minisztérium számára, hogy mindent megtegyen a kérdés rendezésére a Kereskedelmi Minisztérium Nemzetközi Kereskedelmi Igazgatóságának a levelében meghatározott határidőn belül – az egyén számára ingyenesen.

Ez a választott bírósági lehetőség nem vehető igénybe, ha az elveknek az egyén által említett állítólagos megsértése tárgyában (1) korábban már lefolytattak kötelező erejű választott bírósági eljárást; (2) az egyén részvételével folyó bírósági perben jogerős döntést hoztak; vagy (3) a felek azt már korábban rendezték. Ezenkívül, ezzel a lehetőséggel nem lehet élni, ha egy uniós adatvédelmi hatóság (1) az elvek III.5. vagy III.9. pontja szerint hatáskörrel rendelkezik az adott kérdésben; 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 választott bírósági lehetőségnek az alkalmazását egy másik jogi személlyel szemben, amelyre nem vonatkozik az adatvédelmi hatóság hatásköre.

D. **Ítéletek kötelező ereje**

Az egyén döntése, hogy ezzel a választott bírósági lehetőséggel éljen, teljesen önkéntes. A választott bírósági ítélet a választott bírósági 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, hogy amennyiben a nem pénzbeli méltányos jóvátétel nem teljesen orvosolja az állítólagos jogsértést, akkor a választott bírósági eljárás egyén általi kezdeményezése nem zárja ki a kártérítés iránti követelést, amely egyébként bírósági úton elérhető.

([1]) Az elvek I.5. pontja.

E. **Felülvizsgálat és végrehajtás**

Az egyének és az adatvédelmi pajzsban részt vevő szervezetek a választott bíróság végzésének bírósági felülvizsgálatát és végrehajtását kérhetik a USA Szövetségi Választott bírósági Törvénye alapján. ([1]) Minden ilyen ügyet azon szövetségi kerületi bíróság elé kell vinnie, amely az adatvédelmi pajzsban részt vevő szervezet székhelye szerint illetékes bíróság.

Ennek a választott bírósági lehetőségnek a célja egyéni viták rendezése, és a választott bírósági 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 választott bírói testület**

A felek választják ki a választott bírákat a választott bírák alább tárgyalt listájáról.

A vonatkozó jogszabályokkal összhangban az Egyesült Államok Kereskedelmi Minisztériuma és az Európai Bizottság listát állít össze legalább 20 választott bírával, akiket függetlenség, feddhetetlenség és tapasztalat alapján választanak ki. Erre a folyamatra az alábbiak vonatkoznak:

Választott bírák:

(1) a listán maradnak 3 évig, kivételes körülmények vagy okok hiányában, amely időszak további egy alkalommal, 3 évre meghosszabbítható;

(2) nem utasíthatja őket egyik fél vagy az adatvédelmi pajzsban 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; és

(3) engedéllyel kell rendelkezniük az Egyesült Államokban történő jogi praktizálásra, és szakértőknek kell lenniük az Egyesült Államok adatvédelmi törvénye szerint, továbbá tapasztalattal kell rendelkezniük az uniós adatvédelmi jog területén.

G. **Választott bírósági eljárások**

A vonatkozó jogszabályokkal összhangban a megfelelőségi határozat meghozatalától számított 6 hónapon belül a Kereskedelmi Minisztérium és az Európai Bizottság megállapodnak egy bevezetett egyesült államokbeli választott bírósági eljárás rendszerről (mint az AAA vagy JAMS), amely az adatvédelmi pajzzsal foglalkozó testület eljárásaira vonatkozik – az alábbi megfontolások figyelembevételével:

1. A szervezetnek küldött értesítéssel egyén kezdeményezhet kötelező erejű választott bírósági eljárást a fenti választott bírósági 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.

([1]) A szövetségi választott bírósági törvény („FAA") 2. fejezete úgy rendelkezik, hogy „egy akár szerződéses, akár másmilyen jogviszonyból eredő választott bírósági megállapodás vagy választott bírósági ítélet, amely kereskedelmi jellegű, beleértve egy [az FAA 2. pontjában] leírt tranzakciót, szerződést vagy megállapodást, a külföldi választott bírósági 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 választott bírósági eljárásban részt vevő bármelyik fél az e fejezet szerint hatáskörrel rendelkező bírósághoz fordulhat a választott bírósági 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 érvényesítésének 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 választott bírósági 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 tovább 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. §

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

3. Az FTC fellépése a választott bírósági 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 választott bírósági eljárásban – azzal, hogy egy uniós egyén kérésére az uniós adatvédelmi hatóságok segítséget nyújthatnak kizárólag az értesítés megfogalmazásában, de az uniós adatvédelmi hatóságok nem férhetnek hozzá az ilyen választott bírósági eljárások betekintésre szánt vagy más anyagaihoz.

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

7. A választott bíráknak benyújtott anyagokat bizalmasan kezelik, és csak a választott bírósági eljárással kapcsolatban használják fel.

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

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

H. **Költségek**

A választott bíráknak indokolt lépéseket kell tenniük a választott bírósági eljárás költségeinek minimalizálása érdekében.

A vonatkozó jogszabályokkal összhangban a Kereskedelmi Minisztérium előmozdítja egy alap létrehozását, amelybe az adatvédelmi pajzsban részt vevő szervezeteknek – a szervezet mérete alapján – éves hozzájárulást kell fizetniük, amely fedezi a választott bírósági költségeket, beleértve a választott bírák díjazását az Európai Bizottsággal megállapodott felső összeghatár („plafon”) erejéig. Az alapot egy harmadik fél kezeli, amely rendszeresen beszámol az alap működéséről. Az éves felülvizsgálatkor a Kereskedelmi Minisztérium és az Európai Bizottság áttekinti az alap működését, beleértve a hozzájárulások összegének vagy a maximális díjnak a kiigazítását, és megvizsgálják többek között a választott bírósági eljárások számát, valamint költségeit és időzítését – kölcsönösen megállapodva abban, hogy az adatvédelmi pajzsban részt vevő szervezetek számára a díj ne jelentsen túlzott pénzügyi terhet. Az ügyvédi költségekre ez a rendelkezés nem vonatkozik, és azok e rendelkezés szerinti alapból nem fedezhetők.

III. MELLÉKLET

John Kerry amerikai külügyminiszter levele

2016. július 7.

Tisztelt Jourová biztos asszony!

Örömmel tölt el, hogy megállapodásra jutottunk az Európai Unió–Egyesült Államok adatvédelmi pajzsról, amelynek része egy biztosi mechanizmus, melynek segítségével az uniós hatóságok kéréseket tudnak benyújtani uniós egyének nevében az Egyesült Államok jelfelderítési gyakorlatával kapcsolatban.

2014. január 17-én Barack Obama elnök fontos hírszerzési reformokat jelentett be, amelyeket a 28. sz. elnöki rendelet tartalmaz (PPD-28). A PPD-28 keretében kijelöltem Catherine A. Novelli külügyminiszter-helyettest a nemzetközi informatikai diplomácia főkoordinátorának, aki a kapcsolattartónk lesz azon külföldi kormányok felé, amelyek aggodalmukat akarják kifejezni az Egyesült Államok jelfelderítési tevékenysége kapcsán. Ennek a funkciónak az alapján létrehoztam egy adatvédelmi pajzs biztosi mechanizmust az A. mellékletben meghatározott feltételek szerint, amelyeket 2016. február 22-i levelem óta frissítettek. Utasítottam Novelli miniszterhelyettest ennek a funkciónak a betöltésére. Novelli miniszterhelyettes független az Egyesült Államok hírszerzési közösségétől, és közvetlen alárendeltem.

Utasítottam a munkatársaimat, hogy biztosítsák a szükséges erőforrásokat az új biztosi mechanizmus megvalósításához, és bízom benne, hogy ez hatékony eszközt fog jelenteni az uniós egyének aggodalmainak kezelésére.

Üdvözlettel:

John F. Kerry

A. melléklet

EU-USA adatvédelmi pajzs ombudsmani mechanizmus

Jelfelderítés tekintetében az EU-USA adatvédelmi pajzs fontosságának elismeréseként ez a feljegyzés meghatározza az új mechanizmus megvalósításának a folyamatát, összhangban a jelfelderítésre vonatkozó 28. sz. elnöki rendelettel (PPD-28) ([1]).

2014. január 17-én Obama elnök beszédet tartott, amelyben fontos hírszerzési reformokat jelentett be. A beszédében kiemelte, hogy „az erőfeszítéseink segítenek megvédeni nemcsak a nemzetünket, hanem a barátainkat és a szövetségeseinket is. Az erőfeszítéseink csak akkor lesznek hatékonyak, ha más országok polgárai bíznak abban, hogy az Egyesült Államok is tiszteletben tartja az ő magánéletüket." Obama elnök bejelentette egy új elnöki rendelet, a PPD-28 kibocsátását, amelynek célja „világosan leírni, hogy a tengerentúli felderítési tevékenységünk keretében mit teszünk és mit nem."

A PPD-28 4(d) pontja arra utasítja a külügyminisztert, hogy nevezzen ki egy „nemzetközi informatikai diplomáciai főkoordinátort" (főkoordinátor), ... aki a kapcsolattartó lesz azon külföldi kormányok felé, amelyek aggodalmukat akarják kifejezni az Egyesült Államok jelfelderítési tevékenysége kapcsán. 2015. januárja óta C. Novelli miniszterhelyettes tevékenykedik főkoordinátorként.

Ez a feljegyzés leírja az új mechanizmust, amelyet az főkoordinátor követni fog az EU-ból az Egyesült Államokba az adatvédelmi pajzs keretében továbbított adatokhoz nemzetbiztonsági okokból történő hozzáférés iránti kérelmek kezelésének elősegítésére, az általános szerződéses feltételeket (SCC-k), a kötelező erejű vállalati szabályokat (BCR-ek), az „eltéréseket" ([2]) vagy „esetleges jövőbeli eltéréseket" ([3]), az Egyesült Államok vonatkozó jogszabályai és politikája szerinti bevezetett csatornákon keresztül, valamint az ilyen kérelmekre adott válaszokat.

1. **EU-USA adatvédelmi pajzs ombudsman.** A főkoordinátor adatvédelmi pajzs ombudsmanként fog tevékenykedni és szükség szerint további külügyminisztériumi tisztségviselőket jelöl ki az ebben a feljegyzésben meghatározott feladatai teljesítésének segítésére. (A továbbiakban a koordinátor és az ilyen feladatokat végző tisztségviselők megnevezése: „adatvédelmi pajzs ombudsman.") Az adatvédelmi pajzs ombudsman szorosan együttműködik más minisztériumok és hivatalok megfelelő tisztségviselőivel, akiknek feladata a kérelmek kezelése az Egyesült Államok vonatkozó jogszabályaival és politikájával összhangban. Az ombudsman független a hírszerzési közösségtől. Az ombudsman közvetlenül a külügyminiszternek tesz jelentést, aki biztosítja, hogy az ombudsman tárgyilagosan az adandó válasz megváltoztatására alkalmas, helytelen befolyásolásától mentesen láthassa el a feladatát.

2. **Hatékony koordináció.** Az adatvédelmi pajzs ombudsman hatékonyan tudja felhasználni az alábbiakban leírt felügyeleti szerveket, és hatékonyan tud egyeztetni azokkal annak biztosítása érdekében, hogy az uniós polgárok panaszkezelő testületétől érkező megkeresésre adott ombudsmani válasza a szükséges információkon alapuljon. Ha

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

([2]) „Eltérések": ebben a szövegösszefüggésben olyan kereskedelmi adattovábbítás vagy adattovábbítások, amely(ek) az alábbi feltétellel történik/történnek: a) az érintett egyértelműen hozzájárulását adta a tervezett továbbításhoz; vagy b) a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; vagy c) a továbbítás az adatkezelő és valamely harmadik személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; vagy d) a továbbítás fontos közérdekből vagy jogi követelések megállapítása, érvényesítése vagy védelme miatt szükséges, illetve azt jogszabály írja elő; vagy e) a továbbítás az érintett létfontosságú érdekeinek védelme miatt szükséges; vagy f) a továbbítást olyan nyilvántartásból végzik, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, amennyiben a jogszabályok által a betekintésre megállapított feltételek az adott esetben teljesülnek.

([3]) „Esetleges jövőbeli eltérések": ebben a szövegösszefüggésben olyan kereskedelmi adattovábbítás(ok)t, amely(ek) az alábbi feltételek egyikének teljesülésekor történik/történnek, amennyiben a feltétel jogszerű alapot jelent a személyes adatok EU-ból az Egyesült Államokba történő továbbításához: a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról; vagy b) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására; vagy c) egy harmadik országba vagy egy nemzetközi szervezethez történő adattovábbítás esetén, és amennyiben egyetlen más eltérés vagy lehetséges jövőbeni eltérés sem, ha a továbbítás nem ismétlődő jellegű, csak korlátozott számú érintettre vonatkozik, az adatkezelő jogszerű érdekeinek a védelme érdekében szükséges, amelyet nem írnak felül az érintett érdekei, jogai vagy szabadságjoga, valamint az adatkezelő mérlegelte az adattovábbítás minden körülményét, és ezen értékelés alapján megfelelő biztosítékokat nyújtott a személyes adatok védelme tekintetében.

a megkeresés a megfigyelésnek az Egyesült Államok jogával való összeegyeztethetőségére vonatkozik, az adatvédelmi pajzs ombudsman együttműködhet az egyik vizsgálati jogkörrel rendelkező felügyeleti szervvel.

a) Az adatvédelmi pajzs ombudsman szorosan együttműködik az Egyesült Államok más kormánytisztviselőivel – köztük a megfelelő független felügyeleti szervekkel – annak biztosítása érdekében, hogy a benyújtott kérelmeket a vonatkozó jogszabályoknak és politikáknak megfelelően dolgozzák fel, és hozzanak határozatot róluk. Az adatvédelmi pajzs ombudsman koordinálni fogja tevékenységét különösen a nemzeti hírszerzés igazgatójának irodájával, az Igazságügyi Minisztériummal és szükség szerint az Egyesült Államok nemzetbiztonságával foglalkozó más minisztériumokkal és hivatalokkal, valamint főellenőrökkel, az információhoz való szabad hozzáférésről szóló törvényért felelős tisztviselőkkel és a polgári szabadságjogi és adatvédelmi tisztviselőkkel.

b) Az Egyesült Államok kormánya nemzetbiztonsági ügyekben minisztériumokon és hivatalokon átívelő koordinációs és felügyeleti mechanizmusokat alkalmaz annak biztosítása érdekében, hogy az adatvédelmi pajzs ombudsman válaszolni tudjon a 3(b) pont szerint benyújtott kérelmekre a 4(e) pontban meghatározottak szerint.

c) Az adatvédelmi pajzs ombudsman a kérelmekkel kapcsolatos ügyeket az adatvédelmi és polgári szabadságjog felügyeleti tanácshoz továbbíthat megfontolásra.

3. **Kérelmek benyújtása.**

a) A kérelmet először a nemzetbiztonsági szolgálatok felügyeletéért és/vagy a hatóságok általi személyesadat-kezeléséért felelős tagállami felügyeleti hatóságoknak nyújtják be. A kérelmet egy uniós központi szerv (továbbiakban együttesen: az „uniós egyéni panaszkezelő szerv") fogja benyújtani az ombudsmannak.

b) Az EU egyéni panaszkezelő szerve biztosítja az alábbi intézkedéseknek megfelelően, hogy a kérelem hiánytalan:

i) Az egyén azonosítása és annak ellenőrzése, hogy az egyén a saját nevében jár el, és nem egy kormányzati vagy kormányközi szervezet képviselője.

ii) Annak biztosítása, hogy a kérelmet írásban nyújtják be, és a kérelem tartalmazza az alábbi alapvető információkat:

— a kérelem alapját képező bármely információ,

— a kért információ vagy jogorvoslat jellege,

— az Egyesült Államok vélelmezetten érintett jogi személyei, ha vannak ilyenek, és

— a kért információ vagy jogorvoslat elérése érdekében foganatosított egyéb intézkedések és az ilyen intézkedésekre kapott válaszok.

iii) Annak ellenőrzése, hogy a kérelem olyan adatokra vonatkozik, amelyekről alapos indokkal feltételezhető, hogy az EU-ból az Egyesült Államokba továbbították az adatvédelmi pajzs, az általános szerződéses feltételek, a kötelező erejű vállalati szabályok, eltérések vagy esetleges jövőbeli eltérések keretében.

iv) Annak a kezdeti meghatározása, hogy a kérelem nem komolytalan, zaklató vagy rosszhiszemű.

c) Ahhoz, hogy a kérelem a jelen feljegyzés alapján az adatvédelmi pajzs ombudsman általi további kezelésre alkalmas legyen, a kérelemnek nem szükséges bemutatnia, hogy a kérelmező adataihoz az Egyesült Államok kormánya jelfelderítési tevékenység keretében ténylegesen hozzáfért.

4. **Kötelezettségvállalások a benyújtó uniós egyéni panaszkezelő szervvel történő kommunikációra..**

a) Az adatvédelmi pajzs ombudsman a benyújtó uniós egyéni panaszkezelő szervnek igazolja a kérelem kézhezvételét.

b) Az adatvédelmi pajzs ombudsman kezdeti felülvizsgálatot végez annak ellenőrzése érdekében, hogy a kérelmet a 3 (b) pontnak megfelelően állították össze. Ha az adatvédelmi pajzs ombudsman hiányosságot állapít meg vagy kérdése van a kérelem összeállítását illetően, az aggályokat a benyújtó uniós egyéni panaszkezelő szervvel próbálja meg kezelni és megoldani.

c) Ha a kérelem megfelelő kezelésének elősegítése érdekében az adatvédelmi pajzs ombudsmannak további információkra van szüksége, vagy ha konkrét lépéseket kell tennie az egyénnek, aki eredetileg benyújtotta a kérelmet, akkor az adatvédelmi pajzs ombudsman tájékoztatja a benyújtó uniós egyéni panaszkezelő szervet.

d) Az adatvédelmi pajzs ombudsman nyomon követi a kérelmek státusát és szükség esetén tájékoztatja a benyújtó uniós egyéni panaszkezelő szervet az aktuális helyzetről.

e) A kérelem jelen feljegyzés 3. pontjában meghatározottak szerinti kitöltése után az adatvédelmi pajzs ombudsman időben megfelelő választ ad a benyújtó uniós egyéni panaszkezelő szervnek, miközben a vonatkozó jogszabályok és politikák alapján az információ védelmére vonatkozó kötelezettség továbbra is fennáll. Az adatvédelmi pajzs ombudsman választ ad a benyújtó EU egyéni panaszkezelő szervnek, amelyben megerősíti, hogy.i. a panaszt megfelelően kivizsgálták, és ii. az Egyesült Államok jogszabályai, alapszabályai, végrehajtási rendeletei, elnöki rendeletei és hivatali politikái, amelyek az ODNI levélben leírt korlátozásokról és biztosítékokról rendelkeznek, teljesültek vagy nemteljesülés esetén a nemteljesülést orvosolták. Az adatvédelmi pajzs ombudsman nem erősíti meg és nem is cáfolja, hogy az egyén megfigyelés célpontja volt, és az adatvédelmi pajzs ombudsman nem erősíti meg az alkalmazott konkrét jogorvoslatot. Az 5. pontban részletesen kifejtettek szerint a FOIA kérelmeinek kezelése a szóban forgó alapszabálynak és a vonatkozó szabályzatoknak megfelelően történik.

f) Az adatvédelmi pajzs ombudsman közvetlenül az uniós egyéni panaszkezelő szervvel kommunikál, amely viszont felelős a benyújtó egyénnel történő kommunikációért. Ha a közvetlen kommunikáció az alább leírt mögöttes folyamatok része, akkor az ilyen kommunikációk a meglevő eljárásoknak megfelelően történnek.

g) A jelen feljegyzésben tett kötelezettségvállalások nem vonatkoznak olyan általános kérelmekre, amelyek szerint az EU-USA adatvédelmi pajzs nem összeegyeztethető az uniós adatvédelmi előírásokkal. A jelen feljegyzésben szereplő kötelezettségvállalásokat az Európai Bizottság és az Egyesült Államok kormánya közötti azon megállapodás alapján tették, hogy a jelen mechanizmus szerint bekövetkezhetnek erőforrásokkal kapcsolatos korlátozások – például az információhoz való szabad hozzáférésről szóló törvény (FOIA) szerinti kérelmek tekintetében is. Amennyiben az adatvédelmi pajzs ombudsman feladatainak ellátása során az indokolt erőforráskorlátozásokon túlmutató rendelkezésekre lenne szükség, és ez akadályozná e kötelezettségvállalások teljesítését, az Egyesült Államok kormánya megvitatja az Európai Bizottsággal az adott helyzet kezeléséhez szükséges kiigazításokat.

5. **Tájékoztatás adására irányuló kérelem.** Az Egyesült Államok kormányának nyilvántartásához történő hozzáférésre irányuló kérelmek az információhoz való szabad hozzáférésről szóló törvény (FOIA) szerint nyújthatók be, és kezelésük e törvény alapján történik.

a) A FOIA eszközt biztosít a meglevő szövetségi hivatali nyilvántartásokhoz hozzáférést kérelmező személyek számára – a kérelmező állampolgárságától függetlenül. Ezt az alapszabályt az Egyesült Államok Törvénykönyve 5 U.S.C. § 552 paragrafusa kodifikálta. Az alapszabály a FOIA-ra vonatkozó további információkkal együtt elérhető a www.FOIA.gov és http://www.justice.gov/oip/foia-resources címeken. Minden hivatalnak van egy FOIA tisztségviselője, és tájékoztatást ad a nyilvános honlapján arról, hogyan lehet FOIA kérelmet benyújtani a hivatalhoz. A hivataloknak eljárásaik vannak arra, hogyan lehet egymással tanácskozni olyan FOIA kérelmek esetén, amelyekhez egy másik hivatal nyilvántartása is szükséges.

b) Például:

i) A nemzeti hírszerzés igazgatójának irodája (ODNI) létrehozott egy ODNI FOIA portált az ODNI számára: http://www.dni.gov/index.php/about-this-site/foia. Ez a portál tájékoztatást ad a kérelem benyújtásáról, a folyamatban levő kérelem státusának ellenőrzéséről, és olyan információk eléréséről, amelyeket az ODNI a FOIA keretében bocsátott ki és tett közzé. Az ODNI FOIA portál linkeket tartalmaz más hírszerző közösséggel kapcsolatos FOIA honlapokhoz: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Az Igazságügyi Minisztérium Tájékoztatási Politikai Irodája átfogó tájékoztatást nyújt a FOIA-ról: http://www.justice.gov/oip. A tájékoztatás nemcsak a FOIA kérelmek Igazságügyi Minisztérium számára történő benyújtására terjed ki, hanem útmutatást is nyújt az Egyesült Államok kormánya számára a FOIA előírások értelmezéséről és alkalmazásáról.

c) A FOIA keretében a kormányzati nyilvántartásokhoz történő hozzáférésre bizonyos tételesen felsorolt kivételek vonatkoznak. Ezek közé tartoznak a minősített nemzetbiztonsági adatokhoz, harmadik felek személyes adataihoz, valamint bűnüldöző szervek nyomozásaival kapcsolatos adatokhoz történő hozzáférésre vonatkozó korlátozások, és ezek hasonlóak a saját információkhoz történő hozzáférésre vonatkozó jogszabályokban előírt uniós tagállami korlátozásokhoz. Ezek a korlátozások egyaránt vonatkoznak amerikaiakra és nem amerikaiakra.

d) A FOIA keretében kérelmezett nyilvántartások kiadására vonatkozó viták esetén fellebbezéssel lehet élni először közigazgatási szervnél, majd szövetségi bíróságon. A bíróságnak *de novo* határozatot kell hoznia arról, hogy a nyilvántartásokat megfelelően tartották-e vissza, az 5 U.S.C. § 552(a)(4)(B) szerint, és kötelezheti a kormányt a nyilvántartásokhoz történő hozzáférés biztosítására. Néhány esetben a bíróságok elutasították a kormány arra vonatkozó kérelmét, hogy az adatokat minősített adatként vissza kell tartani. Habár pénzügyi kártérítés nem áll rendelkezésre, a bíróságok megítélhetik az ügyvédi költségek megtérítését.

6. **További intézkedések kérelmezése.** A jogsértést vagy más szabálysértés vélelmező kérelmet az Egyesült Államok megfelelő kormányszervéhez utalják, beleértve a független felügyeleti szerveket, amelyeknek hatáskörében áll kivizsgálni az adott kérelmet és az alábbi leírt nemteljesítést megvizsgálni.

a) A főellenőrök törvényileg függetlenek; széles hatáskörük van vizsgálatok, auditok és programok – köztük a csalás, a visszaélések és jogsértések – felülvizsgálatára; ezenfelül korrekciós intézkedéseket is javasolhatnak.

i) Az 1978. évi főellenőrökről szóló, módosított törvény független és objektív egységként a legtöbb hivatalnál létrehozta a Szövetségi Főellenőri Irodát (IG), amelynek feladata az adott hivatal programjai és tevékenysége során a pazarlás, csalás és visszaélés elleni küzdelem. Ebből a célból mindegyik IG feladata az adott hivatal programjaival és tevékenységével kapcsolatos auditok és vizsgálatok végzése. Ezenkívül, az IG-k a gazdaságosság, hatékonyság és eredményesség elősegítését célzó tevékenységekre vonatkozó iránymutatást, koordinációt és ajánlott politikákat adnak ki, továbbá megelőzik és felderítik a hivatal programjai és tevékenységei során a csalást és a visszaéléseket.

ii) A Hírszerző Közösség mindegyik tagjának van saját főellenőri irodája, amelynek feladata többek között a külföldi hírszerző tevékenységek felügyelete. Számos, hírszerző programokról szóló főellenőri jelentést hoztak nyilvánosságra.

iii) Például:

— Az Hírszerző Közösség főellenőri irodáját (IC IG) a 2010. pénzügyi évre vonatkozó hírszerzési felhatalmazási törvény405. cikke alapján hozták létre. Az egész Hírszerző Közösség gazdaságosságának és hatékonyságának javítása érdekében az IC IG feladata az egész Hírszerző Közösségre vonatkozó auditok, vizsgálatok és felülvizsgálatok végzése, amelyek olyan rendszerkockázatokat, sebezhetőséget és hiányosságokat azonosítanak és kezelnek, amelyek átszövik a Hírszerző Közösség valamennyi tevékenységét. Az IC IG felhatalmazással rendelkezik állítólagos jogszabálysértések, szabályok, szabályzatok megsértésére, állítólagos pazarlásra, csalásra, hatalommal való visszaélésre vagy a közegészség és biztonság jelentős vagy konkrét veszélyeztetésére irányuló panaszok és információk kivizsgálására az ODNI, illetve a Hírszerző Közösség programjai és tevékenységei kapcsán. Az IC IG tájékoztatást nyújt arról, hogyan lehet kapcsolatba lépni közvetlenül az IC IG-vel beadvány benyújtása érdekében: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— A Egyesült Államok Igazságügyi Minisztériumának (DOJ) Főellenőri Irodája (OIG) egy törvényileg létrehozott független egység, amelynek a feladata a DOJ programjaiban és munkatársai esetében a pazarlás, csalás, visszaélés vagy szabálysértés felderítése és elhárítása, valamint a programok gazdaságosságának és hatékonyságának az elősegítése. Az OIG vizsgálja a DOJ munkatársai által állítólagosan elkövetett büntető- és polgári jogi jogsértéseket, és a DOJ programjainak auditálását és vizsgálatát is végzi. Az OIG hatáskörrel rendelkezik az Igazságügyi Minisztérium munkatársai ellen szabálysértés miatt tett valamennyi panasz esetében, ideértve a Szövetségi Nyomozó Irodát; Gyógyszerügyi Végrehajtási Igazgatóságot; Szövetségi Börtönügyi Irodát; Egyesült Államok Rendőrbírói Szolgálatát; Alkohol, Dohány, Lőfegyver és Robbanószer Irodát; Egyesült Államok Ügyvédi Irodáit; és az Igazságügyi Minisztérium más osztályain vagy irodáin dolgozó munkavállalókat. (Az egyetlen kivétel az, hogy a Minisztérium ügyvédi vagy bűnüldözési munkatársai által állítólagosan elkövetett szabálysértések, amelyek a Minisztérium ügyvédjeinek vizsgálati,

peres vagy jogi tanácsadási hatáskörével kapcsolatosak, a Minisztérium szakmai felelősség irodájának hatáskörébe tartoznak.) Ezenkívül az Egyesült Államok „Patriot Act" törvénye, amely 2001. október 26-án lépett életbe, arra utasítja a főellenőrt, hogy vizsgálja felül az Igazságügyi Minisztérium munkatársai által állítólagosan elkövetett polgári jogi és polgári szabadságjogi jogsértésekre vonatkozóan kapott információkat, és fogadja az ezzel kapcsolatos panaszokat. Az OIG nyilvános honlapot tart fenn – https://www.oig.justice.gov –, amelynek része egy forróvonal a panaszok benyújtására – https://www.oig.justice.gov/hotline/index.htm.

b) Az Egyesült Államok kormánya adatvédelmi és polgári szabadságjogi irodáinak és egységeinek is vannak erre vonatkozó feladatai. Például:

i) Az Egyesült Államok Törvénykönyvében 42 U.S.C. § 2000-ee1 címen kodifikált 2007. évi 2009/11 bizottsági törvény 803. cikke adatvédelmi és polgári szabadságjogi tisztségviselői funkciókat hoz létre egyes minisztériumoknál és hivataloknál (köztük a Külügyminisztériumban, az Igazságügyi Minisztériumban és az ODNI-nál). A 803. cikk kimondja, hogy ezek az adatvédelmi és polgári szabadságjogi tisztségviselők főtanácsadóként tevékenykednek többek között annak biztosítása érdekében, hogy a minisztérium, a hivatal vagy az egység megfelelő eljárásokkal rendelkezzen egyének panaszainak kezelésére, akik azt állítják, hogy a minisztérium, a hivatal vagy az egység megsértette adatvédelmi vagy polgári szabadságjogaikat.

ii) Az ODNI polgári szabadságjogi és adatvédelmi hivatal (ODNI CLPO) vezetője az ODNI polgári szabadságjogok védelmi igazgatója, amely funkciót az 1948. évi nemzetbiztonsági törvény hozta létre. Az ODNI CLPO feladata többek között annak biztosítása, hogy a Hírszerző Közösség egységeinek politikái és eljárásai megfelelő adatvédelmet és polgári szabadságjogi védelmet biztosítsanak, ezenfelül feladatkörébe tartozik az ODNI programjai és tevékenységei során állítólagosan elkövetett polgári jogi vagy adatvédelmi visszaélésekre vagy jogsértésekre vonatkozó panaszok felülvizsgálata és kivizsgálása. Az ODNI CLPO tájékoztatást nyújt a nyilvánosság számára a honlapján, beleértve a panaszok benyújtására vonatkozó útmutatást: www.dni.gov/clpo. Ha az ODNI CLPO adatvédelemre vagy polgári szabadságjogra vonatkozó panaszt kap, amely érinti a Hírszerző Közösség programjait és tevékenységeit, akkor egyeztet a Hírszerző Közösség más egységeivel arról, hogyan kell a panaszt a továbbiakban kezelni a Hírszerző Közösségen belül. Megjegyzendő, hogy a Nemzetbiztonsági Hivatalnak (NSA) is van polgári szabadságjogi és adatvédelmi irodája, amely tájékoztatást nyújt a feladatairól a saját honlapján – https://www.nsa.gov/civil_liberties/. Ha a tájékoztatás alapján egy hivatal nem felel meg az adatvédelmi előírásoknak (*pl.* a PPD-28 4. pontja szerinti követelménynek), a hivataloknak megfelelési mechanizmusuk van az incidens felülvizsgálatára és orvoslására. A hivataloknak jelenteniük kell az ODNI felé a PPD-28 szerinti incidenseket.

iii) Az Igazságügyi Minisztérium adatvédelmi és polgári szabadságjogi irodája (OPCL) támogatja a Minisztérium adatvédelmi és polgári szabadságjogi főigazgatója (CPCLO) feladatait. Az OPCL fő feladata az amerikai polgárok adatvédelmi és polgári szabadságjogi védelme a Minisztérium adatvédelmi tevékenységének felülvizsgálata, felügyelete és koordinációja révén. Az OPCL jogi tanácsot és útmutatást ad a Minisztérium egységei számára; biztosítja a Minisztérium adatvédelmi megfelelését, beleértve az 1974. évi adatvédelmi törvény, valamint a 2002. évi e-kormányzati törvény és a szövetségi információbiztonsági törvény adatvédelmi rendelkezései, és a fenti törvények elősegítése érdekében kibocsátott közigazgatási politikai irányelvek teljesítését; kidolgozza és megszervezi a Minisztérium adatvédelmi képzését; támogatást nyújt a CPCLO számára a Minisztérium adatvédelmi szabályzatának a kidolgozásában; adatvédelemmel kapcsolatos jelentéseket készít az elnök és a kongresszus számára; valamint felülvizsgálja a Minisztérium információkezelési gyakorlatát annak biztosítása érdekében, hogy ez a gyakorlat összhangban legyen az adatvédelemmel és polgári szabadságjogok védelmével. Az OPCL tájékoztatást nyújt a nyilvánosság számára a feladatairól az alábbi honlapon: http://www.justice.gov/opcl.

iv) A 42 U.S.C. § 2000ee *és az azt követő rendelkezések* szerint az adatvédelmi és polgári szabadságjogi felügyelő tanács folyamatosan felülvizsgálja i. a politikákat és eljárásokat, valamint azok megvalósítását, a minisztériumok, hivatalok és a végrehajtási ág egységei esetében a nemzet terrorizmus elleni védelme során tett erőfeszítésekkel kapcsolatban az adatvédelem és polgári szabadságjogok védelmének a biztosítása érdekében, és ii. a végrehajtó ág ilyen erőfeszítésekkel kapcsolatos egyéb tevékenységeit annak meghatározása érdekében, hogy az ilyen tevékenységek megfelelően garantálják az adatvédelmet és a polgári szabadságjogok védelmét, és összhangban legyenek az adatvédelemre és a polgári szabadságjogok védelmére irányadó jogszabályokkal, szabályzatokkal és politikákkal. Adatvédelmi tisztségviselőktől és polgári szabadságjogi tisztségviselőktől jelentéseket és más információkat kap, azokat felülvizsgálja, és adott esetben ajánlásokat tesz a tevékenységeik tekintetében. Az Egyesült Államok Törvénykönyvében 42 U.S.C. § 2000-ee1 címen kodifikált 2007. évi 2009/11 bizottsági törvény 803. cikke arra utasítja nyolc szövetségi hivatal adatvédelmi és polgári szabadságjogi tisztségviselőit (közte a védelmi minisztert, a belbiztonsági minisztert, a nemzeti hírszerzés igazgatóját és a Központi Hírszerzési Ügynökség igazgatóját) és a tanács által kijelölt további hivatalokat, hogy rendszeres jelentéseket nyújtsanak be a PCLOB számára, beleértve az adott hivatal által vélelmezett jogsértések miatt

kapott panaszok számát, jellegét és megoszlását. A PCLOB felhatalmazásokról rendelkező alapszabálya arra utasítja a tanácsot, hogy fogadja ezeket a jelentéseket, és szükség esetén ajánlásokat tegyen az adatvédelmi tisztségviselők és polgári szabadságjogi tisztségviselők számára a tevékenységeik tekintetében.

IV. MELLÉKLET

Edith Ramirez, a Szövetségi Kereskedelmi Bizottság elnökasszonyának levele

2016. július 7.

E-MAILEN

Věra Jourová
A jogérvényesülésért, a fogyasztópolitikáért és a nemek közötti esélyegyenlőségért felelős biztos
Európai Bizottság
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
Belgium

Tisztelt Jourová biztos asszony!

Az Egyesült Államok Szövetségi Kereskedelmi Bizottsága („FTC") nagyra értékeli a lehetőséget, hogy leírja az új EU-USA adatvédelmi pajzs keretrendszer (az „adatvédelmi pajzs keretrendszer" vagy „keretrendszer") általa történő végrehajtását. Úgy gondoljuk, hogy a keretrendszer kritikus szerepet fog játszani az adatvédelmi jellegű kereskedelmi tranzakciók elősegítésében az egyre inkább összefonódó világban. Lehetővé teszi a vállalkozások számára fontos tevékenységek végzését a globális gazdaságban, ugyanakkor biztosítja az uniós fogyasztók fontos adatvédelmének fenntartását. Az FTC régóta elkötelezett a határokon átívelő adatvédelem iránt, és kiemelt feladatnak tekinti a keretrendszer végrehajtását. Az alábbiakban kifejtjük az FTC eddigi erős adatvédelmi tevékenységének a végrehajtását általánosságban, beleértve az eredeti védett adatkikötő program általunk történt végrehajtását, valamint az FTC eljárását az új keretrendszer végrehajtására.

Az FTC először 2000-ben fejezte ki nyilvánosan a védett adatkikötő program végrehajtása iránti elkötelezettségét. Az akkori FTC elnök, Robert Pitofsky levelet küldött az Európai Bizottságnak, amelyben leírta az FTC vállalását a védett adatkikötő adatvédelmi elveinek a hatékony végrehajtására. Az FTC fenntartotta ezt a kötelezettségvállalását közel 40 végrehajtási tevékenységben, számos további vizsgálat során és az egyes európai adatvédelmi hatóságokkal közös érdekeket érintő ügyekben folytatott együttműködés folyamán.

Miután 2013. novemberben az Európai Bizottság aggodalmát fejezte ki a védett adatkikötő program igazgatása és végrehajtása tekintetében, mi és az Egyesült Államok Kereskedelmi Minisztériuma megbeszéléseket kezdtünk az Európai Bizottság tisztségviselőivel a program erősítésének lehetőségeiről. A tanácskozások időtartama alatt, 2015. október 6-án a Bíróság határozatot tett közzé a *Schrems* ügyben, amely többek között érvénytelenítette az Európai Bizottság döntését a védett adatkikötő program megfelelőségéről. A határozatot követően folytattuk a munkát szoros együttműködésben a Kereskedelmi Minisztériummal és az Európai Bizottsággal az uniós egyének adatvédelmének erősítése érdekében. Az adatvédelmi pajzs keretrendszer ezeknek a folyamatos tanácskozásoknak az eredménye. A védett adatkikötő programhoz hasonlóan az FTC ezennel elkötelezi magát az új keretrendszer hatékony végrehajtása iránt. Ez a levél rögzíti ezt a kötelezettségvállalást.

Nevezetesen, megerősítjük a kötelezettségvállalásunkat négy fontos területen: (1) megkeresések előnyben részesítése és kivizsgálása; (2) hamis vagy megtévesztő adatvédelmi pajzs részvételi nyilatkozatok tárgyalása; (3) határozatok folyamatos nyomon követése; és (4) magasabb szintű részvétel és együttműködés az uniós adatvédelmi hatóságokkal a végrehajtás során. Az alábbiakban részletes tájékoztatást adunk az egyes kötelezettségvállalásokról és az FTC szerepéről a fogyasztók adatvédelme és a védett adatkikötő végrehajtása során, valamint az Egyesült Államokban a szélesebb értelemben vett adatvédelem helyzetéről ([1]).

I. ELŐZMÉNYEK

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

([1]) További tájékoztatás található az Egyesült Államok szövetségi és állami adatvédelmi törvényeiről az A mellékletben, valamint egy összefoglaló a legutóbbi adatvédelmi és biztonsági végrehajtási tevékenységeinkről a B mellékletben. Ez az összefoglaló elérhető az FTC alábbi honlapján: https://www.ftc.gov/reports/privacy-data-security-update-2015.

végre a fogyasztók adatainak védelme és biztonsága érdekében. Az FTC által végrehajtott elsődleges törvény, az FTC törvény tiltja a kereskedelemben végrehajtott vagy arra kiható „tisztességtelen" vagy „megtévesztő" cselekedeteket vagy gyakorlatokat ([1]). Egy állítás, mulasztás vagy gyakorlat akkor megtévesztő, ha jelentős mértékű és várhatóan félrevezeti az adott körülmények között ésszerűen cselekvő fogyasztókat ([2]). Egy cselekmény vagy gyakorlat akkor tisztességtelen, ha olyan jelentős sérelmet okoz vagy várhatóan okoz, amelyet ésszerű módon nem tudnak a fogyasztók elkerülni vagy ellensúlyozni a számukra biztosított előnyökkel vagy verseny révén ([3]). Az FTC célzott alapszabályokat is végrehajt, amelyek védelmet nyújtanak az egészségre, hitel- és más pénzügyi kérdésekre, valamint a gyermekek online információira vonatkozóan, és a fenti egyes alapszabályokat végrehajtó rendelkezéseket bocsátott ki.

Az FTC törvény szerint az FTC hatásköre a „kereskedelemben végrehajtott vagy arra kiható" ügyekre vonatkozik. Az FTC nem rendelkezik hatáskörrel bűnüldözési és nemzetbiztonsági ügyekben. Az FTC a legtöbb egyéb kormányzati intézkedést sem tudja befolyásolni. Ezenkívül az FTC kereskedelmi tevékenységekre vonatkozó hatáskörére is vonatkoznak kivételek, köztük a bankok, légitársaságok, a biztosítási üzletág és a távközlési szolgáltatók közszolgáltatási tevékenysége. 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, beleértve jelentős gazdasági előnyök nyújtását ezeknek a tagoknak ([4]). Néhány esetben az FTC hatásköre egybeesik egyéb bűnüldözési hivatalok hatáskörével.

Erős munkakapcsolatot alakítottunk ki a szövetségi és állami hatóságokkal, és szorosan együttműködünk velük a vizsgálatok koordinálásában és szükség esetén megkeresések benyújtásában.

A végrehajtás az FTC adatvédelemi megközelítésének az alapja. Eddig az FTC több mint 500 adatvédelmi és fogyasztóvédelmi információbiztonsági üggyel foglalkozott. Ezek az ügyek mind offline, mind online információkkal kapcsolatosak; van köztük végrehajtási tevékenység nagy- és kisvállalatokkal szemben olyan ügyekben hogy állítólagosan elmulasztották megfelelően kezelni a fogyasztók különleges adatait, elmulasztották biztosítani a fogyasztók személyes adatait, megtévesztő módon online nyomon követték a fogyasztókat, spameket küldtek a fogyasztóknak, kémprogramokat vagy más rosszindulatú programokat telepítettek a fogyasztók számítógépére, megsértették a kéretlen telemarketinggel kapcsolatos és más telemarketing szabályokat, és nem megfelelően gyűjtöttek és osztottak meg fogyasztói információkat mobil készülékeken. Az FTC végrehajtási tevékenységei – mind a fizikai, mind a digitális világban – fontos üzenetet küldenek a vállalatoknak a fogyasztók adatvédelmének szükségességéről.

Az FTC számos politikai kezdeményezést is folytatott, amelyek célja a fogyasztók adatvédelmének javítása; ezek a kezdeményezések tájékoztatást nyújtanak az FTC végrehajtási munkájáról. Az FTC munkaértekezleteket tartott és jelentéseket adott ki a legjobb gyakorlatokról szóló ajánlásokkal, amelyek célja az adatvédelem javítása a mobil ökorendszerben; az adatkereskedelmi iparág átláthatóságának növelése; a nagy adathalmazok előnyeinek maximalizálása a kockázatok enyhítése mellett, különösen az alacsony jövedelmű és szolgáltatásokkal rosszul ellátott fogyasztók esetében; és többek között az arcfelismerés és a dolgok internete adatvédelmi és biztonsági vonatkozásainak hangsúlyozása.

Az FTC a fogyasztók és a vállalkozások képzésében is részt vesz a végrehajtási és politika-kidolgozási kezdeményezései hatásának javítása érdekében. Az FTC számos eszközt – kiadványokat, online forrásokat, munkaértekezleteket vagy a közösségi médiát – használt oktatási anyagok rendelkezésre bocsátására számos témában, például a mobil alkalmazásokkal, a gyermekek adatvédelmével és az adatbiztonsággal kapcsolatban. Legutóbb a Bizottság elindította a „Kezdjük biztonsággal" kezdeményezését, amelynek része új iránymutatás a vállalkozások számára azoknak a tanulságoknak az alapján, amelyeket a hivatal adatbiztonsági ügyekből, valamint az egész országban tartott munkaértekezletek sorozatából vont le. Ezenkívül, az FTC régóta vezető szerepet tölt be a fogyasztók alapvető számítástechnikai biztonsági oktatásában. Tavaly az OnGuard Online honlap és spanyol nyelvű változata, az Alerta en Línea több mint 5 millió oldalmegtekintést ért el.

B. **Az Egyesült Államok jogvédelme által uniós fogyasztóknak nyújtott előnyök**

A keretrendszer a nagyobb egyesült államokbeli adatvédelmi környezetben fog működni, amely számos módon védi az uniós fogyasztókat.

([1]) 15 U.S.C. § 45(a).
([2]) Lásd FTC megtévesztés-politikai nyilatkozatát, csatolva az alábbihoz: Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), lérhető: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) Lásd15 U.S.C § 45(n); FTC tisztességtelen tevékenység-politikai nyilatkozata, csatolva az alábbihoz: Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), elérhető: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) Lásd California Dental Ass'n kontra FTC, 526 U.S. 756 (1999).

Az FTC törvényben szereplő tisztességtelen és megtévesztő cselekmények és gyakorlatok tilalma nem korlátozódik az egyesült államokbeli fogyasztók egyesült államokbeli vállalatokkal szembeni védelmére, magában foglalja azokat a gyakorlatokat is, amelyek (1) ésszerűen előrelátható sérelmet okoznak vagy várhatóan okoznak majd az Egyesült Államokban, illetve (2) az Egyesült Államokban folytatott jelentős tevékenységre vonatkoznak. Ezenkívül a külföldi fogyasztók védelme során az FTC igénybe vehet minden olyan jogorvoslatot, az eredeti állapot helyreállítását is beleértve, amely rendelkezésre áll a belföldi fogyasztók védelmére.

Ténylegesen az FTC végrehajtási munkája jelentős előnyöket nyújt mind az egyesült államokbeli, mint a külföldi fogyasztók számára. Például az FTC törvény 5. pontjának érvényesítésére irányuló ügyeink egyesült államokbeli és külföldi fogyasztók adatvédelmét egyformán szolgálták. Az Accusearch információkereskedő ellen folytatott ügyben az FTC azt állította, hogy amikor a vállalat bizalmas távbeszélő-nyilvántartásokat adott el harmadik felek számára a fogyasztók tudomása vagy hozzájárulása nélkül, az tisztességtelen gyakorlat volt és megsértette az FTC törvény 5. pontját. Az Accusearch mind egyesült államokbeli, mind külföldi fogyasztókra vonatkozó információkat adott el ([1]). A bíróság gyorsított beavatkozást biztosított az Accusearch ellen, amely megtiltotta többek között a fogyasztók személyes adatainak marketingjét vagy értékesítését írásos hozzájárulás nélkül, hacsak nem jogszerűen szerezték azokat nyilvánosan elérhető információk alapján, és közel 200 000 USD jóvátételt rendelt el ([2]).

Egy másik példa az FTC megállapodása a TRUSTe-val. Ez biztosítja, hogy a fogyasztók, beleértve az uniós fogyasztókat, támaszkodhatnak egy globális önszabályozó szervezet állítására a belföldi és külföldi online szolgáltatások általa történt felülvizsgálatáról és tanúsításáról ([3]). Nagy jelentőségű, hogy a TRUSTe elleni keresetünk erősíti a szélesebb értelemben vett adatvédelmi önszabályozó rendszert azáltal, hogy biztosítja a jogi személyek elszámoltathatóságát, amelyek fontos szerepet játszanak az önszabályozó rendszerekben, beleértve a határokon átnyúló adatvédelmi keretrendszereket.

Az FTC egyéb célzott jogszabályokat is érvényre juttat, amelyek védelme kiterjed nem amerikai fogyasztókra is, mint például a gyermekek online adatvédelmi törvénye („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 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. 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. Az FTC által végrehajtott egyesült államokbeli szövetségi jogszabályok mellett bizonyos más szövetségi vagy állami fogyasztóvédelmi és adatvédelmi jogszabályok az uniós fogyasztóknak nyújtott további előnyökről rendelkezhetnek.

C. **A védett adatkikötő végrehajtása**

Az adatvédelmi és biztonság-végrehajtási programjának részeként az FTC azzal is igyekezett megvédeni az uniós fogyasztókat, hogy végrehajtási tevékenységet végzett a védett adatkikötő megsértésével kapcsolatos ügyekben. Az FTC 39, védett adatkikötővel kapcsolatos végrehajtási intézkedést hozott: 36 állítólagos hamis tanúsítási ügyben, valamint a védett adatkikötő elvek állítólagos megsértésével kapcsolatos ügyben (a Google, a Facebook és a Myspace ellen) ([4]). Ezek az ügyek bemutatták a tanúsítások végrehajthatóságát és a nemteljesítés negatív következményeit. Húszéves hozzájárulási végzések előírják a Google, a Facebook és a Myspace számára olyan átfogó adatvédelmi programok megvalósítását, amelyeket ésszerűen alakítottak ki az új és meglevő termékek és szolgáltatások fejlesztése és kezelése kapcsán felmerülő adatvédelmi kockázatok kezelésére és a személyes adatok adatvédelmének és bizalmasságának a biztosítására. A fenti végzések által elrendelt átfogó adatvédelmi programoknak azonosítaniuk kell az előrelátható jelentős kockázatokat, és rendelkezniük kell a kockázatok kezeléséről. A vállalatoknak folyamatos, független értékelést kell végeztetniük az adatvédelmi programjaik tekintetében, amelyeket át kell adni az FTC-nek. A végzések azt is megtiltják a vállalatok számára, hogy az adatvédelmi gyakorlataikkal és adatvédelmi vagy biztonsági programban való részvételükkel kapcsolatban hamis állítást tegyenek. Ez a tiltás vonatkozik a vállalatok új adatvédelmi pajzs keretrendszer szerinti cselekményeire és gyakorlataira is. Az FTC polgári szankciók eszközlésével érvényesítheti ezeket a végzéseket.

([1]) *Lásd* a kanadai adatvédelmi biztos irodájának panaszát a PIPEDA alapján az Accusearch, Inc. ellen, amely üzleti tevékenységet folytat, pl. Abika.com címen, https://www.priv.gc.ca/cf-dc/2009/20090090731e.asp. A kanadai adatvédelmi biztos irodája egy *amicus curiae* levelet nyújtott be az FTC kereset fellebbezésében és saját vizsgálatot folytatott azzal a következtetéssel, hogy az Accusearch gyakorlata megsértette a kanadai jogszabályokat is.

([2]) Lásd FTC kontra Accusearch, Inc., No. 06CV015D (D. Wyo. Dec. 20, 2007), aff'd 570 F.3d 1187 (10th Cir. 2009

([3]) Lásd a True Ultimate Standards Everywhere, Inc. ügyet, No. C-4512 (F.T.C. 2015. március 12.) (határozat és végzés), hozzáférhető az alábbi internetes oldalon: https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Lásd a Google, Inc. ügyet, No. C-4336 (F.T.C. 2011. október 13.) (határozat és végzés), hozzáférhető az alábbi internetes oldalon: https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz,a Facebook, Inc. ügyben,, No. C-4365 (F.T.C. 2012. július 27.) (határozat és végzés), hozzáférhető az alábbi internetes oldalon: https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; a Myspace LLC ügyben, No. C-4369 (F.T.C. 2012. augusztus 30.) hozzáférhető az alábbi internetes oldalon: https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

Például a Google 2012-ben rekordösszegű, 22,5 millió dolláros (USD) polgári jogi szankciót fizetett annak a vádnak a rendezése érdekében, hogy megszegte a rá vonatkozó végzést. Következésképpen ezek az FTC végzések segítenek megvédeni a több mint egymilliárd fogyasztót az egész világon és többszáz milliót Európában.

Az FTC ügyek középpontjában a védett adat kikötőben történő részvételre vonatkozó hamis, megtévesztő vagy félrevezető nyilatkozatok is álltak. Az FTC komolyan veszi ezeket a nyilatkozatokat. Például az *FTC kontra Karnani* ügy, amelyben az FTC kereset indított 2011-ben egy egyesült államokbeli közvetlen piaci üzletszerzéssel foglalkozó internetes vállalkozás ellen azt állítva, hogy ő és a vállalata azt a látszatot keltette a brit fogyasztókban, hogy a vállalat székhelye az Egyesült Királyságban van, többek között azzal, hogy a.uk kiterjesztést használta és a brit valutára és az Egyesült Királyság postai rendszerére hivatkozott ([1]). A fogyasztók azonban, amikor megkapták a termékeket, azt észlelték, hogy váratlan importvámokat kell fizetniük, a garanciák nem érvényesek az Egyesült Királyságban, és visszatérítés esetén díjakat kell fizetniük. Az FTC azzal is vádolta az alperest, hogy becsapta a fogyasztókat a védett adatkikötő programban való részvételéről. Feltűnő módon valamennyi áldozatul esett fogyasztó az Egyesült Királyságban volt.

A többi védett adatkikötő végrehajtási ügy közül sok esetben olyan szervezet volt érintett, amely csatlakozott a védett adatkikötő programhoz, de nem újította meg az éves tanúsítását, viszont továbbra is azt állította magáról, hogy még tag. Az alábbiakban bővebben tárgyaltak szerint az FTC arra is kötelezettséget vállal, hogy foglalkozik az adatvédelmi pajzs keretrendszerben történő részvételre vonatkozó hamis nyilatkozatokkal. Ez a stratégiai végrehajtási tevékenység kiegészíti a Kereskedelmi Minisztérium fokozott tevékenységeit, amelyek révén ellenőrzi a program tanúsításra és ismételt tanúsításra vonatkozó követelményeinek teljesítését, a hatékony megfelelés általa történő nyomon követését, beleértve a keretrendszer résztvevői által kitöltendő kérdőívek használatát és a fokozott törekvését arra, hogy azonosítsák a keretrendszerben történő részvételre vonatkozó hamis nyilatkozatokat, és megállapítsák a keretrendszer tanúsítási jel indokolatlan használatának eseteit ([2]).

II. MEGKERESÉSEK SORON KÍVÜLI KEZELÉSE ÉS VIZSGÁLATOK

Ahogyan a védett adatkikötő programban tettük, az FTC elkötelezi magát arra, hogy prioritást biztosít az uniós tagállamokból jövő adatvédelmi pajzs megkereséseknek. Az adatvédelmi önszabályozó szervezetektől és más független vitarendező szervektől jövő, adatvédelmi pajzs keretrendszerre vonatkozó, önszabályozó irányelveknek történő megfeleléssel kapcsolatos megkereséseknek is prioritást biztosítunk.

A keretrendszer alapján uniós tagállamokból jövő megkeresések elősegítése érdekében az FTC egy szabvány megkeresési folyamatot hoz létre és iránymutatást nyújt az uniós tagállamoknak arról, hogy milyen típusú információk tudják a legjobban segíteni FTC-t a megkeresés kivizsgálása során. Ennek keretében az FTC kijelöl egy hivatali kapcsolattartót 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.

Az uniós tagállamból vagy önszabályozó szervezettől jövő megkeresés kézhezvétele után az FTC számos intézkedést tehet a felvetett kérdés kezelésére. Például megvizsgálhatjuk a vállalat adatvédelmi szabályzatát, további információkat szerezhetünk be közvetlenül a vállalattól vagy harmadik felektől, tovább vizsgálódhatunk a megkeresést benyújtó 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 fogyasztói vagy vállalkozói képzés segíthet-e, és szükség esetén végrehajtási eljárást kezdeményezhetünk.

Az FTC a megkeresésekre vonatkozó információk megkeresést benyújtó végrehajtási hatóságokkal történő cseréje iránt is elkötelezett, 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

([1]) Lásd FTC kontra Karnani, No. 2:09-cv-05276 (C.D. Cal. 2011. május 20.) (szerződésszerűen megállapított jogerős végzés), hozzáférhető az alábbi internetes oldalon: https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; lásd még Lesley Fair, FTC Business Center Blog, Around the World in Shady Ways, http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways (2011. június 9.).

([2]) Stefan M. Selig, nemzetközi kereskedelemért felelős kereskedelmi miniszterhelyettes (Nemzetközi Kereskedelmi Igazgatóság) levele Věra Jourová jogérvényesüléséért, a fogyasztópolitikáért, és a nemek közötti esélyegyenlőségért felelős biztosnak (2016. február 23.).

végrehajtási eljárását lefolytathassa, az FTC a vizsgálat alatt álló megkeresések számát figyelembe véve, a titkosságra vonatkozó és más jogi előírások betartása mellett fog válaszolni.

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 hivataloknak, ha a külföldi hivatal olyan gyakorlatokat megtiltó jogszabályokat érvényesít, amelyek lényegileg hasonlóak azokhoz a jogszabályokhoz, amelyeket az FTC hajt végre ([1]). 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 ([2]).

Az adatvédelmi pajzs keretében uniós tagállamok és adatvédelmi önszabályozó szervezetek által benyújtott megkeresések soron kívüli kezelése mellett ([3]), az FTC elkötelezett a keretrendszer lehetséges megsértésének saját kezdeményezésre történő kivizsgálása iránt, szükség esetén számos eszköz alkalmazásával.

Több mind egy évtized óta az FTC egy hatékony programot alkalmaz kereskedelmi szervezeteket érintő adatvédelmi és biztonsági kérdések kivizsgálására. Ezen vizsgálatok részeként az FTC rendszeresen vizsgálta, hogy a kérdéses jogi személy tett-e védett adatkikötőre vonatkozó nyilatkozatokat. Ha a jogi személy ilyen nyilatkozatokat tett és a vizsgálat azt állapította meg, hogy nyilvánvalóan megsértette a védett adatkikötő adatvédelmi elveit, az FTC a végrehajtási intézkedésének részeként a védett adatkikötő megsértését is vélelmezte. Tovább folytatjuk ezt a proaktív megközelítést az új keretrendszerben is. Nagy jelentőségű, hogy az FTC sokkal több vizsgálatot folytat, amelyek végső soron nyilvános végrehajtási intézkedéseket eredményeznek. Sok FTC-vizsgálat zárul le azért, mert a munkatársak nem állapítanak meg nyilvánvaló jogsértést. Mivel az FTC-vizsgálatok nem nyilvánosak és bizalmasak, egy vizsgálat lezárultát gyakran nem hozzák nyilvánosságra.

Az FTC által a védett adatkikötő programmal kapcsolatban kezdeményezett közel 40 végrehajtási intézkedés bizonyítja a hivatal elkötelezettségét a határokon átnyúló adatvédelmi programok proaktív végrehajtása iránt. Az FTC a rendszeresen lefolytatott adatvédelmi és biztonsági vizsgálatai részeként a keretrendszer lehetséges megsértéseit kutatja.

III. HAMIS VAGY MEGTÉVESZTŐ ADATVÉDELMI PAJZS RÉSZVÉTELI NYILATKOZATOK TÁRGYALÁSA

A fent hivatkozottak szerint az FTC intézkedéseket foganatosít olyan jogi személyek ellen, amelyek hamis nyilatkozatot tesznek a keretrendszerben történő részvételükről. Az FTC soron kívül vizsgálja a Kereskedelmi Minisztérium által olyan szervezetekkel kapcsolatban benyújtott megkereséseket, amelyekről megállapítja, hogy helytelenül állítják magukról, hogy jelenleg a keretrendszer tagjai vagy engedély nélkül használnak keretrendszer tanúsítási jelet.

Ezenkívül kiemeljük, hogy ha egy szervezet adatvédelmi azt állítja, hogy megfelel az adatvédelmi pajzs elveinek, akkor ha elmulasztja a regisztrációt a Kereskedelmi Minisztériumnál vagy annak meghosszabbítását, az várhatóan önmagában nem mentesíti a szervezetet az alól, hogy az FTC végrehajtsa a keretrendszer szerinti kötelezettségvállalását.

([1]) Annak meghatározása során, hogy éljen-e az USA biztonságos web törvény szerinti jogkörével, az FTC többek között az alábbiakat fontolja meg: „(A) a kérelmező hivatal 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 hivatal 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.

([2]) A 2012–2015. pénzügyi években, például az FTC alkalmazta az USA biztonságos web törvény szerinti jogkörét arra, hogy információkat osszon meg külföldi hivataloktól kapott mintegy 60 kérelemre válaszul, és közel 60 polgári jogi vizsgálati felszólítást (amely közigazgatási idézéssel egyenértékű) bocsátott ki 25 külföldi vizsgálat segítésére.

([3]) Habár az FTC egyéni fogyasztói panaszokat nem rendez vagy közvetít, az FTC megerősíti, hogy elsőbbséget biztosít az uniós adatvédelmi hatóságok 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 polgárok számára rendelkezésre áll panaszok benyújtására az FTC-hez a www.ftc.gov/complaint internetes honlapon. Egyéni adatvédelmi pajzs panaszok esetén azonban a legjobb az lehet az uniós polgárok számára, ha a panaszokat a tagállami adatvédelmi hatósághoz vagy más vitarendezési szolgáltatóhoz nyújtják be.

IV. VÉGZÉSEK NYOMON KÖVETÉSE

Az FTC megerősíti azt a kötelezettségvállalását is, hogy nyomon követi a végrehajtási végzéseket az adatvédelmi pajzs keretrendszer megfelelés biztosítása érdekében.

Megköveteljük a keretrendszernek történő megfelelést számos megfelelő gyorsított beavatkozásra vonatkozó rendelkezéssel az FTC keretrendszerre vonatkozó jövőbeli végzéseiben. Ez tartalmazza annak a megtiltását, hogy hamis nyilatkozatokat tegyenek a keretrendszerről és más adatvédelmi programokról, ha az FTC intézkedése ezen alapul.

Az FTC eredeti védett adatkikötő program végrehajtására vonatkozó ügyei tanulságosak. A védett adatkikötő tanúsításra vonatkozó hamis vagy megtévesztő nyilatkozatokkal kapcsolatos 36 ügyben mindegyik végzés megtiltja az alperes számára a védett adatkikötőben vagy más adatvédelmi vagy biztonsági programban történő részvételre vonatkozó hamis nyilatkozat tételét, és előírja a vállalat számára a megfelelőségi jelentések hozzáférhetővé tételét az FTC számára. A védett adatkikötő adatvédelmi elvek megsértését magában foglaló ügyekben a vállalatoktól azt követelték meg, hogy átfogó adatvédelmi programokat valósítsanak meg, és ezen programok független harmadik fél általi értékelését szerezzék be minden második évben húsz éven keresztül, amelyet be kell nyújtaniuk az FTC-hez.

Az FTC közigazgatási végzéseinek a megsértése maximum 16 000 USD összegű bírságot eredményezhet jogsértésenként vagy folytonos jogsértés esetén napi 16 000 USD összegű bírságot ([1]), 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 rendszeresen nyomon követi a védett adatkikötőre vonatkozó végzések teljesítését, ahogyan minden más végzés esetében is teszi. Az FTC komolyan veszi az adatvédelmi és adatbiztonsági végzéseinek a végrehajtását és szükség esetén keresetet indít a végrehajtás érdekében. Például a fent említettek szerint a Google 22,5 millió USD összegű polgári bírságot fizetett annak a vádnak a rendezése során, hogy megsértette az FTC végzését. Nagy jelentőségű, hogy az FTC végzései továbbra is védelmet nyújtanak azoknak a fogyasztóknak az egész világon, akik kapcsolatba lépnek egy vállalkozással, nemcsak azoknak a fogyasztóknak, akik panaszt nyújtottak be.

Végezetül, az FTC továbbra is fenntart egy online listát azokról a vállalatokról, amelyekre a védett adatkikötő program vagy az új adatvédelmi pajzs keretrendszer végrehajtásával kapcsolatban végzést adtak ki ([2]). Ezenkívül, az elvek nemteljesítése miatt az FTC vagy egy bíróság végzésének hatálya alatt álló vállalatok számára az adatvédelmi pajzs elvei jelenleg előírják az FTC számára benyújtott megfelelőségi vagy értékelési jelentés keretrendszerrel kapcsolatos részeinek a közzétételét, amennyiben az összhangban van a titoktartásra vonatkozó jogszabályokkal és szabályokkal.

V. UNIÓS ADATVÉDELMI HATÓSÁGOK BEVONÁSA ÉS EGYÜTTMŰKÖDÉS A VÉGREHAJTÁS SORÁN

Az FTC elismeri az uniós adatvédelmi hatóságok által a keretrendszer teljesítésével kapcsolatban játszott fontos szerepet, és támogatja a fokozott együttműködést a tanácskozás és a végrehajtás során. Az esetspecifikus ügyekben megkeresést benyújtó adatvédelmi hatóságokkal folytatott tanácskozás mellett az FTC elkötelezett a 29. cikk szerinti munkacsoport kijelölt képviselőivel folytatott rendszeres megbeszéléseken történő részvétel iránt annak megvitatása érdekében, hogyan lehet általánosságban javítani a keretrendszerrel kapcsolatos végrehajtási együttműködést. Az FTC részt vesz a Kereskedelmi Minisztériummal, az Európai Bizottsággal és a 29. cikk szerinti munkacsoport képviselőivel együtt a keretrendszer éves felülvizsgálatában, ahol megvitatják annak megvalósítását.

Az FTC bátorítja olyan eszközök kidolgozását is, amelyek javítják az uniós adatvédelmi hatóságokkal valamint a világ más adatvédelmet végrehajtó hatóságaival a végrehajtás során folytatott együttműködést. Konkrétan az FTC az Európai Unióban és a világ többi részén levő végrehajtási partnerekkel együtt tavaly egy riasztási rendszert indított be a Globális Adatvédelem Végrehajtási Hálózat („GPEN") keretében a vizsgálatokra vonatkozó információk megosztása és a végrehajtás összehangolásának elősegítése érdekében. Ez a GPEN riasztási eszköz különösen hasznos lehet az adatvédelmi pajzs keretrendszer esetében. Az FTC és az uniós adatvédelmi hatóságok használhatják arra, hogy összehangolják az intézkedéseiket a keretrendszerrel és más adatvédelmi vizsgálatokkal kapcsolatban, beleértve kiindulásként információk cseréjét annak érdekében, hogy összehangolt és hatékonyabb adatvédelmet tudjanak biztosítani a fogyasztók

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

([2]) *Lásd* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

számára. Várakozással tekintünk a résztvevő uniós hatóságokkal végzett munka folytatására a GPEN riasztási rendszer szélesebb körű létesítése és más eszközök kidolgozása érdekében, amelyek javítják adatvédelmi ügyekben a végrehajtási együttműködést, beleértve a keretrendszerrel kapcsolatosakat.

Az FTC örömmel erősíti meg a kötelezettségvállalását, hogy végrehajtsa az új adatvédelmi pajzs keretrendszert. Szintén várakozással tekintünk az uniós kollégáink részvételére az atlanti térség két oldalán folytatott fogyasztói adatvédelem során végzett munkánk keretében.

Üdvözlettel:

Edith Ramirez

elnök

A. Függelék

Az amerikai adatvédelmi és biztonsági helyzet áttekintése az EU–USA adatvédelmi pajzs keretelveinek összefüggésében

Az EU–USA adatvédelmi pajzs keretelvei (a továbbiakban: keretelvek) által biztosított védelem az Egyesült Államok jogrendszere egésze által nyújtott szélesebb körű adatvédelem keretében létezik. Először is az Egyesült Államok Szövetségi Kereskedelmi Bizottsága (a továbbiakban: FTC) az amerikai kereskedelmi gyakorlatokra vonatkozóan egy erőteljes adatvédelmi és adatbiztonsági programmal rendelkezik, amely világszerte védelmet nyújt a fogyasztók számára. Másodszor az Egyesült Államokban a fogyasztók személyes adatai védelmének és a fogyasztók biztonságának helyzete 2000 óta, azaz a védett adatkikötőre vonatkozó eredeti USA-EU program elfogadását követően jelentős mértékben javult. Azóta több adatvédelemről és biztonságról szóló szövetségi és állami törvényt elfogadtak, valamint a magánélethez fűződő jogok érvényesítése céljából indított közérdekű és magánjogi jogviták száma jelentősen nőtt. A kereskedelmi gyakorlatra alkalmazandó, a fogyasztók személyes adatai védelmét és a fogyasztók biztonságát biztosító amerikai jogvédelem széles körű hatálya kiegészíti az új keretelvek által az uniós egyének számára biztosított védelmet.

I. AZ FTC ÁLTALÁNOS ADATVÉDELMI ÉS ADATBIZTONSÁGI PROGRAM

Az FTC a vezető amerikai fogyasztóvédelmi ügynökség, amely a kereskedelmi ágazaton belüli adatvédelemre összpontosít. A FTC hatáskörrel rendelkezik ahhoz, hogy a fogyasztói személyes adatokat sértő tisztességtelen vagy megtévesztő cselekmények vagy gyakorlatok tekintetében eljárást indítson, valamint érvényesítse azon célzottabb adatvédelmi jogszabályokat, amelyek a fogyasztókra vonatkozó egyes pénzügyi és egészségügyi információk, a gyermekekkel kapcsolatos információk, valamint bizonyos jogosultsági döntésekhez felhasznált információk védelmét szolgálják.

Az FTC egyedülálló tapasztalatokkal rendelkezik a fogyasztói személyes adatok védelme terén. Az FTC végrehajtási intézkedései egyaránt foglalkoztak az offline és online közeg jogellenes gyakorlataival. Az FTC például végrehajtási intézkedéseket hozott az olyan jól ismert vállalatokkal szemben, mint például a Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC, és a Snapchat, valamint kevésbé ismert vállalatokkal szemben is. Az FTC pert indított olyan vállalkozások ellen, amelyek állítólag a kéretlen elektronikus leveleket küldtek a fogyasztóknak, kémszoftvereket telepítettek számítógépekre, nem biztosították a fogyasztók személyes adatainak védelmét, megtévesztő módon nyomon követték a fogyasztókat az interneten, megsértették a gyermekek magánéletét, jogellenesen gyűjtöttek információkat a fogyasztók mobilkészülékein, és nem biztosították a személyes adatok tárolására használt, internethez csatlakoztatott eszközök biztonságát. A megszületett rendeletek általában rendelkeztek az FTC által egy húsz éves időszak során történő folyamatos nyomon követésről, megtiltották a további törvénysértéseket, és a vállalkozásokra a végzések megsértése miatt jelentős pénzbírságokat szabtak ki ([1]). Fontos, hogy az FTC végzései nemcsak azokat az egyéneket védik, akik egy probléma kapcsán panaszt tettek, hanem a vállalkozásokkal a jövőben kapcsolatba kerülő valamennyi fogyasztót is. A határon átnyúló ügyekben az FTC joghatósággal rendelkezik abban, hogy a fogyasztókat világszerte megvédje az Egyesült Államokban zajló gyakorlatokkal szemben ([2]).

Ezidáig az FTC több mint 130 kéretlen elektronikus levelekkel és kémszoftverekkel kapcsolatos üggyel, több mint 120 blokkolt telemarketinggel kapcsolatos üggyel, a méltányos hitelminősítésről szóló törvényt érintő több mint 100 fellépéssel, közel 60 adatbiztonsági üggyel, több mint 50 általános adatvédelmi fellépéssel, közel 30, a Gramm-Leach-Bliley törvény megsértésével kapcsolatos üggyel, valamint a gyermekek személyiségi jogainak online védelméről szóló törvény (COPPA) jogérvényesítésével kapcsolatos több mint 20 intézkedéssel foglalkozott ([3]). Ezen ügyeken felül az FTC figyelmezető leveleket is adott ki és tett közzé ([4]).

([1]) Bármely szervezet, amely nem tesz eleget az FTC-végzésnek, 16 000 USD-ig terjedő, illetve a folyamatos szabálysértés esetén napi 16 000 USD polgári bírsággal sújtható. *Lásd* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

([2]) A Kongresszus kifejezetten megerősítette az FTC azon hatáskörét, hogy jogorvoslatot kérhessen – ideértve a helyreállítást – minden olyan külkereskedelmet érintő cselekmény vagy gyakorlat esetében, amely (1) megalapozottan előrelátható kárt okoz vagy okozhat, vagy (2) az Egyesült Államokon belül történő érdemi cselekményt foglal magában. *Lásd* 15 U.S.C. § 45(a)(4).

([3]) Bizonyos esetekben az FTC az adatvédelmi és adatbiztonsági ügyekben azt állítja, hogy a vállalat egyszerre folytatott megtévesztő és tisztességtelen gyakorlatokat; ezekben az ügyekben esetenként több jogszabályt – például a méltányos hitelminősítésről szóló törvényt, a Gramm-Leach-Bliley törvényt és a gyermekek személyiségi jogainak online védelméről szóló törvényt – is megsértettek.

([4]) *Lásd például* a Szövetségi Kereskedelmi Bizottság „FTC Warns Children's App Maker BabyBus About Potential COPPA Violations" (Az FTC figyelmezteti a gyermekeknek szóló alkalmazásokat gyártó BabyBus-t a COPA esetleges megsértésére) című sajtóközleményét (2014. december 22.), https://www.ftc.gov/news-events/press- releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; a Szövetségi Kereskedelmi Bizottság „FTC Warns Data Broker Operations of Possible Privacy Violations" (Az FTC figyelmezteti az adatbrókereket az adatvédelem esetleges megsértésére) című sajtóközleményét (2013. május 7.), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible- privacy-violations; a Szövetségi Kereskedelmi Bizottság „FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act" (Az FTC figyelmezteti a bérlőminősítő adatokat nyújtó adatbrókereket a méltányos hitelminősítésről szóló törvény esetleges megsértésére) című sajtóközleményét (2013. április 3.), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental- histories-they-may.

A szigorú adatvédelmi gyakorlat részeként az FTC rendszeresen megvizsgálta a védett adatkikötőre vonatkozó programmal kapcsolatos esetleges jogsértéseket is. A védett adatkikötőre vonatkozó program elfogadása óta az FTC hivatalból számos vizsgálatot folyatott a programnak való megfelelés tekintetében, és 39 ügyben indított lejárást amerikai vállalatok ellen a védett adatkikötőre vonatkozó program megsértése miatt. Az FTC továbbra is alkalmazza ezt a proaktív megközelítést azáltal, hogy az új keretelvek érvényesítését kiemelten kezeli.

II. A FOGYASZTÓI SZEMÉLYES ADATOK SZÖVETSÉGI ÉS ÁLLAMI SZINTŰ VÉDELME

A biztonságos kikötő végrehajtásának áttekintése – amely a biztonságos kikötő megfelelőségéről szóló bizottsági határozat mellékleteként szerepel – magában foglal több olyan szövetségi és állami adatvédelmi törvény összefoglalóját, amelyek a védett adatkikötőre vonatkozó program 2000. évi elfogadása idején hatályban volt ([1]). Abban az időben számos szövetségi jogszabály szabályozta a személyes adatok kereskedelmi összegyűjtését és felhasználását az FTC törvény 5. szakaszának hatályán túlmenően, ideértve a következőket: a kábel távközlési politikáról szóló törvény, a gépjárművezetők adatainak védelméről szóló törvény, az elektronikus távközlési adatvédelmi törvény, az elektronikus pénzátutalási törvény, a méltányos hitelminősítésről szóló törvény, a Gramm-Leach-Bliley törvény, a pénzügyi adatok védelméről szóló törvény, a telefonos fogyasztóvédelmi törvény és a videokölcsönzési adatok védelméről szóló törvény. Sok államban hasonló jogszabályok vannak ezeken a területeken.

2000 óta számos előrelépés történt mind szövetségi, mind pedig állami szinten a fogyasztói személyes adatok további védelmének biztosítására ([2]). Szövetségi szinten például 2013-ban az FTC módosította a COPPA törvényt a gyermekek személyes adatainak további védelme érdekében. Az FTC a Gramm- Leach-Bliley törvényt végrehajtó két szabályt adott ki – az adatvédelmi szabályt és a biztosítékokra vonatkozó szabályt – amelyek előírják a pénzügyi intézmények ([3]) számára, hogy információkat tegyenek közzé az információmegosztás gyakorlatairól és hajtsanak végre átfogó információbiztonsági programot a fogyasztói adatok védelme érdekében ([4]). Hasonlóképpen a 2003-ban elfogadott, a tisztességes és pontos hitelügyletekről szóló törvény (FACTA) kiegészíti a régóta hatályos amerikai hiteltörvényeket bizonyos érzékeny pénzügyi adatok elrejtésére, megosztására és megsemmisítésére vonatkozó követelmények létrehozása érdekében. Az FTC a FACTA alapján számos szabályt hirdetett ki többek között a következőkre vonatkozóan: a fogyasztó joga az ingyenes éves hitelinformációhoz; a fogyasztói jelentésekben szereplő információk biztonságos megsemmisítésére vonatkozó követelmények; a fogyasztó joga bizonyos hitel- és biztosítási ajánlatok visszautasításához; a fogyasztó joga a termékeit és szolgáltatásait értékesítő kapcsolt vállalkozás által nyújtott információk felhasználásának visszautasításához; a pénzügyi intézményekre és hitelezőkre vonatkozó kötelezettség a személyazonosság-lopás felderítésére és megelőzésére irányuló programok végrehajtása tekintetében ([5]). Ezen felül 2013-ban felülvizsgálták az egészségbiztosítás hordozhatóságáról és elszámolási kötelezettségéről szóló törvény szerint kihirdetett szabályokat, és kiegészítették azokat a személyes egészségügyi adatok védelmével és biztonságával kapcsolatos további biztosítékokkal ([6]). Szintén hatályba léptek a fogyasztók nem kívánt telemarketing hívásokkal, robothívásokkal és kéretlen elektronikus levelekkel szembeni védelmét biztosító szabályok. A Kongresszus elfogadta azt a törvényt, amely az egészségügyi információkat gyűjtő bizonyos vállalatok számára előírja fogyasztók tájékoztatását az adatok sérelme esetén ([7]).

Az államok szintén aktívak voltak az adatvédelmi és biztonsági törvények elfogadása terén. 2000 óta 47 állam, Columbia Kerület (District of Columbia), Guam, Puerto Rico és a Virgin-szigetek olyan törvényeket fogadtak el, amelyek

([1]) *Lásd* U.S. Dep't of Commerce, Safe Harbor Enforcement Overview (az Egyesült Államok Kereskedelmi Minisztériuma, A biztonságos kikötő végrehajtásának áttekintése) https://build.export.gov/main/safeharbor/eu/eg main 018481.

([2]) Az amerikai jogvédelem átfogóbb áttekintését lásd Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (Az információvédelemre vonatkozó törvények, 5. kiadás 2015).

([3]) A pénzügyi intézmények fogalmát a Gramm-Leach-Bliley törvény igen tágan határozza meg, ideértve minden olyan vállalkozást, amely „jelentős mértékben" nyújt pénzügyi termékeket vagy szolgáltatásokat. Mindez magában foglalja például a csekkbeváltó vállalkozásokat, gyorskölcsönt nyújtó vállalkozásokat, jelzálogügynököket, nem banki hitelezőket, személyes tulajdon vagy ingatlan értékbecslőket, hivatásos adótanácsadókat.

([4]) A pénzügyi fogyasztóvédelemről szóló 2010. évi törvény (CFPA) – (X. cím Pub. L. 111-203, 124 Stat. 1955) (2010. július 21.), más néven Dodd–Frank-törvény (Dodd-Frank Wall Street Reform and Consumer Protection Act) – szerint a Gramm-Leach-Bliley törvény által az FTC-re ruházott hatáskör nagy részét a pénzügyi fogyasztóvédelmi hivatalra (Consumer Financial Protection Bureau, CFPB) ruházták át. Az FTC megtartja a Gramm-Leach-Bliley törvény szerinti végrehajtási hatáskörét, valamint a biztosítékokra vonatkozó szabály tekintetében a szabályozói hatáskörét, továbbá a gépjármű-kereskedők tekintetében az adatvédelmi szabály alapján korlátozott hatáskörrel rendelkezik.

([5]) A CFPA szerint az FTC megosztja a méltányos hitelminősítésről szóló törvénnyel kapcsolatos végrehajtási szerepét az CFPB-vel, azonban a szabályozói hatáskörének nagy részét a CFPB-re ruházták (kivéve a figyelmeztető jelzésekre és a megsemmisítésre vonatkozó szabályok tekintetében).

([6]) *Lásd* 45 C.F.R. 160., 162., 164. pontja

([7]) *Lásd például* American Recovery & Reinvestment Act of 2009 (a 2009. évi amerikai gazdaságélénkítő törvény), Pub. L. No. 111-5, 123 Stat. 115 (2009) és a vonatkozó szabályozást, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. 318. pont.

arra kötelezik a vállalkozásokat, hogy a személyes adatok biztonságának megsértéséről tájékoztassák az egyéneket ([1]). Legalább 32 állam és Puerto Rico rendelkezik adatmegsemmisítési törvényekkel, amelyek meghatározzák a személyes információk megsemmisítésére vonatkozó követelményeket ([2]). Számos állam fogadott el általános adatbiztonsági törvényt. Ezen felül Kalifornia számos adatvédelmi törvényt fogadott el, ideértve egy olyan törvényt, amely előírja a vállalatok számára, hogy adatvédelmi politikával rendelkezzenek és tegyék nyilvánossá a Do Not Track („ne kövess nyomon") gyakorlataikat ([3]), a „Shine the Light" törvény, amely az adatbrókerek számára nagyobb átláthatóságot ír elő ([4]), valamint egy olyan törvényt, amely felhatalmazást ad egy olyan „törlőgomb" létrehozására, amely lehetővé teszi a kiskorúak számára, hogy a közösségi médiában szereplő egyes információkat törölhessék ([5]). E törvények és egyéb hatáskörök révén a szövetségi és állami kormányok jelentős bírságokat szabtak ki azon vállalatokra, amelyek elmulasztották a fogyasztói személyes adatok védelmének és biztonságának biztosítását ([6]).

A magánperek szintén sikeres ítéletekhez és perbeli egyezségekhez vezettek, amelyek további adatvédelmet és -biztonságot nyújtanak a fogyasztók számára. 2015-ben például a Target beleegyezett abba, hogy 10 millió USD összeget fizessen egy perbeli egyezség keretében azon fogyasztók számára, aki állítása szerint személyes pénzügyi információik egy széles körű adatvédelmi szabálysértés során veszélybe kerültek. 2013-ban az AOL beleegyezett abba, hogy 5 millió USD összeget fizessen az ellene indított kollektív kereset rendezése érdekében, mivel az állítások szerint több százezer AOL tag keresési eredményeinek közzététele során az anonimizálás nem volt megfelelő. Ezen felül egy szövetségi bíróság jóváhagyta a kölcsönzési információknak a videokölcsönzési adatok védelméről szóló 1988. évi törvény sértő állítólagos megőrzése miatt a Netflix által fizetendő 9 millió USD összeget. A kaliforniai szövetségi bíróságok két különböző perbeli egyezséget hagytak jóvá a Facebook esetében – 20 millió USD, illetve 9,5 millió USD összegben – a felhasználók személyes információinak a vállalat által történt gyűjtése, felhasználása és megosztása vonatkozásában. 2008-ban Kalifornia állami bírósága jóváhagyta a LensCrafters-szel kötött 20 millió USD összegű perbeli egyezséget a fogyasztók egészségügyi adatainak jogellenes nyilvánosságra hozatala miatt.

Ahogy azt az ezen összefoglaló is szemlélteti, az Egyesült Államok jelentős jogvédelmet biztosít a fogyasztók adatvédelme és biztonsága terén. Az adatvédelmi pajzs új keretelvei. amelyek az uniós egyének számára valódi biztosítékokat nyújtanak, e széleskörű háttérrel fognak működni, amelyben továbbra is kiemelt szerepet játszik a fogyasztók adatainak védelme és biztonsága.

([1]) *Lásd*, National Conference of State Legislatures (NCSL), *State Security Breach Notification Laws* (a jogalkotók nemzeti konferenciája, Az állambiztonság megsértésének bejelentéséről szóló törvények) (2016. január 4.), *elérhető a következő linken:* http://www.ncsl.org/research/telecommunications-and-information- technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (adatmegsemmistési törvények) (2016. január 12.), *elérhető a következő linken:* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) *Lásd*Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*(Az USA világelső az adatvédelmi bírságok kiosztásában), Computerworld (2014. február 17.),*elérhető a következő linken:* http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

V. MELLÉKLET

Anthony Foxx amerikai közlekedési miniszter levele

2016. február 19.

Vera Jourová biztos
Európai Bizottság
Rue de la Loi/Wetstraat 200
1049 l049 Brussels
Belgium

Tárgy: EU-USA adatvédelmi pajzs adatvédelmi pajzs keretrendszer

Tisztelt Jourová biztos asszony!

Az Egyesült Államok Közlekedési Minisztériuma („Minisztérium" vagy „DOT") nagyra értékeli a lehetőséget, hogy leírhatja az EU-USA adatvédelmi pajzs keretrendszer végrehajtásában játszott szerepét. Ez a keretrendszer kritikus szerepet játszik a kereskedelmi tranzakciók keretében továbbított személyes adatok védelmében az egyre inkább összefonódó világban. Lehetővé teszi a vállalkozások számára fontos tevékenységek végzését a globális gazdaságban, ugyanakkor biztosítja az uniós fogyasztók fontos adatvédelmének fenntartását.

A DOT először több mint 15 évvel ezelőtt fejezte ki elkötelezettségét a védett adatkikötő keretrendszer végrehajtása iránt egy Európai Bizottságnak küldött levélben. Abban a levélben a DOT vállalta a védett adatkikötő adatvédelmi elvek a hatékony végrehajtását. A DOT továbbra is fenntartja ezt a kötelezettségvállalását és ez a levél rögzíti ezt a kötelezettségvállalást.

Nevezetesen a DOT megismétli a kötelezettségvállalását az alábbi fontos területeken: (1) az adatvédelmi pajzs állítólagos megsértésének soron kívüli kivizsgálása; (2) megfelelő végrehajtási intézkedések olyan jogi személyek ellen, amelyek hamis vagy megtévesztő nyilatkozatokat tesznek az adatvédelmi pajzs tanúsításról; és (3) az adatvédelmi pajzs megsértésével kapcsolatos végzések végrehajtásának nyomon követése és közzététele. Tájékoztatást adunk az egyes kötelezettségvállalásokról és a szükséges mértékben a DOT eddigi szerepéről a fogyasztói adatvédelem területén és az adatvédelmi pajzs keretrendszer végrehajtása során.

I. ELŐZMÉNYEK

A. **A DOT adatvédelmi hatásköre**

A Minisztérium erősen elkötelezett a fogyasztók által a légitársaságok és jegyértékesítők számára nyújtott információk védelmének biztosítása iránt. A DOT e területen foganatosított intézkedésekre vonatkozó hatáskörének az alapja a 49 U. S.C. 41712, amely megtiltja a fuvarozók és a jegyértékesítők számára, hogy „tisztességtelen vagy megtévesztő gyakorlatot folytassanak vagy tisztességtelen verseny módszereket alkalmazzanak" a légi közlekedés értékesítése során, amely a fogyasztók sérelmét eredményezi vagy várhatóan eredményezi. A 41712. szakasz a Szövetségi Kereskedelmi Bizottságról szóló törvény (15 U. S. C. 45) 5. szakasza mintájára épül fel. A mi értelmezésünk szerint a tisztességtelen vagy megtévesztő gyakorlatról szóló alapszabály megtiltja a légitársaságok és a jegyértékesítők számára az alábbiakat: (1) az adatvédelmi szabályzatuk feltételeinek a nemteljesítése; vagy (2) magánjellegű információk gyűjtése vagy felfedése olyan módon, amely ellentétes a közrenddel, erkölcstelen vagy jelentős sérelmet okoz a fogyasztóknak, és ezt nem ellensúlyozzák előnyök. Az értelmezésünk szerint a 41712. szakasz megtiltja a légitársaságok és jegyértékesítők számára az alábbiakat is: (1) a Minisztérium által kiadott olyan szabályok megsértése, amelyek konkrét adatvédelmi gyakorlatokat tisztességtelennek vagy megtévesztőnek minősítenek; vagy (2) a gyermekek online adatvédelmi törvényének (COPPA) vagy a COPPA FTC általi megvalósítását jelentő szabályoknak a megsértése. 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 adatvédelmi pajzs keretrendszer adatvédelmi elvek 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 adatvédelmi pajzs keretrendszer adatvédelmi elveinek a követését, akkor az elvek be nem tartása a 41712. szakasz megsértésének minősülne.

B. **Végrehajtási gyakorlat**

A Minisztérium légi közlekedés végrehajtási és eljárási irodája (Légi Közlekedés Végrehajtási Iroda) 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,. Az iroda az esetleges jogsértésekről leginkább magánszemélyektől, utazási irodáktól, légitársaságoktól, valamint az Egyesült Államok és más országok kormányzati ügynökségeitől értesül. A fogyasztók a DOT honlapját használhatják adatvédelmi panaszok benyújtására a légitársaságok és jegyértékesítők ellen ([1]).

Ha egy ügyben nem jutnak ésszerű és megfelelő megállapodásra, a Légi Közlekedés Végrehajtási Iroda 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 27 500 USD.

A Minisztériumnak nem áll hatáskörében kártérítés vagy pénzügyi jóvátétel megítélése az egyéni felperes számára. A Minisztérium azonban rendelkezik hatáskörrel a Légi Közlekedés Végrehajtási Iroda 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 adatvédelmi pajzs keretrendszer elvei kapcsán is így történhet. Ha egy légitársaság ismételten megsértené 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 jegyértékesítők vagy légitársaságok adatvédelmi rendelkezések állítólagos megsértésére vonatkozott. Ilyen esetekben a fenti elvek szerint történik a vizsgálat.

C. **A DOT által 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.

A DOT a légitársaságok kapcsán egyéb célzott jogszabályokat is végrehajt, amelyek védelme kiterjed nem amerikai fogyasztókra is, mint például a 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 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 tételére.

II. AZ ADATVÉDELMI PAJZS VÉGREHAJTÁSA

Ha egy légitársaság vagy jegyértékesítő úgy dönt, hogy részt vesz az adatvédelmi pajzs keretrendszerben és a Minisztériumhoz olyan panasz érkezik, amely szerint a légitársaság vagy a jegyértékesítő állítólagosan megsértette a keretrendszert, a Minisztérium az alábbi lépéseket teszi a keretrendszer hatékony végrehajtása érdekében.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Állítólagos jogsértések soron kívüli kivizsgálása**

A Minisztérium Légi Közlekedés Végrehajtási Irodája kivizsgál minden egyes panaszt, amely az adatvédelmi pajzs megsértését állítja (beleértve az uniós adatvédelmi hatóságoktól kapott panaszokat), és végrehajtási intézkedéseket tesz, ha bizonyíték van a jogsértésre. Ezenkívül a Légi Közlekedés Végrehajtási Iroda együttműködik az FTC-vel és a Kereskedelmi Minisztériummal és soron kívül vizsgálja azokat az állításokat, amelyek szerint a szabályozás alá eső jogi személyek nem teljesítik az adatvédelmi pajzs keretrendszerben tett adatvédelmi kötelezettségvállalásaikat.

Az adatvédelmi pajzs keretrendszer állítólagos megsértésére vonatkozó panasz kézhezvétele után a Minisztérium Légi Közlekedés Végrehajtási Irodája 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 tudomására jut az adatvédelmi pajzs jegyértékesítők általi esetleges megsértése, akkor egyeztet az FTC-vel az ügyről.Ezen túlmenően tájékoztatjuk az FTC-t és a Kereskedelmi Minisztériumot az adatvédelmi pajzs végrehajtási intézkedések eredményeiről.

B. **Hamis vagy megtévesztő részvételi nyilatkozatok tárgyalása**

A Minisztérium továbbra is elkötelezett az adatvédelmi pajzs megsértésének kivizsgálása iránt, beleértve az adatvédelmi pajzs program tagságára 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 adatvédelmi pajzs keretrendszer tagjai vagy engedély nélkül használják a keretrendszer tanúsítási jelet.

Ezenkívül kiemeljük, hogy ha egy szervezet adatvédelmi szabályzata azt állítja, hogy megfelel az adatvédelmi pajzs lényeges elveinek, akkor ha elmulasztja a regisztrációt a Kereskedelmi Minisztériumnál vagy annak meghosszabbítását, az várhatóan önmagában nem mentesíti a szervezetet az alól, hogy a DOT végrehajtsa a kötelezettségvállalását.

C. **Az adatvédelmi pajzzsal kapcsolatos végrehajtási végzések nyomon követése és közzététele**

A Minisztérium Légi Közlekedés Végrehajtási Irodája továbbra is elkötelezett aziránt, hogy nyomon követi a végrehajtási végzéseket az adatvédelmi pajzs program teljesítésének biztosítása érdekében. Konkrétan, ha az iroda olyan végzést ad ki, amely utasítja a légitársaságot vagy jegyértékesítőt az adatvédelmi pajzs és a 41712. szakasz jövőbeli megsértésének abbahagyására, akkor nyomon követi a végzésben levő abbahagyásra vonatkozó rendelkezés teljesítését. Ezenkívül, az iroda biztosítja, hogy az adatvédelmi pajzs ügyekből eredő végzések elérhetők legyenek a honlapján.

Várakozással tekintünk a szövetségi partnereinkkel és uniós érintett felekkel végzett munkánk folytatására az adatvédelmi pajzzsal kapcsolatos ügyekben.

Remélem, hogy a fenti tájékoztatás hasznosnak bizonyul. Amennyiben még kérdése van, vagy további felvilágosításra volna szüksége, kérem, forduljon hozzám bizalommal.

Üdvözlettel:

Anthony R. Foxx

közlekedési miniszter

VI. MELLÉKLET

Robert Litt főtanácsos levele
A nemzeti titkosszolgálat igazgatójának hivatala

2016. február 22.

Justin S. Antonipillai úr
Tanácsos
Az USA Kereskedelmi Minisztériuma
1401 Constitution Ave., NW
Washington, DC, 20230

Ted Dean úr
államtitkár-helyettes
Nemzetközi Kereskedelmi Minisztérium
1401 Constitution Ave., NW
Washington, DC, 20230

Tisztelt Antonipillai és Dean úr!

Az elmúlt két és fél év során az EU-USA adatvédelmi pajzs érdekében folytatott tárgyalásokkal összefüggésben az Egyesült Államok érdemi tájékoztatást adott az USA hírszerző közössége jelfelderítési tevékenységének működéséről. Ennek részét képezték a irányadó jogi keretre, e tevékenységek többrétű felügyeletére, a tevékenységekkel kapcsolatos kiterjedt átláthatóságra, és a magánélet, illetve az alapvető szabadságjogok átfogó védelmére vonatkozó információk – annak érdekében, hogy az Európai Bizottságot segítsük annak eldöntésében, hogy a védelem megfelelő-e, mivel az adatvédelmi pajzs elvei alóli nemzetbiztonsági kivételhez kapcsolódnak. Ez a dokumentum az átadott információkat foglalja össze.

I. A PPD-28 ÉS AZ USA JELFELDERÍTŐ TEVÉKENYSÉGÉNEK FOLYTATÁSA

Az USA hírszerző közössége körültekintően szabályozott módon, az USA jogszabályait szigorúan betartva gyűjt külföldi információkat, többrétű ellenőrzés mellett, a fontos külföldi információkra és nemzetbiztonsági prioritásokra összpontosítva. Az USA jelfelderítő tevékenységére sokféle jogszabály és szabályzat vonatkozik, ideértve az USA alkotmányát, a külföldi hírszerzői tevékenység megfigyeléséről szóló törvényt (50 U.S.C. § 1801 *és ezt követő rendelkezések*) (FISA), a 12333 sz. elnöki rendeletet és annak végrehajtási eljárásait, elnöki iránymutatásokat, valamint a FISA-bíróság és a legfőbb ügyész által jóváhagyott számos eljárást és útmutatót, amelyek további, a külföldi hírszerzési adatok gyűjtését, megőrzését, felhasználását és terjesztését korlátozó szabályokat állapítanak meg ([1]).

a. **A PPD 28 áttekintése**

Obama elnök 2014 januárjában tartott egy beszédet az USA jelfelderítő tevékenységének különféle reformjairól, valamint ezekről a tevékenységekről elnöki szakpolitikai irányelvet (Presidential Policy Directive 28 – PPD-28) adott ki ([2]). Az elnök hangsúlyozta, hogy az USA jelfelderítő tevékenysége nemcsak országa és annak szabadságjogai garantálásában segít, hanem az uniós tagállamokat is beleértve más olyan országok biztonságának és szabadságjogainak védelmét is előmozdítja, amelyek saját polgáraik védelme végett az USA hírszerző ügynökségeinek információira hagyatkoznak.

A PPD-28 olyan elvek és követelmények sorát állapítja meg, amelyek az USA valamennyi jelfelderítő tevékenységére és – állampolgárságra vagy tartózkodási helyre tekintet nélkül – mindenkire vonatkoznak. Meghatároz különösen bizonyos követelményeket az amerikai jelfelderítés keretében szerzett, nem egyesült államokbeli személyekre vonatkozó személyes adatok gyűjtésével, megőrzésével és terjesztésével kapcsolatos eljárásokra. Ezek a követelmények a későbbiekben részletesen kifejtésre kerülnek, de összefoglalva az alábbiak:

— A PPD megismétli, hogy az Egyesült Államok csak törvény, elnöki rendelet vagy más elnöki irányelv felhatalmazásának megfelelően gyűjt jelfelderítési adatokat.

([1]) Az USA külföldi hírszerzési tevékenységére vonatkozó további információk elérhetőek az interneten és a nyilvánosság számára elérhetőek az IC on the Record (www.icontherecord.tumblr.com) szolgáltatáson – az ODNI kormányzati hírszerzés nagyobb nyilvánosságának támogatására szentelt nyilvános webhelyén – keresztül.
([2]) *Elérhető itt:* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— A PPD eljárásrendet hoz létre azt biztosítandó, hogy a jelfelderítési tevékenységet csak jogszerű és megengedett nemzetbiztonsági célok előmozdítására végezzék.

— A PPD előírja továbbá, hogy jelfelderítési tevékenységek tervezésekor a magánéletnek és az alapvető szabadságjogoknak központi megfontolásnak kell lennie. Az Egyesült Államok nem gyűjt hírszerzési adatokat különösen bírálat vagy egyet nem értés elnyomására; személyek etnikumuk, fajuk, nemük, szexuális beállítottságuk vagy vallásuk alapján történő hátrányos megkülönböztetésére; vagy pedig egyesült államokbeli vállalatok vagy üzleti ágazatok számára kereskedelmi versenyelőny biztosítására.

— A PPD előírja, hogy a jelfelderítési adatok gyűjtésének a lehető legcélzottabbnak kell lennie, és a tömeges jelfelderítési adatgyűjtés csak konkrét megnevezett célokra használható fel.

— A PPD előírja, hogy a hírszerző közösség olyan eljárásrendeket fogad el, amelyek „kialakítása ésszerűen a minimumra csökkenti a jelfelderítési tevékenységekből gyűjtött személyes adatok terjesztését és megőrzését", és kiterjeszti különösen az egyesült államokbeli személyek személyes adataira vonatkozó védelmet nem egyesült államokbeli személyek adataira.

— A PPD-28-at végrehajtó hivatali eljárásrendek elfogadása és közzététele megtörtént.

Egyértelmű, hogy az itt meghatározott eljárások és védelem az adatvédelmi pajzsra is vonatkozik. Amennyiben Egyesült Államokban található vállalatokhoz történik adatok továbbítása az adatvédelmi pajzsnak megfelelően vagy ténylegesen bármilyen módon, az egyesült államokbeli hírszerző ügynökségek csak akkor kérhetik le ezeket az adatokat a vállalatoktól, ha a kérés a FISA-nak megfelel, vagy azt az alábbiakban ismertetett valamely nemzetbiztonsági levél jogszabályi rendelkezései szerint küldik meg ([1]). Emellett – az azt állító médiabeszámolók megerősítése vagy tagadása nélkül, hogy az USA hírszerző közössége adatokat gyűjt az Atlanti óceánt átszelő kábeleken történő adatforgalomból – ha az USA hírszerző közössége az Atlanti óceánt átszelő kábelekről gyűjtene adatokat, arra is vonatkoznának az itt ismertetett korlátozások és biztosítékok, beleértve a PPD-28 követelményeit is.

b. **Az adatgyűjtés korlátai**

A PPD-28 több jelentős általános elvet rögzít, amelyek a a jelfelderítési adatok gyűjtését szabályozzák:

— A jelfelderítési adatok gyűjtését törvénynek vagy elnöki felhatalmazásnak kell engedélyeznie, és azt az alkotmánynak és a törvényeknek megfelelően kell végezni.

— A magánélet és az alapvető szabadságjogok védelmének a jelfelderítési tevékenységek tervezésekor alapvető megfontolásnak kell lennie.

— Jelfelderítési adatok gyűjtésére csak akkor kerül sor, amikor annak érvényes külföldi hírszerzési vagy kémelhárítási célja van.

— Az Egyesült Államok nem fog jelfelderítési adatokat gyűjteni bírálat vagy egyet nem értés elfojtására vagy megnehezítésére.

— Az Egyesült Államok nem fog jelfelderítési adatokat gyűjteni abból a célból, hogy személyeket etnikumuk, fajuk, nemük, szexuális beállítottságuk vagy vallásuk alapján hátrányosan megkülönböztessen.

— Az Egyesült Államok nem fog jelfelderítési adatokat gyűjteni abból a célból, hogy egyesült államokbeli vállalatok vagy üzleti ágazatok számára kereskedelmi versenyelőnyt biztosítson.

— Az Egyesült Államok jelfelderítési tevékenységének *minden esetben* a lehető legcélzottabbnak kell lennie, figyelemmel az elérhető egyéb információforrásokra. Ez egyebek mellett azt is jelenti, hogy – amennyiben az a gyakorlatban megvalósítható – a jelfelderítési adatok gyűjtési tevékenységét célzottan, nem pedig tömegesen végzik.

Az a követelmény, hogy a jelfelderítési tevékenységnek „a lehető legcélzottabbnak kell lennie", vonatkozik a jelfelderítési adatok gyűjtésének módjára és a ténylegesen gyűjtött adatok körére is. Például annak meghatározásakor, hogy kell-e

([1]) A bűnüldöző vagy szabályozó szervek az Egyesült Államokban vizsgálati célokra olyan információkat is bekérhetnek vállalatoktól a más büntető, polgári és szabályozó hatóságokra előírtak szerint, amelyek kívül esnek e dokumentum keretein, de ez a nemzetbiztonsági hatóságokra korlátozódik.

jelfelderítési adatokat gyűjteni, a hírszerző közösségnek figyelembe kell vennie egyéb információk elérhetőségét, beleértve a diplomáciai vagy állami forrásokat, és az adatgyűjtésben ezeknek az eszközöknek kell prioritást biztosítania, amennyiben ez ésszerű és megvalósítható. Emellett a hírszerző közösség tagjai szabályzatainak elő kell írniuk, hogy amennyiben az a gyakorlatban megvalósítható, az adatgyűjtést konkrét külföldi hírszerzési célpontokra vagy témakörökre kell koncentrálni, diszkriminánsok (pl. konkrét létesítmények, kiválasztási feltételek és azonosítók).

Fontos a Bizottságnak adott tájékoztatást egészében nézni. Annak eldöntését, hogy mi a „megvalósítható" vagy „gyakorlatban megvalósítható", nem bízzák egyéni mérlegelésre, hanem azt a hivatalok PPD-28 alapján kiadott és nyilvánosságra hozott szabályzatai és az itt ismertetett többi eljárás rendezi ([1]). Amint azt a PPD-28 kimondja, a jelfelderítési adatok tömeges gyűjtése az az adatgyűjtés, amely „műszaki vagy operatív megfontolások miatt diszkriminánsok (pl. konkrét azonosítók, kiválasztási feltételek stb.) használata nélkül történik." Ebben a vonatkozásban a PPD-28 elismeri, hogy a hírszerző közösség tagjainak bizonyos körülmények között a jelfelderítési adatokat tömegesen kell gyűjteniük az új vagy kialakuló veszélyek és más létfontosságú nemzetbiztonsági információk azonosítására, amelyek gyakran el vannak rejtve a modern globális kommunikáció hatalmas és összetett rendszerében. Elismeri továbbá a magánélettel és az alapvető szabadságjogokkal kapcsolatban a jelfelderítési adatok tömeges gyűjtésekor felmerülő aggályokat. A PPD-28 ezért a hírszerző közösséget arra utasítja, hogy részesítse előnyben azokat a lehetőségeket, amelyek a jelfelderítési adatok tömeges gyűjtése helyett azok célzott gyűjtését teszik lehetővé. Ennélfogva a hírszerző közösség tagjainak minden olyan esetben, amikor az a gyakorlatban megvalósítható, a jelfelderítési adatok tömeges gyűjtése helyett célzott gyűjtést kell végeznie ([2]). Ezek az elvek biztosítják, hogy a tömeges adatgyűjtés alóli kivételek ne iktassák ki az általános szabályt.

Az „ésszerűség" fogalmát illetően: ez az USA jogának alapköve. Azt jelzi, hogy a hírszerző közösség tagjai számára nem kötelező minden elméletileg lehetséges intézkedés elfogadása, hanem ehelyett egyensúlyt kell teremteniük a magánélet és az alapvető szabadságjogok védelméhez fűződő érdek jogszerű védelmére irányuló erőfeszítéseik és a jelfelderítési tevékenységek gyakorlati szükségletei között. Ebben a kérdésben is elérhetőek a hivatalok szabályzatai, és bizonyosságot nyújthatnak arra, hogy a „kialakítása ésszerűen a minimumra csökkenti a jelfelderítési tevékenységekből gyűjtött személyes adatok terjesztését és megőrzését" megfogalmazás ne gyengítse az általános szabályt.

A PPD-28 előírja továbbá, hogy a tömeges jelfelderítési adatgyűjtés csak hat konkrét célra használható fel: külföldi hatalmak bizonyos tevékenységeinek felkutatása és megakadályozása; terrorizmus elleni küzdelem; fegyverek elterjedése elleni küzdelem; kiberbiztonság; az USA-t vagy szövetséges fegyveres erőket fenyegető veszélyek felkutatása és elhárítása; valamint nemzetközi bűnügyi fenyegetések elleni küzdelem, ideértve a szankciók megkerülését. Az elnök nemzetbiztonsági tanácsadója a nemzeti hírszerzés igazgatójával (Director for National Intelligence – DNI) egyeztetve évente felülvizsgálja a tömeges jelfelderítési adatgyűjtés megengedett felhasználási módjait annak felmérésére, hogy azokat szükséges-e megváltoztatni. A DNI ezt a listát a nemzetbiztonsággal összeegyeztethető legnagyobb mértékben nyilvánosan elérhetővé teszi. Ez fontos és átlátható korlátot szab a tömeges jelfelderítési adatgyűjtés felhasználása elé.

Ezen túlmenően a hírszerző közösség PPD-28-at végrehajtó tagjai megerősítették a nem értékelt jelfelderítési adatok lekérdezésére vonatkozó meglevő elemzési gyakorlatukat és normáikat ([3]). Az elemzőknek lekérdezéseiket, illetve az egyéb keresési feltételeket és technikákat úgy kell kialakítaniuk, hogy azok biztosítsák a jogszerű külföldi hírszerzési vagy bűnüldözési feladat tekintetében releváns hírszerzési információk azonosítását. Ebből a célból a hírszerző közösség tagjainak személyekre vonatkozó lekérdezéseiket a külföldi hírszerzési vagy bűnüldözési követelményeknek megfelelő jelfelderítési információkra kell összpontosítaniuk annak érdekében, hogy a személyes adatok külföldi hírszerzési vagy bűnüldözési követelményekhez nem tartozó felhasználása megelőzhető legyen.

Fontos hangsúlyozni, hogy az internetes kommunikációra vonatkozó minden olyan tömeges adatgyűjtési tevékenység, amelyet az USA hírszerző közössége jelfelderítésen keresztül végez, csak az internet kis részén történik. Ezen túlmenően a célzott lekérdezések fent ismertetett felhasználása biztosítja, hogy az elemzőkhöz csak azok az adatok kerüljenek vizsgálatra, amelyekről potenciális hírszerzési értéket feltételeznek. E korlátok célja minden ember magánéletének és alapvető szabadságjogainak védelme, állampolgárságtól és tartózkodási helytől függetlenül.

([1]) *Elérhető itt:* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Ezek az eljárások a célra irányultság és személyre szabás ebben a levélben tárgyalt fogalmát a hírszerző közösség minden egyes tagjára szabottan hajtják végre.

([2]) Csak hogy egy példát idézzünk, az NSA PPD-28-at végrehajtó eljárásrendje kimondja, hogy „[m]inden olyan esetben, ahol az a gyakorlatban ésszerűen megvalósítható, az adatgyűjtés egy vagy több kiválasztási feltétel alkalmazásával történik annak érdekében, hogy az adatgyűjtést konkrét külföldi hírszerzési célpontokra (pl. egy meghatározott, ismert nemzetközi terroristára vagy terrorista csoportra) vagy egy konkrét külföldi hírszerzési témakörre (*pl.* tömegpusztító fegyverek külföldi hatalom vagy megbízottai általi terjesztése) lehessen irányozni."

([3]) *Elérhető itt:* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Az Egyesült Államok eljárásokat dolgozott ki annak biztosítására, hogy jelfelderítési tevékenységeket csak megfelelő nemzetbiztonsági célok támogatására folytassanak. Minden évben az elnök jelöli ki – kiterjedt, hivatalos hivatalközi folyamatot követően – a külföldi hírszerzési adatgyűjtés kiemelt országos prioritásait. A DNI feladata ezeknek a hírszerzési prioritásoknak a nemzeti hírszerzési prioritási keretbe (NIPF) történő átültetése. A PPD-28 erősítette és továbbfejlesztette ezt a hivatalközi folyamatot annak biztosítására, hogy a hírszerző közösség valamennyi hírszerzési prioritását magas szintű politikai szereplők tekintsék át és hagyják jóvá. A hírszerző közösség 204. sz. irányelve (Intelligence Community Directive – ICD) további útmutatást nyújt a NIPF-ről és azt 2015 januárjában frissítették a PPD-28 követelményeinek beépítése céljából ([1]). Noha a NIPF titkos, az USA konkrét külföldi hírszerzési prioritásai évente megjelennek a DNI nem titkos globális fenyegetésértékelésében (*Worldwide Threat Assessment*), amely szabadon elérhető az ODNI weboldalán.

A nemzeti hírszerzési prioritási keret (National Intelligence Priorities Framework – NIPF) a prioritásokat meglehetősen általánosan fogalmazza meg. Ide tartoznak olyan kérdések, mint adott külföldi ellenfelek részéről nukleáris és ballisztikus rakétakapacitások kiépítése, a kábítószerkartell-korrupció hatásainak és meghatározott országokban az emberi jogi visszaéléseknek a figyelemmel kísérése. És ezek nem csak a jelfelderítésre, hanem valamennyi hírszerzési tevékenységre vonatkoznak. A NIPF prioritásainak tényleges jelfelderítési adatgyűjtésbe történő átültetéséért felelős szervezet a Nemzeti Jelfelderítési Bizottság (National Signals Intelligence Committee vagy SIGCOM). A bizottság a Nemzetbiztonsági Ügynökség (National Security Agency – NSA) igazgatójának égisze alatt működik, akit a 12333. sz. elnöki rendelet a „jelfelderítés funkcionális irányítójának" jelöl ki, aki a jelfelderítés felügyeletéért és a hírszerző közösség egészén belüli koordinálásáért felel, a védelmi miniszter és a DNI együttes felügyelete alatt. A SIGCOM-ban a hírszerző közösség valamennyi tagja képviselve van, és mivel az Egyesült Államok teljes körűen végrehajtja a PPD-28-at, teljes körű képviseletet kapnak a jelfelderítésben politikailag érdekelt más minisztériumok és hivatalok is.

Minden olyan egyesült államokbeli minisztérium és hivatal, amely a külföldi hírszerzést igénybe veszi, adatgyűjtési kérését a SIGCOM-hoz terjeszti be. A SIGCOM felülvizsgálja ezeket a kéréseket, biztosítja, hogy azok összhangban álljanak a NIPF-fel, és azokat prioritásokhoz rendeli a következő szempontok felhasználásával:

— Képesek a jelfelderítési adatok hasznos információkat nyújtani ebben az esetben vagy léteznek jobb vagy költséghatékonyabb információforrások – köztük például műholdképes vagy nyílt forrású információk – a követelmény teljesítésére?

— Mennyire lényeges az információ iránti igény? Ha a NIPF-ben előresorolt prioritás, a leggyakrabban kiemelt jelfelderítési prioritás lesz.

— Milyen típusú jelfelderítés használható?

— Az adatgyűjtés a lehető legcélzottabb? Szükség van időbeli, földrajzi vagy egyéb korlátozásokra?

Az USA jelfelderítési követelményekkel kapcsolatos eljárása más tényezők kifejezett mérlegelését is megköveteli, jelesül:

— Az adatgyűjtés célpontja vagy az adatgyűjtéshez használt módszer különösen kényes? Ha igen, azt magas rangú politikai szereplőknek is meg kell vizsgálnia.

— Az adatgyűjtés indokolatlan kockázatot fog jelenteni a magánélet és az alapvető szabadságjogok tekintetében, állampolgárságtól függetlenül?

— Szükségesek további terjesztési vagy megőrzési garanciák a magánélethez vagy nemzetbiztonsághoz fűződő érdekek megvédéséhez?

Végezetül – a folyamat végén – az NSA képzett személyzetéhez kerülnek a SIGCOM által validált prioritások, és felkutatják és megjelölik a konkrét kiválasztási feltételeket, így a telefonszámokat vagy e-mail címeket, amelyek várhatóan a prioritásoknak megfelelő külföldi hírszerzési adatgyűjtést eredményeznek. Az NSA adatgyűjtési rendszerébe való felvitel előtt minden kiválasztási feltételt felül kell vizsgálni és jóvá kell hagyni. Még ebben az esetben is az, hogy a tényleges adatgyűjtés megvalósul-e és mikor, részben olyan további megfontolásokon fog múlni, mint a megfelelő

([1]) *Elérhető itt* http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

adatgyűjtési források elérhetősége. Ez a folyamat biztosítja, hogy az USA jelfelderítési adatgyűjtésének célpontjai érvényes és fontos külföldi hírszerzési szükségleteket tükrözzenek. És természetesen a FISA szerinti adatgyűjtéskor az NSA-nak és más hivataloknak követniük kell a külföldi hírszerzést felügyelő bíróság által jóváhagyott korlátozásokat. Röviden: sem az NSA, sem pedig más egyesült államokbeli hírszerző ügynökség nem dönt saját maga arról, hogy milyen adatot gyűjtsön.

Összességében ez a folyamat biztosítja, hogy az USA valamennyi hírszerzési prioritását olyan magas szintű politikai szereplők határozzák meg, akik a legmegfelelőbb helyzetben vannak az USA külföldi hírszerzési követelményeinek meghatározásához, és hogy ezek a politikai szereplők ne csak a hírszerzési adatgyűjtés potenciális értékét vegyék figyelembe, hanem az adatgyűjtéshez társuló kockázatokat is, ideértve a magánélettel, nemzetgazdasági érdekekkel és külkapcsolatokkal kapcsolatos kockázatokat is.

Az adatvédelmi pajzs szerint az Egyesült Államokba továbbított adatok vonatkozásában – noha az Egyesült Államok nem tudja megerősíteni vagy tagadni konkrét hírszerzési módszerek vagy műveletek létét – a PPD-28 követelményei vonatkoznak az Egyesült Államok által végzett valamennyi jelfelderítési műveletre, a gyűjtött adatok típusától vagy forrásától függetlenül. Továbbá a jelfelderítési adatgyűjtésre vonatkozó korlátok és biztosítékok vonatkoznak a nem engedélyezett célú jelfelderítésre is, egyaránt ideértve a külkapcsolati és a nemzetbiztonsági célokat is.

A fent tárgyalt eljárások egyértelmű elkötelezettséget tükröznek az önkényes és megkülönböztetés nélküli jelfelderítési adatgyűjtés megelőzése, valamint kormányunk legmagasabb szintje részéről az ésszerűség elvének érvényesítése mellett. A PPD-28 és a hivatali végrehajtási eljárások pontosítják az Egyesült Államok jelfelderítési adatgyűjtésének és az ilyen adatok felhasználásának új és a meglevő korlátozásait, valamint konkretizálják annak céljait. Ezek bizonyosságot adnak arra vonatkozóan, hogy a jelfelderítési tevékenységek jelenleg és a jövőben is csak jogszerű külföldi hírszerzési célok előmozdítását szolgálják.

c. **Az adatok megőrzésére és terjesztésére vonatkozó korlátozások**

A PPD-28 4. szakasza előírja, hogy a hírszerző közösség minden tagjának kifejezett, az egyesült államokbeli személyekre vonatkozó korlátokkal összehasonlítható korlátozásokkal kell rendelkeznie a nem egyesült államokbeli személyekre vonatkozó, jelfelderítéssel gyűjtött személyes adatok megőrzése és terjesztése vonatkozásában. Ezek a szabályok beépítésre kerültek a hírszerző közösség minden egyes ügynökségének eljárásaiba, amelyeket 2015 februárjában adtak ki és nyilvánosan hozzáférhetőek. Ahhoz, hogy valamely személyes adat külföldi hírszerzési adatként megőrizhető és terjeszthető legyen, annak a fent ismertetett NIPF-folyamatban meghatározott, engedélyezett hírszerzési követelményhez kell kapcsolódnia; feltételezhetőnek kell lennie róla, hogy bűncselekmény bizonyítéka, vagy pedig meg kell felelnie a 12333. sz. elnöki rendelet 2.3. szakaszában meghatározott, az egyesült államokbeli személyekre vonatkozó adatmegőrzési normák egyikének.

Az olyan adatokat, amelyekre ez a vizsgálat nem történt meg, legfeljebb öt évig lehet megőrizni, kivéve, ha a DNI kifejezetten úgy dönt, hogy a további megőrzés az Egyesült Államok nemzetbiztonsági érdeke. Így a hírszerző közösség tagjainak az adatgyűjtést követően öt évvel törölniük kell a nem egyesült államokbeli személyekre vonatkozó, jelfelderítéssel gyűjtött adatokat, kivéve, ha például megállapítást nyer, hogy az információ valamely engedélyezett külföldi hírszerzési követelményhez releváns, vagy ha a DNI úgy dönt – az ODNI alapvető szabadságjogok védelmével foglalkozó hivatalnoka álláspontjának megfontolását követően –, hogy az adatok további megőrzése nemzetbiztonsági érdek.

Ezen túlmenően valamennyi hivatal PPD-28-at végrehajtó szabályzatai most kifejezetten előírják, hogy valamely személyre vonatkozó információk nem terjeszthetőek pusztán azon az alapon, hogy az illető nem egyesült államokbeli személy, és az ODNI irányelvet adott ki a hírszerző közösség valamennyi tagjának ([1]), amely tartalmazza ezt a követelményt. A hírszerző közösség személyzete számára a hírszerzési jelentések elkészítésekor és terjesztésekor konkrét előírás a nem egyesült államokbeli személyek magánélet védelméhez fűződő érdekeinek figyelembevétele. Nem minősülnek különösen terjeszthetőnek vagy tartósan megőrizhetőnek a külföldi személy rutinszerű tevékenységeire vonatkozó jelfelderítési adatok egyedül amiatt, mert külföldiről van szó, kivéve, ha ezek az adatok egyébként felhasználhatóak egy engedélyezett külföldi hírszerzési követelmény céljaira. Ez egy fontos korlátozás elismerése és válasz az Európai Bizottság külföldi hírszerzés 12333. sz. elnöki rendeletben szereplő fogalommeghatározásának tág hatókörével kapcsolatban megfogalmazott aggályaira.

([1]) A hírszerző közösségre vonatkozó irányelv (Intelligence Community Directive – ICD) 203, elérhető itt: http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Megfelelés és felügyelet**

A külföldi hírszerzés felügyeletének egyesült államokbeli rendszere szigorú és többrétű felügyeletet nyújt a vonatkozó jogszabályok és eljárások betartásának biztosítására, ideértve a nem egyesült államokbeli személyekre vonatkozó, jelfelderítéssel szerzett adatok PPD-28-ban meghatározott gyűjtésére, megőrzésére és terjesztésére vonatkozó jogszabályokat és eljárásokat. Ezek közé tartoznak a következők:

— A hírszerző közösség több száz felügyeleti tevékenységet ellátó személyt foglalkoztat. Egyedül az NSA-nál több mint 300 fő foglalkozik a megfeleléssel, és a többi tagnak is van megfelelési irodája. Emellett az Igazságügyi Minisztérium kiterjedt felügyeletet gyakorol a hírszerzési tevékenységek felett, valamint a Védelmi Minisztérium is lát el felügyeletet.

— A hírszerző közösség minden tagjánál saját főellenőri iroda működik, amelynek egyebek mellett a külföldi hírszerzési tevékenységek felügyelete is a feladatai közé tartozik. A főellenőrök függetlenségét jogszabály írja elő, tág vizsgálati, ellenőrzési és programfelügyeleti hatáskörük van, ideértve a csalást vagy a joggal való visszaélést,illetve jogsértéseket, és korrekciós intézkedéseket javasolhatnak. Noha a főellenőri ajánlások nem kötelezőek, a főellenőr jelentését gyakran nyilvánosságra hozzák és minden esetben beterjesztik a Kongresszusnak; ebbe beletartoznak az utójelentések is, ha a korábbi jelentésben ajánlott korrekciós intézkedéseket még nem hajtották végre. A Kongresszus ezért értesül minden meg nem felelési esetről és nyomást gyakorolhat a korrekciós intézkedés megvalósítása érdekében, a költségvetési eszközökön keresztül történő nyomásgyakorlást is ideértve. A hírszerzési programokról szóló számos főellenőri jelentés nyilvánosan is közzé lett téve ([1]).

— Az ODNI polgári szabadságjogi és adatvédelmi hivatalának (Civil Liberties and Privacy Office – CLPO) feladata annak biztosítása, hogy a hírszerző közösség működésének módja az alapvető szabadságjogok és a magánélethez fűződő jogok védelme mellett mozdítsa elő a nemzetbiztonságot ([2]). A hírszerző közösség más tagjainak saját adatvédelmi tisztviselőjük van.

— Az adatvédelmi és polgári szabadságjogi felügyelő tanács (Privacy and Civil Liberties Oversight Board – PCLOB), egy törvénnyel létrehozott független szerv feladata a terrorizmus elleni programok és szakpolitikák elemzése és áttekintése a jelfelderítés alkalmazására kiterjedően, azt biztosítandó, hogy azok megfelelően óvják a magánéletet és az alapvető szabadságjogokat. A tanács több nyilvános jelentést adott ki a hírszerzési tevékenységekről.

— Amint az a későbbiekben részletesebben kifejtésre kerül, a független szövetségi bírákból álló, külföldi hírszerzést felügyelő bíróság feladata a FISA szerint folytatott jelfelderítési adatgyűjtési tevékenységek felügyelete és megfelelésének biztosítása.

— Végezetül az USA Kongresszusa, konkrétan a Képviselőház és a Szenátus hírszerzési és igazságügyi bizottsága rendelkezik jelentős felügyeleti feladatkörökkel az USA valamennyi külföldi hírszerzés tevékenysége tekintetében, az USA jelfelderítési tevékenységét is ideértve.

E hivatalos felügyeleti mechanizmusok mellett a hírszerző közösség is számos mechanizmust rendszeresített annak biztosítására, hogy a hírszerző közösség megfeleljen az adatgyűjtés fent ismertetett korlátozásainak. Például:

— A kabinet tisztviselőinek minden évben ellenőrizniük kell jelfelderítési követelményeiket.

— Az NSA a teljes adatgyűjtési folyamat alatt ellenőrzi a jelfelderítési célpontokat annak megállapítására, hogy azok ténylegesen a prioritásoknak megfelelő értékes külföldi hírszerzési információkat adnak-e, és amennyiben nem, leállítja az adott célpontokra vonatkozó adatgyűjtést. További eljárások biztosítják a kiválasztási feltételek időszakos felülvizsgálatát.

([1]) *Lásd pl.* az USA Igazságügyi Minisztériuma főellenőrének jelentését: „A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008"(A Szövetségi Nyomozóiroda tevékenységeinek a külföldi hírszerzői tevékenység megfigyeléséről szóló 2008. évi törvény 702. szakasza szerinti felülvizsgálata) (2012. szeptember), *elérhető itt:* https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) *Lásd:* www.dni.gov/clpo.

— Az Obama elnök által kinevezett független felülvizsgáló csoport ajánlására a DNI új mechanizmust hozott létre a célpont jellegére vagy az adatgyűjtés módjára figyelemmel különösen kényes jelfelderítési adatok gyűjtése és terjesztése nyomon követésére azt biztosítandó, hogy az összhangban álljon a politikai szereplők szándékaival.

— Végezetül az ODNI évente felülvizsgálja a hírszerző közösség erőforrásainak elosztását a NIPF prioritásaihoz és a hírszerzés egészének küldetéséhez képest. Ez a felülvizsgálat kiterjed a hírszerzési adatgyűjtés valamennyi fajtája, így a jelfelderítési adatgyűjtés értékére, mind visszamenőlegesen – mennyire volt sikeres a hírszerző közösség céljai elérésében? –, mind pedig a jövőre nézve – melyek lesznek a hírszerző közösség jövőbeli szükségletei? Ez biztosítja, hogy a jelfelderítési erőforrásokat a legfontosabb nemzeti prioritásokra fordítsák.

Amint ez az átfogó áttekintés is bizonyítja, a hírszerző közösség nem saját maga dönti el, hogy mely beszélgetéseket hallgassa le, nem próbál meg minden adatot begyűjteni, illetve nem ellenőrizetlenül működik. Tevékenységei politikai szereplők által kitűzött prioritások köré csoportosulnak egy olyan folyamat révén, amelynek részét képezik a kormányzat minden részéről érkező hozzászólások, és amelyet az NSA-n belül, illetőleg az ODNI, az Igazságügyi Minisztérium és a Védelmi Minisztérium részéről is felügyelnek.

A PPD-28-nak része több más, annak biztosítását szolgáló intézkedés is, hogy a jelfelderítéssel gyűjtött személyes adatok állampolgárságra tekintet nélkül védelemben részesüljenek. A PPD-28 rendelkezik például adatbiztonsági, adatbetekintési és adatminőségi eljárásokról a jelfelderítéssel gyűjtött személyes adatok védelmére, és kötelező képzést ír elő azt biztosítandó, hogy a munkaerő megértse a személyes adatok állampolgárságtól független védelmének felelősségét. A PPD további felügyeleti és megfelelési mechanizmusokról is rendelkezik. Ide tartoznak az illetékes felügyelő és megfelelési tisztviselők részéről a jelfelderítéssel érintett személyes adatok védelmi gyakorlata tekintetében lefolytatott időszaki ellenőrzések és felülvizsgálatok. A felülvizsgálatnak le kell fednie az ilyen információk védelmére szolgáló eljárások hivatal általi betartásának vizsgálatát is.

Emellett a PPD-28 rendelkezik arról, hogy a nem egyesült államokbeli személyekhez kapcsolódó jelentős megfelelési problémákat felsőbb kormányzati szinten fogják rendezni. Amennyiben a jelfelderítéssel bármely személyről gyűjtött személyes adatokat érintő jelentős megfelelési probléma merül fel, a problémát – a meglevő beszámolási követelményeken túl – a DNI-nek is haladéktalanul jelenteni kell. Ha a probléma nem egyesült államokbeli személy személyes adataival kapcsolatos, a DNI a külügyminiszterrel és a hírszerző közösség érintett tagjának vezetőjével egyeztetve határozza meg, hogy lépéseket kell-e tenni az érintett külföldi kormány értesítésére, a források, módszerek és az egyesült államokbeli személyzet védelmével összeegyeztethető módon. Emellett – a PPD-28-ban előírtaknak megfelelően – a külügyminiszter kijelölt egy magas rangú tisztviselőt, Catherine Novelli miniszter-helyettest, azon külföldi kormányokkal való kapcsolattartásra, amelyek az Egyesült Államok jelfelderítési tevékenységeivel kapcsolatban aggályaiknak kívánnak hangot adni. A magas szintű részvétel melletti elkötelezettség példázza az USA kormánya által az elmúlt évtizedekben annak érdekében tett erőfeszítéseket, hogy megerősítse az egyesült államokbeli személyek és nem egyesült államokbeli személyek adatai tekintetében a magánélet védelmére rendszeresített számos és egymást átfedő védekezési intézkedésbe vetett bizalmat.

e. **Összefoglalás**

Az Egyesült Államok külföldi hírszerzési adatok gyűjtésére, megőrzésére és terjesztésére vonatkozó folyamatai jelentős magánélet-védelmi eszközöket nyújtanak minden ember személyes adatai vonatkozásában, állampolgárságra tekintet nélkül. Ezek a folyamatok biztosítják különösen, hogy hírszerző közösségünk nemzetbiztonsági küldetésére összpontosítson, az irányadó törvények, elnöki rendeletek és elnöki irányelvek falhatalmazásának megfelelően; védje az adatokat az illetéktelen hozzáféréstől, felhasználástól és feltárástól, és tevékenységeit többrétű ellenőrzés és felügyelet mellett folytassa, beleértve a kongresszusi bizottságok általi felügyeletet. A PPD-28 és az azt végrehajtó eljárások képviselik arra irányuló erőfeszítéseinket, hogy kiterjesszünk bizonyos minimalizálási és más alapvető adatvédelmi elveket állampolgárságra tekintet nélkül valamennyi személy személyes adataira. Az USA részéről történő jelfelderítési adatgyűjtésre az USA jogának és elnöki útmutatásainak elvei és követelményei vonatkoznak, beleértve a PPD-28-ban meghatározott védelmi eszközöket. Ezek az elvek és követelmények biztosítják, hogy valamennyi személyt állampolgárságára és lakóhelyére tekintet nélkül méltósággal és tisztelettel kezeljenek, és elismerjék, hogy mindenkinek jogos adatvédelmi érdeke fűződik személyes adatainak kezeléséhez.

II. A KÜLFÖLDI HÍRSZERZŐI TEVÉKENYSÉG MEGFIGYELÉSÉRŐL SZÓLÓ TÖRVÉNY – 702. SZAKASZ

A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény ([1]) 702. szakasza szerinti adatgyűjtés nem „tömeges és megkülönböztetés nélküli", hanem szűk körben a jogszerű célpontként azonosított magánszemélyekre vonatkozó külföldi hírszerzési adatok gyűjtésére irányul, valamint független bírói ellenőrzés és a végrehajtó hatalom és a Kongresszus részéről egyaránt jelentős ellenőrzés és felügyelet alatt áll. A 702. szakasz szerinti adatgyűjtés a PPD-28 követelményeinek hatálya alá tartozó jelfelderítésnek minősül ([2]).

A 702. szakasz szerinti adatgyűjtés a legértékesebb hírszerzési források egyike, amely egyszerre védi az Egyesült Államok és európai partnereink érdekeit is. Nyilvánosan elérhető a 702. szakasz működésére és felügyeletére vonatkozó részletes tájékoztatás. A programhoz kapcsolódó számos bírósági beadvány, bírósági határozat és felügyeleti jelentés titkosítását feloldották, és azokat az ODNI nyilvános közzétételi webhelyén közzétették: www.icontherecord.tumblr.com. Emellett a PCLOB átfogó elemzést végzett a 702. szakasz vonatkozásában, amelyről a jelentés elérhető itt: https://www.pclob.gov/library/702-Report.pdf. ([3])

A 702. szakasz a FISA 2008. évi módosításakor került elfogadásra ([4]), hosszadalmas kongresszusi vitát követően. Felhatalmazást ad külföldi hírszerzési információk Egyesült Államokon kívül tartózkodó nem egyesült államokbeli célszemélyeken keresztül történő beszerzésére, az USA elektronikus kommunikációs szolgáltatóinak kötelező támogatásával. A 702. szakasz felhatalmazza a legfőbb ügyészt és a DNI-t – mindkettő az elnök által kinevezett és a Szenátus által megerősített kabinet tisztviselő – éves tanúsítványoknak a FISA-bírósághoz történő benyújtására ([5]). Ezek a tanúsítványok adják meg a gyűjtendő külföldi hírszerzési adatok konkrét kategóriáit, ilyenek a terrorizmus vagy tömegpusztító fegyverek elleni küzdelemmel kapcsolatos hírszerzési adatok, amelyeknek a FISA-törvényben meghatározott külföldi hírszerzési kategóriákba kell tartozniuk ([6]). Ahogy a PCLOB megjegyezte, „[e]zek a korlátozások *nem* engedélyezik a külföldiekre vonatkozó információk korlátlan gyűjtését." ([7])

A tanúsítványok szükségesek a FISA-bíróság által kötelezően áttekintendő és jóváhagyandó „célzási" és „minimalizálási" eljárások felvételéhez is ([8]). A célzási eljárások annak biztosítására szolgálnak, hogy az adatgyűjtési eljárásokra csak a törvényi felhatalmazásnak megfelelően és a tanúsítványok hatókörén belül kerüljön sor, a minimalizálási eljárások célja pedig az egyesült államokbeli személyekre vonatkozó információk megszerzésének, terjesztésének és megőrzésének korlátozása, de tartalmaznak olyan rendelkezéseket is, amelyek érdemi védelmet nyújtanak a nem egyesült államokbeli személyekre vonatkozó információknak, az alább ismertetettek szerint. Emellett, ahogy fent tárgyaltuk, az elnök a PPD-28-ban azt az utasítást adta, hogy a hírszerző közösségnek további védelmi eszközöket kell biztosítania a nem egyesült államokbeli személyekre vonatkozó személyes adatok tekintetében, és ezek érvényesülnek a 702. szakasz szerint gyűjtött információk esetében is.

Amint a bíróság jóváhagyja a célzási és minimalizálási eljárást, a 702. szakasz szerinti adatgyűjtés nem tömeges vagy megkülönböztetés nélküli, hanem „teljes egészében azokra a konkrét személyekre irányuló, akikre vonatkozóan egyedi döntés született" – magyarázza a PCLOB ([9]). Az adatgyűjtés célzása egyedi kiválasztási feltételek alkalmazásával történik, így olyan e-mail-címekkel vagy telefonszámokkal, amelyekről az USA hírszerzési személyzete megállapította, hogy

([1]) 50 U. S. C. § 1881a.

([2]) Az Egyesült Államok a FISA egyéb rendelkezései alapján is kérhet bírói végzést adatok szolgáltatására, az adatvédelmi pajzson keresztül továbbított adatokra is kiterjedően. *Lásd:* 50 U.S.C. § 1801 és további rendelkezések. TA FISA elektronikus megfigyelést engedélyező I. és fizikai kutatást engedélyező III. címe is előírja a bírósági végzést (rendkívüli körülmények kivételével), és minden esetben követelmény annak alapos gyanúja, hogy a célpont egy külföldi hatalom vagy külföldi hatalom megbízottja. A FISA IV. címe engedélyezi a hívásrögzítő és a lehallgató eszközök bírói végzéshez kötött használatát (rendkívüli körülmények kivételével) engedélyezett külföldi hírszerzési, kémelhárítási vagy terrorizmus elleni nyomozásokban. A FISA V. címe megengedi az FBI-nak, hogy (rendkívüli körülmények kivételével) bírói végzéssel beszerezze azokat az üzleti nyilvántartásokat, amelyek egy engedélyezett külföldi hírszerzési, kémelhárítási vagy terrorizmus elleni nyomozásban jelentőséggel bírnak. Az alább tárgyaltaknak megfelelően az USA szabadságjogokról szóló törvénye (FREEDOM Act) kifejezetten megtiltja a FISA szerinti hívásrögzítésre vagy üzleti nyilvántartások kiadására vonatkozó, tömeges adatgyűjtésre szóló végzéseket, és előírja a „konkrét kiválasztási feltétel" követelményét annak biztosítására, hogy ezeket a hatósági eszközöket célzott módon használják.

([3]) 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) (2014. július 2.) („a PCLOB jelentése").

([4]) *Lásd:* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) Lásd: 50 U. S. C. § 1881a(f).

([6]) Lásd: u.o. § 1801(e)

([7]) Lásd a PCLOB jelentésének a 99. oldalát.

([8]) Lásd: 50 U. S. C. § 1881a(f).

([9]) Lásd a PCLOB jelentésének 111. oldalát

valószínűleg a bírósághoz benyújtott tanúsítvány hatókörébe tartozó külföldi hírszerzési információk közlésére használják ([1]). A cél kiválasztásának alapját dokumentálni kell, és minden egyes kiválasztási szempont dokumentációját később az Igazságügyi Minisztérium ellenőrzi ([2]). Az USA kormánya nyilvánosságra hozott olyan információkat, amelyek tanúsága szerint 2014-ben mintegy 90 000 magánszemély volt a 702. szakasz alapján célszemély, ami elenyésző töredéke az internetezők világszerte 3 milliárdot meghaladó táborának ([3]).

A 702. szakasz alapján gyűjtött információkra a bíróság által jóváhagyott minimalizálási eljárások vonatkoznak, amelyek védelmet nyújtanak a nem egyesült államokbeli személyek, illetve az egyesült államokbeli személyek számára is, és ezeket az eljárásokat nyilvánosságra hozták ([4]). Például a 702. szakasz szerint megszerzett közléseket szigorú hozzáférési korlátozásokkal védett adatbázisokban tárolják, tekintet nélkül arra, hogy egyesült államokbeli személyektől vagy nem egyesült államokbeli személyektől származnak. Ezeket csak a magánélet védelmét szolgáló minimalizálási eljárásokban képzett, és engedélyezett feladatainak elvégzése érdekében az adott betekintésre jóváhagyott hírszerzési személyzet tekintheti meg ([5]). Az adatok felhasználása külföldi hírszerzési információk vagy bűncselekmény bizonyítékának azonosítására korlátozódik ([6]). A PPD-28 szerint ezt az információkat csak akkor lehet terjeszteni, ha arra érvényes külföldi hírszerzési vagy bűnüldözési indok áll fenn; nem elegendő az a puszta tény, hogy a kommunikáció egyik résztvevője nem egyesült államokbeli személy ([7]). A minimalizálási eljárások és a PPD-28 továbbá korlátot szabnak meg arra vonatkozóan is, hogy milyen hosszú ideig lehet a 702. szakasz szerint szerzett adatokat megőrizni ([8]).

A 702. szakasz felügyelete kiterjedt, és azt a kormányzat mindhárom hatalmi ága végzi. A törvényt végrehajtó hivatalokban többszintű belső ellenőrzés működik, ideértve a független főellenőr általi ellenőrzést, valamint az adatbetekintés technológiai korlátozásait is. Az Igazságügyi Minisztérium és az ODNI szigorúan figyelemmel kíséri és ellenőrzi a 702. szakasz alkalmazását a jogszabályi előírásoknak való megfelelés ellenőrzésére; a hivatalokat is független kötelezettség terheli az esetleges nem megfelelési esetek jelentésére. Ezeket az eseteket kivizsgálják és valamennyi megfelelési esetet jelentenek a külföldi hírszerzést felügyelő bíróságnak, az elnök hírszerzést felügyelő tanácsának és a Kongresszusnak, és megfelelően orvosolják ([9]). Eddig nem történt olyan eset, amely a jogszabályi követelmények megsértésére irányuló szándékos kísérletet jelezne ([10]).

A FISA-bíróság fontos szerepet tölt be a 702. szakasz végrehajtásában. A bíróság független szövetségi bírákból áll, akiknek a FISA-bíróságnál hét év a megbízatásuk, de a szövetségi bírákéhoz hasonlóan bírói megbízatásuk élethosszig szól. Amint fent említettük, a bíróságnak felül kell vizsgálnia az éves tanúsítványokat és célzási, illetve minimalizálási eljárásokat a jogszabályoknak való megfelelés szempontjából. Emellett, amint arról fentebb ugyancsak említést tettünk, a kormánynak haladéktalanul értesítenie kell a bíróságot a megfelelési esetekről ([11]), és több olyan bírósági vélemény titkosítását is feloldották, illetve nyilvánosságra hoztak olyan véleményeket, amelyek a bírói ellenőrzés kiemelkedően magas fokát és az ilyen esetek felülvizsgálatában gyakorolt bírói függetlenséget szemléltetik.

A bíróság szigorú eljárásait a korábbi elnöklő bíró ismerteti a Kongresszusnak szóló, nyilvánosságra hozott levelében ([12]). Továbbá az USA szabadságjogokról szóló törvénye eredményeként a bíróság kifejezett felhatalmazást kapott egy külső ügyvéd kijelölésére abból a célból, hogy független adatvédelmi védőügyvédként járjon el az új és jelentős jogkérdéseket felvonultató ügyekben ([13]). Szokatlan, de talán példátlan is egy ország független bíróságának ilyen fokú részvétele az olyan külföldi hírszerzés tevékenységekben, amelyek nem az ország állampolgáraira, illetve az országban tartózkodó személyekre irányulnak, és segít annak biztosításában, hogy a 702. szakasz szerinti adatgyűjtésre a megfelelő jogi keretek között kerüljön sor.

([1]) *u.o.*

([2]) u.o. a 8. oldalon; 50 U.S.C. § 1881a(l); *lásd még: az* NSA alapvető szabadságjogok és magánélet védelméért felelős igazgatójának jelentését: „NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (A külföldi hírszerzői tevékenység megfigyeléséről szóló törvény 702. szakaszának NSA általi végrehajtása (a továbbiakban: „az NSA-jelentés"), a 4. oldalon, elérhető itt: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) A nemzeti hírszerzési igazgató 2014. évi átláthatósági jelentése, elérhető itt: http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) A minimalizálási eljárások elérhetők itt: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) *Lásd:* az NSA-jelentés 4. oldalát

([6]) *Lásd még: az* NSA minimalizálási eljárásainak 6. oldalát.

([7]) A hírszerző ügynökségekre PPD-28 szerinti eljárások elérhetőek itt: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Lásd: az NSA minimalizálási eljárásai; PPD-28, 4. szakasz.

([9]) Lásd: 50 U.S.C. § 1881(l); *lásd még:* a PCLOB jelentésének 66-76. oldalát.

([10]) *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 értékelésének 2–3. oldalát, elérhető itt: http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) A külföldi hírszerzést felügyelő bíróság eljárási szabályzatának 13. pontja, *elérhető itt:* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) Reggi B. Walton bíró 2013. július 29-i levele Patrick J. Leahy bíróhoz, *elérhető itt:* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Lásd az USA szabadságjogokról szóló törvényének 401. szakaszát, P.L. 114-23.

A Kongresszus a hírszerzési és igazságügyi bizottság részére törvényben előírt jelentéseken, valamint gyakori eligazításokon és meghallgatásokon keresztül gyakorol felügyeletet. Ezek közé tartozik a legfőbb ügyész 702. szakasz alkalmazását és a megfelelési eseteket dokumentáló féléves jelentése ([1]); a legfőbb ügyész és a DNI külön féléves jelentése a célzási és minimalizálási eljárások betartásáról, beleértve az annak biztosítását szolgáló eljárásokat, hogy az adatgyűjtés érvényes külföldi hírszerzési célra történjen ([2]), valamint a hírszerzés tagjainak éves jelentése, amelynek része annak tanúsítása, hogy a 702. szakasz szerinti adatgyűjtés továbbra is külföldi hírszerzési információkat ad ([3]).

Röviden, a 702. szakasz szerinti adatgyűjtésre törvényi felhatalmazás van; az adatgyűjtés többszintű ellenőrzés, bírói felügyelet és felügyelet alatt áll, valamint – ahogy a FISA-bíróság kimondta egy olyan véleményben, amelynek titkosítását a közelmúltban oldották fel – azt „nem tömegesen vagy megkülönböztetés nélkül végzik," hanem „… az egyes (kommunikációs) létesítmények diszkrét célzási döntései alapján." ([4])

III. AZ EGYESÜLT ÁLLAMOK SZABADSÁGJOGOKRÓL SZÓLÓ (USA FREEDOM) TÖRVÉNYE

Az USA 2015 júniusában törvénybe iktatott szabadságjogokról szóló törvénye (USA FREEDOM törvény) jelentősen módosította az USA megfigyelési és más nemzetbiztonsági hatásköreit, és növelte e hatáskörök és a FISA-bíróság határozatainak nyilvános átláthatóságát, az alább ismertetettek szerint ([5]). A törvény biztosítja, hogy hírszerzési és bűnüldözési szakembereink rendelkezzenek azokkal a hatáskörökkel, amelyek a nemzet védelméhez szükségesek, egyidejűleg biztosítva az egyének magánéletének megfelelő védelmét e hatáskörök alkalmazása során. Ez fokozza a magánélet és az alapvető szabadságjogok védelmét és növeli az átláthatóságot.

A törvény megtiltja bármely adatnak a FISA különböző rendelkezései szerinti vagy nemzetbiztonsági levelek (a törvényi felhatalmazáson alapuló közigazgatási idézés egy formája) felhasználásával történő tömeges gyűjtését, az USA-beli személyekre és a nem egyesült államokbeli személyekre vonatkozó adatokra egyaránt kiterjedő hatállyal ([6]). Ez a tilalom konkrétan megnevezi a az USA-n belül és azon kívül tartózkodó személyek közötti hívásokhoz kapcsolódó telefonmetaadatok gyűjtését, és az említett hatáskörök alapján az adatvédelmi pajzs szerinti információk gyűjtésére is kiterjedne. A törvény előírja, hogy a kormánynak az említett hatáskörök szerinti adatigénylést „konkrét kiválasztási feltételre" kell alapoznia, olyan feltételre, amely konkrétan azonosít egy személyt, felhasználói fiókot, lakcímet vagy személyes eszközt, olyan módon, amely a gyakorlatban ésszerű lehető legnagyobb mértékben bekorlátozza a kért információk körét ([7]). Ez még inkább biztosítja, hogy a hírszerzési célokra történő adatgyűjtés pontosan fókuszált és célzott legyen.

A törvény jelentős módosításokat eszközölt továbbá a FISA-bíróság előtt folyó eljárásokban, amelyek egyszerre növelik az átláthatóságot és további biztosítékot adnak arra, hogy a magánélet védelemben fog részesülni. Amint fentebb említettük, a törvény engedélyezte egy biztonsági átvilágításon átesett, adatvédelmi és alapvető szabadságjogi, hírszerzési adatgyűjtési, kommunikációtechnológiai vagy más idevágó területen gyakorlattal rendelkező ügyvédekből álló állandó testület létrehozását, akiket *amicus curiae* (tanácsadó) szerepkörben ki lehet jelölni a jelentős vagy új jogkérdéseket felvonultató ügyekben. Ezek az ügyvédek jogi érvelést terjeszthetnek be az egyének magánéletének és alapvető szabadságjogainak előmozdítására, valamint hozzáférnek minden olyan információhoz, amely a bíróság szerint feladatuk ellátásához szükséges, a titkos információkat is ideértve ([8]).

A törvény az USA kormányának a hírszerzési tevékenységekkel kapcsolatos példátlan átláthatóságára hagyatkozik azzal, hogy a DNI a legfőbb ügyésszel egyeztetve kérheti a FISA-bíróság vagy a külföldi hírszerzést felügyelő fellebbviteli bíróság által kiadott minden egyes olyan döntés, végzés vagy vélemény titkosításának feloldását vagy azok nem bizalmas összefoglalóját, amely valamely jogszabályi rendelkezés jelentős értelmezését tartalmazza.

([1]) Lásd 50 U.S.C. § 1881f.
([2]) Lásd 15 U. S. C. 1881a(f)(1).
([3]) Lásd 15 U. S. C. 1881a(f)(3). E jelentések némelyike titkosítva van.
([4]) Mem. vélemény és végzés 26. oldala (FISC 2014), *elérhető itt:* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) USA FREEDOM Act, 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.
([6]) Lásd u.o. §§ 103, 201 és 501. A nemzetbiztonsági leveleket többféle törvény is engedélyezi és lehetővé teszik az FBI számára, hogy információkat kapjon bizonyos típusú vállalatok hiteljelentéseiből, pénzügyi nyilvántartásaiból és elektronikus előfizetői és tranzakciós adataiból, kizárólag a nemzetközi terrorizmus vagy a titkos hírszerzési tevékenység elleni védekezés céljára. *Lásd:* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. Az FBI a nemzetbiztonsági leveleket rendszerint kritikus, tartalmat nem képező információknak a terrorizmus ellenes és kémelhárítási nyomozások korai szakaszában való gyűjtésére használja – ilyen például valamely olyan felhasználói fiók előfizetőjének személyazonossága, aki esetleg kommunikációt folytatott valamely terrorista csoporttal, pl. az ISIL-lel. A nemzetbiztonsági levelek címzettjei azokat bíróság előtt megtámadhatják. Lásd 18 U. S. C. § 3511.
([7]) *Lásd u.o.*
([8]) Lásd u.o. § 401

Emellett a törvény kiterjedt közzétételt ír elő a FISA szerinti adatgyűjtésről és a nemzetbiztonsági levelek iránti kérésekre. Az Egyesült Államoknak minden évben tájékoztatnia kell a Kongresszust és a lakosságot a kért és kiadott FISA-végzések és tanúsítványok számáról; a megfigyelt egyesült államokbeli célszemélyek és a nem egyesült államokbeli célszemélyek becsült számáról; és egyéb adatok mellett az *amici curiae* kinevezések számáról ([1]). A törvény a kormány számára további nyilvános beszámolást is előír az egyesült államokbeli személyek és nem egyesült államokbeli személyekre vonatkozó nemzetbiztonsági levelek számáról ([2]).

A vállalati átláthatóságot illetően a törvény többféle lehetőséget biztosít a vállalatoknak a kormánytól kapott FISA-végzések és irányelvek, illetve nemzetbiztonsági levelek összesített számáról történő nyilvános beszámolásra, illetve azon felhasználói fiókok számáról, amelyekre az említett végzések irányultak ([3]). Több vállalat már közzétett ilyen adatokat, és az adatközlésekből látható, milyen korlátozott volt azon ügyfelek száma, akiknek az adatait átvizsgálták.

Ezek a vállalati átláthatósági jelentések szemléltetik, hogy az USA hírszerzési kérései csak az adatok elenyésző töredékét érintik. Például egy vezető vállalat közelmúltbeli átláthatósági jelentése azt mutatja, hogy kevesebb mint 20 000 felhasználói fiókjára vonatkozóan kapott nemzetbiztonsági kérést (a FISA szerint vagy nemzetbiztonsági levelet), miközben legalább 400 millió előfizetője volt. Más megfogalmazásban, a vállalat beszámolója szerint az USA nemzetbiztonsági kérései előfizetőinek kevesebb mint 5 ezrelékét érintették. Még ha mindegyik ilyen kérés védett adatkikötő adatra vonatkozott is volna (persze ez nem így volt), nyilvánvaló, hogy a kérések célzottak és megfelelő léptékűek, és nem tekinthetőek sem tömegesnek, sem pedig megkülönböztetés nélkülinek.

Végezetül, noha a nemzetbiztonsági leveleket engedélyező törvény már korlátozza azokat a körülményeket, amelyek mellett a levél címzettjének megtiltható annak közlése, a törvény előírja azt is, hogy a közlés megtagadásának követelményét időszakonként felül kell vizsgálni; előírja továbbá, hogy a nemzetbiztonsági levelek címzettjeit értesíteni kell arról, hogy nem állnak fenn a közlés megtagadásának követelményét alátámasztó tények; továbbá eljárásokat iktat törvénybe a címzettek számára a közlés megtagadása követelményének vitatására ([4]).

Összegezve, az USA szabadságjogokról szóló törvényének az USA hírszerzési hatásköreit érintő jelentős módosításai egyértelmű bizonyítékot jelentenek az Egyesült Államok azon nagyszabású erőfeszítéseire, hogy a személyes adatok, a magánélet és az alapvető szabadságjogok védelmét, valamint az átláthatóságot az USA valamennyi hírszerzési gyakorlatának homlokterébe helyezze.

IV. ÁTLÁTHATÓSÁG

Az USA szabadságjogokról szóló törvénye által előírt átláthatóság mellett az USA hírszerző közössége számos további információt nyújt a lakosságnak, jó példát mutatva hírszerzési tevékenységei átláthatóságát illetően. A hírszerző közösség nyilvánosságra hozta számos szabályzatát, eljárásrendjét, a külföldi hírszerzést felügyelő bíróság döntéseit, és más olyan anyagokat, amelyek titkosítását feloldották, ezzel megteremtve az átláthatóság rendkívüli mértékét. Ezen túlmenően a hírszerző közösség lényegesen bővítette a nemzetbiztonsági adatgyűjtési hatáskörök kormányzati felhasználási statisztikáinak közzétételét. A hírszerző közösség 2015. április 22-én adta ki második éves jelentését, amely statisztikákat mutat be arról, hogy a kormány milyen gyakran él ezekkel a fontos hatáskörökkel. Az ODNI is közzétette – az ODNI webhelyén és az *IC On the Record* alkalmazásban konkrét átláthatósági elveinek csomagját ([5]) és egy végrehajtási tervet is, amely az elveket gyakorlati, mérhető kezdeményezésekbe ülteti át ([6]). A nemzeti hírszerzési igazgató 2015 októberében utasítást adott ki, hogy minden egyes hírszerző ügynökség jelöljön ki hírszerzési átláthatósági tisztviselőt a vezetésén belül, az átláthatóság előmozdítására és az átláthatósági kezdeményezések vezetésére ([7]). Az átláthatósági tisztviselő szorosan együtt fog működni minden egyes hírszerző ügynökség adatvédelmi és polgári szabadságjogi tisztségviselőjével annak biztosítására, hogy az átláthatóság, a magánélet és az alapvető szabadságjogok védelme továbbra is kiemelt prioritás maradjon.

([1]) Lásd u.o. § 602.
([2]) *Lásd u.o.*
([3]) Lásd u.o. § 603.
([4]) Lásd u.o. §§ 502(f)-503.
([5]) *Elérhető itt:* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) *Elérhető itt:* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) *Lásd u.o.*

Ezeket az erőfeszítéseket példázza, hogy az NSA vezető adatvédelmi és polgári szabadságjogi tisztségviselője az elmúlt pár évben több olyan jelentést nyilvánosságra hozott, amelynek titkosítását feloldották, köztük a 702. szakasz, a 12333. sz. elnöki rendelet és az USA szabadságjogokról szóló törvénye szerinti tevékenységekre vonatkozó jelentést ([1]). Emellett a hírszerző közösség munkájában szorosan együttműködik a PCLOB-val, a Kongresszussal és az USA adatvédelmi tanácsadói közösségével annak érdekében, hogy további átláthatóságot vigyen az USA hírszerzési tevékenységeibe, amennyiben az megvalósítható és összeegyeztethető a kényes hírszerzési források és módszerek védelmével. Egészében véve az USA hírszerzési tevékenységei legalább annyira vagy még inkább átláthatóak, mint a világ bármely más nemzetéé, és a kényes hírszerzési források és módszerek védelme szükségességével összeegyeztethető lehető legátláthatóbbak.

Az USA hírszerzési tevékenységeivel fennálló átláthatóság magas fokát összegzendő:

— A hírszerző közösség több ezer oldalnyi, hírszerzési tevékenységeink konkrét eljárásait és követelményeit bemutató bírósági vélemény és ügynökségi eljárás titkosítását oldotta fel és tette az interneten elérhetővé. Jelentéseket adtunk ki továbbá az irányadó korlátozások hírszerző ügynökségek általi betartásáról is.

— A magas rangú hírszerző tisztviselők rendszeresen nyilatkoznak szervezetük szerepköréről és tevékenységeiről, a munkájukra vonatkozó megfelelési rendszerekre és biztosítékokra kiterjedően.

— A hírszerző közösség számos további dokumentumot adott ki az információhoz való szabad hozzáférésről szóló törvény szerinti hírszerzési tevékenységekről.

— Az elnök kiadta a PPD-28-at, további nyilvános korlátokat szabva hírszerzési tevékenységeinknek, és az ODNI két nyilvános jelentést is kiadott e korlátozások végrehajtásáról.

— A hírszerző közösséget most törvény kötelezi a FISA-bíróság által kiadott jelentős jogi vélemények vagy e vélemények összefoglalója titkosításának feloldására.

— A kormánynak évente be kell számolnia arról, hogy milyen mértékben használ bizonyos nemzetbiztonsági hatásköröket és erre a vállalatok is felhatalmazást kaptak.

— A PCLOB több részletes nyilvános jelentést adott ki a hírszerzési tevékenységekről, és ezt a jövőben is folytatni fogja.

— A hírszerző közösség nagy mennyiségű titkos információt bocsát a Kongresszus felügyeleti bizottságai rendelkezésére.

— A DNI átláthatósági elveket adott ki a hírszerző közösség tevékenységei vonatkozásában.

Ez a kiterjedt átláthatóság még tovább fog erősödni. Természetesen valamennyi nyilvánosságra hozott információ elérhető lesz a Kereskedelmi Minisztérium és az Európai Bizottság számára egyaránt. A Kereskedelmi Minisztérium és az Európai Bizottság közötti, az adatvédelmi pajzs végrehajtásáról folytatott éves felülvizsgálat lehetőséget nyújt majd az Európai Bizottságnak az újonnan nyilvánosságra hozott információk által felvetett minden kérdés, illetve az adatvédelmi pajzsot és annak működését érintő minden más kérdés megvitatására, és értelmezésünk szerint a Minisztérium saját mérlegelési jogkörében felkérheti más hivatalok – a hírszerző közösséget is ideértve – képviselőit az említett felülvizsgálatban való részvételre. Ez természetesen azon mechanizmusok mellett él, amelyeket a PPD-28 az uniós tagállamok számára biztosít a megfigyelési vonatkozású aggályok kijelölt külügyminisztériumi tisztviselőnél való felvetésére.

V. JOGORVOSLAT

Az USA joga számos jogorvoslati utat biztosít azoknak a magánszemélyeknek, akiket nemzetbiztonsági okokból jogellenes elektronikus megfigyelésnek vetettek alá. A FISA értelmében az USA bíróságaihoz fordulás nem korlátozódik egyesült államokbeli személyekre. Minden olyan egyén, aki perképességét igazolni tudja, jogorvoslatot kap a FISA

([1]) *Elérhető itt:* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

szerinti, jogellenes elektronikus megfigyelés vitatására. Például a FISA lehetővé teszi a jogellenes elektronikus megfigyelés alatt állók számára az USA kormánytisztviselői ellen személyes minőségükben kártérítési kereset indítását, beleértve a megtorló kártérítést és az ügyvédi díjakat is. *Lásd:* 50 U. S. C. § 1810. A perképességét igazolni képes magánszemélyek polgári pert indíthatnak az Egyesült Államok ellen pénzbeli kártérítés iránt, a perköltségekre kiterjedően, amennyiben a FISA szerinti elektronikus megfigyelés során róluk gyűjtött információkat jogellenesen és szándékosan felhasználták vagy nyilvánosságra hozták. *Lásd*: 18 U. S. C. § 2712. Amennyiben a kormány a FISA alapján sérelmet szenvedett személy elektronikus megfigyeléséből kapott vagy kinyert információt kívánja felhasználni az adott személy ellen az Egyesült Államokban folyó bírósági vagy közigazgatási eljárásban, a szándékáról a bíróságot és az adott személyt előzetesen értesítenie kell, aki ebben az esetben vitathatja a megfigyelés jogszerűségét és kérheti az információ mellőzését. *Lásd:* 50 U. S. C. § 1806. Végül a FISA büntetőjogi szankcióról is rendelkezik azon magánszemélyek esetében, akik hivatali visszaéléssel vesznek részt jogellenes elektronikus adatgyűjtésben, vagy akik szándékosan felhasználnak vagy közölnek jogellenes megfigyeléssel szerzett információkat. *Lásd* 50 U. S. C. § 1809.

Az uniós polgároknak más jogorvoslati lehetőségeik vannak az USA kormánytisztviselőivel szemben az adatok jogtalan felhasználása vagy megtekintése miatt, ideértve azokat a kormányzati tisztviselőket, akik adatbetekintés vagy információk színlelt nemzetbiztonsági célokra történő felhasználása során sértenek törvényt. A számítógépes csalásról és visszaélésről szóló törvény tiltja a szándékos illetéktelen hozzáférést (vagy az engedélyezett hozzáférés túllépését) pénzügyi intézménytől, az USA kormányzati számítógépes rendszeréből vagy internetes eléréssel valamely számítógépről történő információszerzés érdekében, illetve védett számítógépek zsarolási vagy csalási célú megrongálásával való fenyegetést. *Lásd*: 18 U. S. C. § 1030. Állampolgárságától függetlenül minden olyan személy, aki e törvény megszegése miatt kárt vagy veszteséget szenved, az 1030(g) cikk alapján perelheti a jogsértőt (a kormánytisztviselőt ideértve) kompenzációs kártérítésre vagy elrendelő vagy méltányos kártérítésre, függetlenül attól, hogy a büntetőeljárás megindult-e, feltéve, hogy a magatartás a törvényben meghatározott körülmények közül legalább egyet magában foglal. Az elektronikus hírközlési adatvédelmi törvény (Electronic Communications Privacy Act – ECPA) szabályozza a tárolt elektronikus kommunikációba, ügyleti nyilvántartásokba és harmadik személy hírközlési szolgáltató által tárolt előfizetői adatokba való kormányzati betekintést. *Lásd*: 18 U. S. C. §§ 2701-2712. Az ECPA feljogosítja a sérelmet szenvedett magánszemélyt a tárolt adatokba szándékosan illetéktelenül betekintő kormányzati tisztviselő elleni perindításra. Az ECPA állampolgárságtól függetlenül minden személyre vonatkozik és a sérelmet szenvedett személyek kártérítést és ügyvédi díjakat követelhetik. A pénzügyi adatok védelméhez való jogról szóló törvény (Right to Financial Privacy Act – RFPA) korlátozza az egyes ügyfelek banki és brókeri-kereskedési adataiba való kormányzati betekintést. *Lásd* 12 U. S. C. §§ 3401-3422. Az RFPA értelmében a bank vagy bróker-kereskedő ügyfele perelheti az USA kormányát törvényes, tényleges és megtorló kártérítésért az ügyféladatokba való jogellenes betekintés miatt, és annak megállapítása, hogy a jogellenes betekintés szándékos volt, automatikusan vizsgálatot eredményez az érintett kormánytisztviselők esetleges fegyelmi felelősségre vonása céljából. *Lásd* 12 U. S. C. § 3417.

Végül az információhoz való szabad hozzáférésről szóló törvény (Freedom of Information Act – FOIA) mindenki számára eszközt biztosít a bármely témában meglevő szövetségi ügynökségi adatokba betekinteni kívánó személyeknek, néhány kivételi kategóriával. *Lásd*: 5 U. S. C. § 552. Ide tartoznak a titkos nemzetbiztonsági információkba, mások személyes adataiba és bűnügyi nyomozásokba való betekintésre vonatkozó korlátok, és ezek hasonlóak az országok saját, információhoz való hozzáférési törvényeiben előírt korlátokhoz. Ezek a korlátok egyformán vonatkoznak az amerikaiakra és a nem amerikaiakra. A FOIA szerint kért adatok kiadása miatti jogviták esetében közigazgatási fellebbezésnek, majd bírói útnak van helye. A bíróságnak újból döntenie kell arról, hogy az adatok visszatartása jogszerű volt-e az 5 U.S.C. § 552(a)(4)(B) szerint, és kötelezheti a kormányt az adatokba való betekintés biztosítására. Egyes esetekben a bíróságok elutasították azon kormányzati állításokat, hogy az információkat titkosságuk miatt kell visszatartani ([1]). Noha pénzbeli kártérítés nem kérhető, a bíróság megítélheti az ügyvédi díjakat.

VI. KÖVETKEZTETÉS

Az Egyesült Államok elismeri, hogy jelfelderítési és egyéb hírszerzési tevékenységeinknek figyelembe kell vennie, hogy mindenkit – állampolgárságára és lakóhelyére tekintet nélkül – méltósággal és tisztelettel kell kezelni, és hogy minden személynek jogos adatvédelmi érdeke fűződik személyes adatai kezeléséhez. Az Egyesült Államok jelfelderítést csak nemzetbiztonsági és külpolitikai érdekei előmozdítására és polgárai, illetve szövetségeseinek és partnereinek polgárai védelmére használ. Röviden, a hírszerző közösség nem folytat bárkire – köztük egyszerű európai polgárokra – megkülönböztetés nélkül kiterjedő megfigyelést. Jelfelderítési adatgyűjtésre csak akkor kerül sor, ha azt szabályszerűen engedélyezik, és olyan módon, amely ezeknek a korlátozásoknak szigorúan megfelel; csak a helyettesítő források

([1]) *Lásd pl. New York Times kontra Igazságügyi Minisztérium*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union kontra CIA*, 710 F.3d 422 (D.C. Cir. 2014.

– a diplomáciai és nyilvános forrásokat is ideértve – elérhetőségének figyelembevételével, és olyan módon, amely előnyben részesíti a célszerű és megvalósítható alternatívákat. És minden olyan esetben, ha az a gyakorlatban megvalósítható, a jelfelderítés konkrét külföldi hírszerzési célpontokra vagy témákra összpontosítva folyik, diszkriminánsok használatával.

Az USA erre vonatkozó politikáját a PPD-28 erősítette meg. Ebben a keretben az egyesült államokbeli hírszerző ügynökségek nem rendelkeznek jogi hatáskörrel, erőforrásokkal és műszaki kapacitásokkal a világ teljes kommunikációjának lehallgatására. Ezek a hivatalok nem olvassák el az Egyesült Államokban vagy világszerte mindenkinek az e-mailjeit. A PPD-28-nak megfelelően az Egyesült Államok szilárd védelmi eszközöket biztosít a nem egyesült államokbeli személyek jelfelderítési tevékenységekkel gyűjtött személyes adatainak. A nemzetbiztonsággal összeegyeztethető legnagyobb mértékig ennek részét képezik a nem egyesült államokbeli személyekre vonatkozó személyes adatok megőrzésének és terjesztésének minimalizálását célzó szabályzatok és eljárásrendek, amelyek hasonlóak az egyesült államokbeli személyekre vonatkozókhoz. Emellett, a fentiekben kifejtetteknek megfelelően a 702. szakasz szerinti célzott FISA-hatáskör átfogó felügyelete példátlan. Végezetül az USA hírszerzési jogának az USA szabadságjogokról szóló törvényében meghatározott jelentős módosításai és a hírszerző közösségen belül az átláthatóság előmozdítását szolgáló, az ODNI által vezetett kezdeményezések nagyban fokozzák állampolgárságra tekintet nélkül valamennyi egyén magánéletének és alapvető szabadságjogainak védelmét.

Üdvözlettel:

Robert S. Litt

2016. június 21.

Mr. Justin S. Antonipillai
Tanácsos
Egyesült Államok Kereskedelmi Minisztérium
1401 Constitution Avenue, N.W.
Washington, DC 20230

Mr. Ted Dean
Államtitkár helyettes
Nemzetközi Kereskedelmi Igazgatóság
1401 Constitution Avenue, N.W.
Washington, DC 20230

Tisztelt Antonipillai Úr és Dean Úr!

Ezúton szeretnék további tájékoztatást nyújtani arról, hogy az Egyesült Államok hogyan végzi a jelfelderítési adatok tömeges gyűjtését. Amint a 28. elnöki politikai irányelv (PPD-28) 5 lábjegyzetében kifejtik, a „nagy mennyiségű" gyűjtés viszonylag nagy mennyiségű jelfelderítési információ vagy adat megszerzésére utal, olyan körülmények között, amikor a hírszerzés nem tud a konkrét célszemélyhez társítható azonosítót (pl. a célszemély e-mailcímét vagy telefonszámát) alkalmazni az adatgyűjtés fókuszálása céljából. Ez azonban nem jelenti, hogy az ilyen fajta adatgyűjtés „tömeges", vagy „megkülönböztetés nélküli" volna. A PPD-28 ugyanis azt is előírja, hogy „a jelfelderítési tevékenységnek a lehető legcélzottabbnak kell lennie". E megbízatás teljesítése érdekében a hírszerzés lépéseket tesz annak biztosítására, hogy még ha nem is tudjuk konkrét azonosítókkal célzottá tenni az adatgyűjtést, a gyűjtendő adatok valószínűleg olyan külföldi hírszerzési információkat tartalmazzanak, amelyek megfelelnek a korábbi levelemben ismertetett folyamat alapján az amerikai döntéshozók által megfogalmazott követelményeknek, és minimálisra csökkentik a begyűjtött, nem releváns információk mennyiségét.

Például a hírszerzés felkérést kaphat arra, hogy szerezzen jelfelderítési információkat valamely közel-keleti ország egyik régiójában működő olyan terrorista csoport tevékenységéről, amelyről azt feltételezik, hogy nyugat-európai országok elleni támadásra készül, azonban esetleg nem ismeri a terrorista csoportban közreműködő személyek nevét, telefonszámát, e-mailcímét vagy más konkrét azonosítóját. Ezt a csoportot adott esetben úgy célozhatjuk meg, hogy gyűjtjük az adott régióból származó és oda irányuló kommunikációt, és annak további felülvizsgálata és elemzése révén azonosítjuk a csoporthoz kapcsolódó kommunikációt. Ennek során a hírszerzés arra törekszik, hogy a „lehető legnagyobb mértékben" szűkítse az adatgyűjtést. Ez „nagy mennyiségű" adatgyűjtésnek tekinthető, mert a diszkriminánsok alkalmazása nem megvalósítható, de se nem „tömeges", se „nem megkülönböztetés nélküli", hanem a lehető legpontosabban fókuszált.

Tehát még ha nem is lehet konkrét kiválasztási tényezőket alkalmazni, az Egyesült Államok nem gyűjt minden kommunikációt a világszerte meglévő összes kommunikációs eszközből, hanem szűrőket és más technikai eszközöket alkalmaz, hogy azokra az eszközökre összpontosítsa az adatgyűjtést, amelyek valószínűleg külföldi hírszerzési értékkel rendelkező kommunikációt tartalmaznak. Ennek során az Egyesült Államok jelfelderítési tevékenysége csak egy töredékét érinti az interneten zajló kommunikációnak.

Továbbá amint a korábbi levelemben említettem, a PPD-28 hat konkrét célra korlátozza azokat az eseteket, amikor a hírszerzés felhasználhatja a tömegesen gyűjtött jelfelderítést, mivel a nagy mennyiségű adatgyűjtés a nem releváns kommunikáció gyűjtésének nagyobb kockázatával jár. A PPD-28 és a PPD-28-at végrehajtó ügynökségek szabályzatait a jelfelderítés révén szerzett személyes adatok megőrzésére és terjesztésére vonatkozóan is korlátozásokat állapítanak meg, függetlenül attól, hogy az információkat tömegesen vagy célzottan gyűjtötték, és attól, hogy az érintett milyen állampolgárságú.

Tehát a hírszerzés „nagy mennyiségű" adatgyűjtése nem „tömeges" vagy „megkülönböztetés nélküli", hanem az adatgyűjtés szűrésére szolgáló módszerek és eszközök alkalmazását jelenti annak érdekében, hogy olyan anyagokra fókuszálják az adatgyűjtést, amelyek megfelelnek a döntéshozók által a külföldi hírszerzésre vonatkozóan megfogalmazott követelményeknek, miközben minimálisra csökkentik a nem releváns információk gyűjtését, valamint szigorú

szabályokat írnak elő az esetleg megszerzett, nem releváns információk védelmére. Az e levélben ismertetett politikák és eljárások valamennyi nagy mennyiségű jelfelderítési adatgyűjtésre vonatkoznak, ideértve az Európába irányuló vagy onnan kiinduló kommunikációt, anélkül, hogy megerősíteném vagy cáfolnám, hogy történik-e ilyen adatgyűjtés.

Önök további tájékoztatást kértek tőlem az adatvédelmi és polgári szabadságjogi felügyelő tanács (PCLOB), a főellenőrök és azok jogkörei tekintetében is. A PCLOB a végrehajtó hatalmi ágba tartozó, független hivatal. Az öttagú, kétpárti tanács tagjait az elnök nevezi ki és a Szenátus erősíti meg ([1]). A tanács minden tagja hatéves hivatali időt tölt el. A tanács tagjait és személyzetét megfelelő személyi biztonsági tanúsítvánnyal látják el annak érdekében, hogy maradéktalanul eleget tehessenek törvényi feladataiknak és felelősségeiknek ([2]).

A PCLOB megbízatása annak biztosítására vonatkozik, hogy a szövetségi kormánynak a terrorizmus megelőzésére irányuló erőfeszítései egyensúlyban legyenek a magánélet és a polgári szabadságjogok védelmének szükségességével. A tanács két alapvető feladata a felügyelet és a tanácsadás. A PCLOB állapítja meg a saját napirendjét, és meghatározza, hogy milyen felügyeleti és tanácsadási tevékenységet kíván ellátni.

A PCLOB *felügyeleti* szerepében felülvizsgálja és elemzi a végrehajtó hatalmi ág által, a nemzetnek a terrorizmussal szembeni védelme értekében tett intézkedéseket, és gondoskodik arról, hogy az ilyen intézkedések iránti igény egyensúlyban legyen a magánélet és a polgári szabadságjogok védelmének szükségességével ([3]). A PCLOB a közelmúltban fejezte be a FISA 702. szakasza alapján működtetett megfigyelési programokra összpontosító, áttekintő felülvizsgálatot ([4]). Jelenleg az 12333. elnöki rendelet alapján működtetett hírszerzési tevékenységek felülvizsgálatát végzi ([5]).

A PCLOB *tanácsadói* szerepében gondoskodik arról, hogy a szabadságjogokkal kapcsolatos aggályokat megfelelően figyelembe vegyék a nemzetnek a terrorizmussal szembeni védelmére irányuló erőfeszítésekkel kapcsolatos törvények, rendeletek és politikák kidolgozása és végrehajtása folyamán ([6]).

A tanács törvényi felhatalmazással rendelkezik arra, hogy megbízatásának elvégzése érdekében betekintsen valamennyi vonatkozó ügynökségi nyilvántartásba, jelentésbe, ellenőrzésbe, felülvizsgálatba, dokumentumba, iratba, ajánlásba vagy egyéb vonatkozó anyagba, beleértve a törvény értelmében bizalmas információkat is ([7]). A tanács emellett meghallgatásokat végezhet, nyilatkozatokat vagy nyilvános tanúvallomásokat vehet fel a végrehajtó hatalmi ág tisztségviselőitől vagy alkalmazottaitól ([8]). A tanács továbbá írásban kérheti a legfőbb ügyészt, hogy a tanács nevében bocsásson ki bizonyításban való közreműködésre kötelező határozatot, amely arra kötelezi a végrehajtó hatalmi ágon kívüli feleket, hogy nyújtsák be a releváns információkat ([9]).

A PCLOB-t végül törvényben meghatározott nyilvános átláthatósági követelmények terhelik, amelyek kiterjednek arra, hogy nyilvános meghallgatások tartása és nyilvánosan hozzáférhető jelentések révén folyamatosan tájékoztassa tevékenységéről a közvéleményt, a lehető legnagyobb mértékben tiszteletben tartva a minősített adatok védelmét ([10]). A PCLOB emellett köteles jelentést tenni arról, ha egy végrehajtó hatalmi ügynökség nem követi az ajánlását.

A hírszerzésen (IC) belüli főellenőrök (IGs) a hírszerzés programjainak és tevékenységeinek ellenőrzését, vizsgálatát és felülvizsgálatát végzik, a rendszerszintű kockázatok, sebezhetőségek és hiányosságok meghatározása és kezelése céljából. A főellenőrök emellett kivizsgálják azokat a panaszokat vagy azon vádakra vonatkozó információkat, miszerint

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) *Lásd általában véve:* https://www.pclob.gov/library.html#oversightreports.
([5]) *Lásd általában véve:* https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); *lásd továbbá:* A PCLOB tanácsadó feladatra vonatkozó politikája és eljárása, Politika 2015-004, *elérhető az alábbi internetcímen:* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

a hírszerzés programjai és tevékenységei során törvények, szabályok vagy rendeletek megsértését, illetve hűtlen kezelést; pénzeszközök nagymértékű pazarlását; hatalommal való visszaélést követtek le, vagy a közegészségügyet és biztonságot érintő lényeges és konkrét veszélyt idéztek elő. A főellenőr függetlensége alapvető eleme az általa kiadott minden jelentés, megállapítás és ajánlás tárgyilagosságának és feddhetetlenségének. A főellenőr függetlenségének megőrzésével kapcsolatos legkritikusabb mozzanatok közé tartozik a főellenőr kinevezésének és felmentésének eljárása; a különálló operatív, költségvetési, valamint személyzeti jogkörök; továbbá a végrehajtó hatalmi ügynökség vezetőinek és a Kongresszusnak címzett kettős jelentéstételi kötelezettség.

A Kongresszus független főellenőri hivatalt hozott létre mindegyik végrehajtó hatalmi ügynökségnél, többek között a hírszerzés mindegyik szervezeténél ([1]). A 2015-ös költségvetési évre vonatkozó hírszerzési engedélyezési törvény elfogadását követően majdnem mindegyik hírszerzési szervezetet felügyelő főellenőrt az elnök nevezi ki és a Szenátus erősíti meg, beleértve az Igazságügyi Minisztériumot, a Központi Hírszerző Ügynökséget, a Nemzetbiztonsági Ügynökséget és a hírszerzést ([2]). Továbbá a főellenőrök határozatlan időre kinevezett, pártatlan tisztviselők, akiket csak az elnök menthet fel. Bár az Egyesült Államok Alkotmánya úgy rendelkezik, hogy a főellenőr felmentése az elnök jogköre, az elnök ritkán élt ezzel a jogosítvánnyal, és ehhez az elnöknek a főellenőr felmentése előtt 30 nappal írásbeli indokolást kell küldenie a Kongresszusnak ([3]). A főellenőr kinevezésére vonatkozó, említett eljárás biztosítja, hogy a végrehajtó hatalmi ág tisztviselői ne befolyásolják jogtalanul a főellenőr kiválasztását, kinevezését vagy felmentését.

Másrészt a főellenőrök jelentős törvényi felhatalmazással rendelkeznek arra, hogy ellenőrzéseket, vizsgálatokat és felülvizsgálatokat folytassanak a végrehajtó hatalom programjai és műveletei tekintetében. A törvényben előírt áttekintő vizsgálatok és felülvizsgálatok mellett a főellenőrök tág mérlegelési jogkörrel rendelkeznek, hogy a felügyeleti jogkörükkel élve felülvizsgálják az általuk kiválasztott programokat és tevékenységeket ([4]). A törvény szavatolja, hogy e jogkör gyakorlása során a főellenőrök független forrásokkal rendelkezzenek feladataik ellátáshoz, többek között joguk van saját személyzetük felvételéhez, és költségvetési igényüket külön dokumentálhatják a Kongresszus számára ([5]). A törvény biztosítja, hogy a főellenőrök hozzáférjenek a feladataik ellátásához szükséges információkhoz. Ez a jogkörük kiterjed arra, hogy közvetlenül hozzáférhetnek az ügynökség minden nyilvántartásához és minősítésre tekintet nélkül az ügynökség programjainak és műveleteinek részleteit tartalmazó információkhoz; bizonyításban való közreműködésre kötelező közigazgatási határozatot adhatnak ki információk és dokumentumok beszerzése céljából; valamint eskütételt végezhetnek ([6]). A végrehajtó hatalmi ügynökség vezetője korlátozott esetekben megtilthatja a főellenőr tevékenységét, például ha egy főellenőri ellenőrzés vagy vizsgálat jelentősen sértené az Egyesült Államok nemzetbiztonsági érdekeit. E jogkör érvényesítése szintén rendkívül ritka, és ehhez arra van szükség, hogy az ügynökség vezetője 30 napon belül értesítse a Kongresszust a jogkör gyakorlásának indokáról ([7]). A nemzeti hírszerzés igazgatója eddig még soha nem élt ezzel a korlátozási jogkörrel semmiféle főellenőri tevékenység esetében.

Harmadrészt a főellenőrök feladata, hogy a végrehajtó hatalmi ág programjaival és tevékenységeivel kapcsolatos csalásokról és egyéb súlyos problémákról, visszaélésekről, valamint hiányosságokról szóló jelentésekben teljes körű és aktuális tájékoztatást nyújtsanak a végrehajtó hatalmi ügynökségek vezetőinek és a Kongresszusnak ([8]). A kettős jelentéstétel fokozza a főellenőr függetlenségét azáltal, hogy biztosítja a főellenőri felügyelet átláthatóságát, valamint lehetővé teszi az ügynökségek vezetőinek, hogy még azt megelőzően végrehajtsák a főellenőr ajánlásait, hogy a Kongresszus jogalkotási intézkedést tehetne. Például a főellenőrök a törvény értelmében kötelesek féléves jelentéseket készíteni, amelyekben ismertetik a szóban forgó problémákat, valamint az addig az időpontig megtett korrekciós intézkedéseket ([9]). A végrehajtó hatalmi ügynökségek komolyan veszik a főellenőri megállapításokat és ajánlásokat, és a főellenőrök ezekben a jelentésekben, valamint a Kongresszusnak küldött, és bizonyos esetekben a nagyközönség

([1]) A főellenőrről szóló 1978. évi módosított törvény (a továbbiakban: IG-törvény) 2. és 4. szakasza; az 1947. évi módosított nemzetbiztonsági törvény (a továbbiakban: NB-törvény) 103H(b) és (e) szakasza; a központi hírszerzésről szóló törvény (a továbbiakban: CIA-törvény) 17(a) szakasza.

([2]) *Lásd:* Pub. L. No. 113-293, 128 Stat. 3990, (2014. dec. 19.). Kizárólag a Védelmi Hírszerzési Ügynökség és a Nemzeti Térinformatikai Hírszerző Ügynökség főellenőreit nem az elnök nevezi ki; a DOD főellenőre és a hírszerzés főellenőre azonban párhuzamos hatáskörrel rendelkeznek az említett ügynökségek felett.

([3]) Lásd a módosított 1978. évi IG-törvény 3. szakaszát; az NB-törvény 103H(c) szakaszát; valamint a CIA-törvény 17(b) szakaszát.

([4]) *Lásd* az 1947. évi IG-törvény 4(a) és 6(a)(2) szakaszait; az NB-törvény 103H(e) és (g)(2)(A) szakaszát; a CIA-törvény 17(a) és (c) szakaszát.

([5]) Az IG-törvény 3(d), 6(a)(7) és 6(f) szakasza. az NB-törvény 103H(d), (i), (j) és (m) szakasza; a CIA-törvény 17(e)(7) és (f) szakasza.

([6]) Az IG-törvény 6(a)(1), (3), (4), (5) és (6) szakasza; az NB-törvény 103H(g)(2) szakasza; a CIA-törvény 17(e)(1), (2), (4) és (5) szakasza.

([7]) *Lásd pl.* az IG-törvény 8(b) és 8E(a) szakaszait; az NB-törvény 103H(f) szakaszát; a CIA-törvény 17(b) szakaszát.

([8]) Az IG-törvény 4(a)(5) szakasza; az NB-törvény 103H(a)(b)(3) és (4) szakasza; a CIA-törvény 17(a)(2) és (4) szakasza.

([9]) Az IG-törvény 2(3), 4(a), és 5. szakasza; az NB-törvény 103H(k) szakasza; a CIA-törvény 17(d) szakasza. Az Igazságügyi Minisztérium főellenőre nyilvánosságra hozott jelentéseit hozzáférhetővé teszi az interneten az alábbi címen: http://oig.justice.gov/reports/all.htm. A hírszerzés főellenőre hasonlóan nyilvánosságra hozza féléves jelentéseit az alábbi internetcímen: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

számára készített jelentésekben gyakran számolhatnak be arról, hogy az ügynökségek elfogadják és végrehajtják a főellenőri ajánlásokat ([1]). E kettős jelentéstételi struktúra mellett szintén a főellenőrök felelősek a végrehajtó hatalmi ág visszaéléseit bejelentő személyeknek a megfelelő kongresszusi felügyelő bizottságokhoz kalauzolásáért, hogy azok közölhessék a végrehajtó hatalmi programok és tevékenységek során bekövetkező állítólagos csalásra, pazarlásra vagy visszaélésre vonatkozó információkat. A bejelentők személyazonosságát nem hozzák a végrehajtó hatalom tudomására, ami megóvja a visszaélést bejelentő személyeket a főellenőrnek tett bejelentés megtorlásaként hozott esetleges tiltott személyzeti intézkedésektől vagy biztonsági ellenőrzéssel kapcsolatos intézkedéstől ([2]). Mivel a főellenőri vizsgálatok forrásai gyakran a visszaélést bejelentő személyek, fokozza a főellenőri felügyelet hatékonyságát, hogy e személyek a végrehajtó hatalom általi befolyásolás nélkül beszámolhatnak aggályaikról a Kongresszusnak. E függetlenségből eredően a főellenőrök tárgyilagosan és feddhetetlenül segíthetik elő a végrehajtó hatalmi ügynökségek gazdaságos működését, hatékonyságát és elszámoltathatóságát.

Végezetül a Kongresszus létrehozta a főellenőrök feddhetetlenségével és hatékonyságával foglalkozó tanácsot. E tanács többek között kidolgozza az ellenőrzésekre, vizsgálatokra és felülvizsgálatokra vonatkozó főellenőri normákat; előmozdítja a képzést; valamint a főellenőrök hivatali kötelezettségszegésével kapcsolatos állítások felülvizsgálatára vonatkozó jogkörrel rendelkezik, így kritikusan tekinthet azokra a főellenőrökre, akiket minden más szerv megfigyelésével bíztak meg ([3]).

Bízom benne, hogy hasznavehető információval szolgálhattam az Önök számára.

Tisztelettel:
Robert S. Litt
Főtanácsos

([1]) Az IG-törvény 2(3), 4(a), és 5. szakasza; az NB-törvény 103H(k) szakasza; a CIA-törvény 17(d) szakasza. Az Igazságügyi Minisztérium főellenőre nyilvánosságra hozott jelentéseit hozzáférhetővé teszi az interneten az alábbi címen: http://oig.justice.gov/reports/all.htm. A hírszerzés főellenőre hasonlóan nyilvánosságra hozza féléves jelentéseit az alábbi internetcímen: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Az IG-törvény 7. szakasza; az NB-törvény 103H(g)(3) szakasza; a CIA-törvény 17(e)(3) szakasza.

([3]) Az IG-törvény 11. szakasza.

VII. MELLÉKLET

Bruce Swartz, a legfőbb ügyész helyettese és nemzetközi ügyek tanácsosa (az USA Igazságügyi Minisztériuma) levele

2016. február 19.

Justin S. Antonipillai úr
Tanácsos
Az USA Kereskedelmi Minisztériuma
1401 Constitution Ave., NW
Washington, DC, 20230

Ted Dean úr
államtitkár-helyettes
Nemzetközi Kereskedelmi Minisztérium
1401 Constitution Ave., NW
Washington, DC, 20230

Tisztelt Antonipillai és Dean úr!

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]). Ezek a jogi eljárások megkülönböztetésmentesek annyiban, hogy azokat használják az Egyesült Államokban a vállalatoktól történő információszerzéshez, ideértve azokat a vállalatokat is, amelyek önmaguk tanúsítják az USA-EU adatvédelmi pajzs keretnek való megfelelésüket, tekintet nélkül az érintett állampolgárságára. 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 USA 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 Kiegészítés 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). Amennyiben a végzés követelménye nem érvényesül, a kormányzati tevékenységnek a Negyedik Kiegészítés szerinti „ésszerűségi” tesztnek kell megfelelnie. Ezért maga az Alkotmány biztosítja, hogy az USA kormánya ne rendelkezzen korlátlan vagy önkényes hatalommal magánadatok megszerzésére.

Büntetőügyekben eljáró bűnüldöző hatóságok:

A szövetségi ügyészek, akik az Igazságügyi Minisztérium tisztviselői(DOJ), 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

([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, *lásd:* 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 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 rákövetkező rendelkezések.

([2]) Ez a dokumentum a szövetségi bűnüldözési és szabályozó hatóságokat tárgyalja; az állami jog megsértése ügyében az államok 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 előírt védelem vonatkozhat. Az állami jogban előírt védelemnek legalább az USA Alkotmányában – a Negyedik Kiegészítést is beleértve – nyújtott védelemmel azonos szintűnek kell lennie.

dokumentumok és más adatok kiadását, beleértve az esküdtszék által kibocsátott idézéseket, közigazgatási idézéseket és házkutatási parancsokat, és a szövetségi bűnügyi lehallgatási és hívásrögzítési hatáskörök szerint más kommunikációkhoz is hozzáférhet.

Bizonyításfelvételben vagy a tárgyaláson való közreműködésre vagy kötelező vádesküdtszéki parancs: A bizonyításfelvételben való közreműködésre kötelező parancsot célzott bűnüldözési nyomozások alátámasztására használják. Az esküdtszék által kiadott parancs a vádesküdtszék hivatalos kötelezése (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 ésszerűtlen annak túlzó hatóköre, elnyomó vagy terhes jellege miatt. A címzett indítványt terjeszthet be a parancs ezen okok miatti vitatására. *Lásd:* Fed. R. Crim. 17. o. 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 felhasználására üzleti adatok, elektronikusan tárolt információk vagy más ingók egészségügyi csalással, gyermekbántalmazással, titkosszolgálati védelemmel, ellenőrzött anyagok használatával kapcsolatos vizsgálatokban, és kormányzati hivatalokat érintő legfőbb ügyészi vizsgálatokban 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 ésszerűségét annak túlzott hatóköre, elnyomó vagy terhes jellege miatt.

Hívásrögzítésre és lehallgatásra vonatkozó bírósági végzések: A bűnügyi hívásrögzítésre és lehallgatásra vonatkozó rendelkezések értelmében a bűnüldöző szervek bírósági végzést kaphatnak valamely telefonszámról vagy e-mail címről valós idejű, tartalmat nem felfedő tárcsázási, átirányítási, hívásfogadási és jelzési információk beszerzésére annak igazolása mellett, hogy a kapott információ egy folyamatban levő bűnügyi nyomozásban jelentőséggel bír. *Lásd:* 18 U. S. C. §§ 3121-3127. Ilyen eszközök jogellenes használata vagy beszerelése szövetségi bűncselekmény.

Az elektronikus hírközlési adatvédelmi 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 tárolt kommunikációról 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 adatgyűjtés tolakodó jellegétől függően emeli az adatvédelmi garanciák szintjét. Az előfizetői regisztrációs adatok, IP-címek és kapcsolódó időbélyegek esetében a büntetőügyekben eljáró 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 hatóságok az arra vonatkozó alapos gyanú alapján szereznek be bírói parancsot, hogy a szóban forgó felhasználói fiók bűncselekmény bizonyítékát tartalmazza. Az SCA rendelkezik a polgári jogi helytállásról és a büntetőjogi szankciókról is.

A szövetségi lehallgatási törvény szerinti megfigyelésre szóló 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. §§ 2510-2522. Ez a hatáskör csak bírósági végzésre elérhető, 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. A törvény polgári jogi helytállást és büntetőjogi szankciókat ír elő a lehallgatási rendelkezések megszegése esetére.

Házkutatási parancs – 41. szabály: A bűnüldöző szervek az Egyesült Államokban helyiségeket vizsgálhatnak át, 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 akkor használják, ha a helyiség rendőrségi fizikai átvizsgálása azért szükséges, mert fennáll a bizonyítékok megsemmisítésének veszélye, ha idézést vagy a bemutatást előíró egyéb végzést küldenek a vállalatnak. Lásd az USA Alkotmányának IV. kiegészítését (részletesebben fentebb tárgyaltuk), Fed. R. Crim. 41. o. A házkutatási parancs alanya kérelmezheti a parancs visszavonását annak túlzó hatóköre, zaklató jellege vagy beszerzésének egyéb szabálytalansága miatt, és a sérelmet szenvedett fél indítványozhatja a jogellenes házkutatás során beszerzett bizonyíték kizárását. Lásd a *Mapp kontra Ohio ügyet*, 367 U.S. 643 (1961).

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 elé, és amelyek a magánélet és az alapvető szabadságok védelmére vonatkozó védelmi eszközöket is tartalmaznak. Például a legfőbb ügyész irányelvei a Szövetségi Nyomozó Iroda (FBI) belföldi nyomozási műveleteire (2008 szeptembere) (a továbbiakban: a legfőbb ügyész FBI irányelvei), elérhető itt: http://www.justice.gov/archive/opa/docs/guidelines.pdf, korlátokat szabnak meg a szövetségi bűncselekmények nyomozásához kapcsolódó nyomozati eszközök használatára. 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 vizsgálatait és egyéb tevékenységeit jogszerűen és ésszerűen 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. oldalát. 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(DIOG), az útmutató egy olyan átfogó kézikönyv, amely részletes korlátokat állít fel a nyomozati eszközök használatára és útmutatást ad annak biztosítására, hogy az alapvető szabadságjogok és a magánélet minden nyomozásban védelmet kapjon. A szövetségi ügyészek nyomozati tevékenységének korlátait ismertető további szabályokat és szabályzatokat az **Egyesült Államok ügyészségi kézikönyve** (USAM) fekteti le, amely elérhető az interneten itt: http://www.justice.gov/usam/united-states-attorneys-manual.

Polgári és szabályozó hatóságok (közérdek):

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 idézéseket adhatnak ki vállalatoknak üzleti adatok, elektronikusan tárolt információk vagy más ingóságok tárgyában. Ezeket a hivatalokat a közigazgatási vagy polgári idézési hatáskör gyakorlásában nem csak szervezeti alapszabályuk korlátozza, hanem az idézések 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 feladatkörükhöz jelentőséggel bírnak. A közigazgatási idézés címzettje továbbá bíróságon vitathatja az adott idézés végrehajtását annak bizonyításával, hogy a hivatal nem a korábban tárgyalt alapvető ésszerűségi 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 közigazgatási idézéseket azon az alapon, hogy azok a banktitokról szóló törvénybe és végrehajtási rendeleteibe ütköznek. *Lásd:* 31 U.S.C. § 5318, 31 C.F.R. X. rész. Más vállalkozások a tisztességes hiteljelentési törvényre hagyatkozhatnak, *lásd:* 15 U.S.C. § 1681b, vagy más ágazati jogszabályok gazdájára. 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 törvény, 12 U.S.C. §§ 3401–3422. 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 Kiegészítés követelményeinek. Lásd az FTC kontra Travelers Health Association 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.

Üdvözlettel:

Bruce C. Swartz

A legfőbb ügyész helyettese és a nemzetközi ügyek tanácsosa