



EURÓPAI
BIZOTTSÁG

Brüsszel, 2013.11.27.
COM(2013) 847 final

**A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A
TANÁCSNAK**

**a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedet vállalatok
szempontjából**

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedet vállalatok szempontjából

BEVEZETÉS

A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK irányelv (a továbbiakban: adatvédelmi irányelv) határozza meg a személyes adatok uniós tagállamokból más, Unión kívüli országokba való továbbítására vonatkozó szabályokat¹, amennyiben az ilyen adattovábbítások e jogi aktus hatálya alá tartoznak².

Az irányelv értelmében a Bizottság megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít a belföldi jog, vagy az egyének jogainak védelme érdekében vállalt nemzetközi kötelezettségek révén. Ebben az esetben nem kell alkalmazni az ilyen országokba történő adattovábbításokra vonatkozó különleges korlátozásokat. E határozatokat általában „megfelelési határozatokként” említik.

A Bizottság által 2000. július 26-án elfogadott 520/2000/EK határozat³ (a továbbiakban: **védett adatkikötőről szóló határozat**) elismeri az Egyesült Államok Kereskedelmi Minisztériuma által kiadott, védett adatkikötőre (Safe Harbour) vonatkozó alapelveket és az ezzel kapcsolatos gyakran felvetődő kérdéseket (a továbbiakban: alapelvek, illetve gyakran felvetődő kérdések), mivel azok megfelelő védelmet biztosítanak az EU-ból továbbított személyes adatok számára. A védett adatkikötőről szóló határozat meghozatalára a 29. cikk szerinti munkacsoport véleményét, valamint a 31. cikk szerinti bizottságnak a tagállamok minősített többsége által elfogadott véleményét követően került sor. Az 1999/468/EK tanácsi határozattal összhangban, az Európai Parlament előzetesen megvizsgálta a védett adatkikötőről szóló határozatot.

Ennek következtében a védett adatkikötőről szóló jelenlegi határozat olyan feltételek mellett is lehetővé teszi személyes adatok továbbítását⁴ az uniós tagállamokból⁵ az alapelveket elfogadó amerikai vállalatok számára, amelyek a két kontinens adatvédelmi szabályozásának lényeges eltérései miatt egyébként nem felelnének meg a megfelelő szintű adatvédelemre vonatkozó uniós normáknak.

A védett adatkikötőre vonatkozó jelenlegi szabályozás működése a csatlakozó vállalatok kötelezettségvállalásaira és öntanúsítására épül. E szabályok elfogadása önkéntes, de a

¹ Az adatvédelmi irányelv 25. és 26. cikke állapítja meg az EU-ból az EGT-n kívüli harmadik országokba történő személyesadat-továbbítások jogi keretét.

² A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló, 2008. november 27-i 2008/977/IB kerethatározat 13. cikke kiegészítő szabályokat állapít meg, amennyiben a szóban forgó adattovábbítás az egyik tagállam által egy másik tagállam számára továbbított vagy hozzáférhetővé tett adatokra vonatkozik, és az utóbbi tagállam harmadik államnak vagy nemzetközi szervnek szándékozik továbbítani a szóban forgó adatokat, bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából.

³ 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., 2000.8.25., 7. o.

⁴ A fentiek nem zárják ki, hogy az uniós adatvédelmi irányelvet végrehajtó tagállami jogszabályok esetleges egyéb követelményeit alkalmazzák az adatok feldolgozására.

⁵ Az EGT három tagállamából történő adattovábbítás hasonlóképpen érintett, miután az 1999. június 25-i 38/1999 határozat (HL L 296., 2000.11.23. 41. o.) az EGT-megállapodásra is kiterjesztette a 95/46/EGK irányelv hatályát.

szabályok kötelezők a csatlakozók számára. A szóban forgó szabályozás alapelvei a következők:

- (a) A csatlakozó vállalatok adatvédelmi politikájának átláthatósága,
- (b) A védett adatkikötőre vonatkozó alapelvek beépítése a vállalatok adatvédelmi politikájába, valamint
- (c) Végrehajtás, ideértve a hatósági végrehajtást is.

A védett adatkikötő említett alapvető kérdései felülvizsgálatra szorulnak az alábbi **új összefüggésekre tekintettel**:

- (a) az adatáramlás exponenciális növekedése, amely korábban csupán kísérőjelensége volt a digitális gazdaság gyors növekedésének, mára azonban annak központi elemévé vált, továbbá az adatgyűjtés, -feldolgozás és -használat terén rendkívül jelentős fejlődés következett be,
- (b) az adatáramlások kiemelkedő fontossága, különösen a transzatlanti gazdaság számára,⁶
- (c) a védett adatkikötőre vonatkozó szabályozáshoz csatlakozó amerikai vállalatok számának gyors emelkedése, amely 2004 óta nyolcszorosára (a 2004. évi 400-ról a 2013-ban 3246-ra) nőtt,
- (d) az Egyesült Államok hírszerzési programjairól a közelmúltban napvilágra jutott információk, amelyek újból megkérdőjelezzik azon védelem szintjét, amelyet a védett adatkikötőre vonatkozó szabályozás garantálni látszott.

A fentiekre tekintettel a Bizottság felméri a védett adatkikötőre vonatkozó szabályozás működését. A felmérés a Bizottság által gyűjtött **bizonyítékokon**, az EU-USA adatvédelmi kapcsolattartó csoport 2009-ben végzett munkáján, egy független vállalkozó 2008-ban készített tanulmányán⁷, valamint az USA hírszerzési programjairól napvilágra került értesítéseket *(lásd a párhuzamos dokumentumot)* követően létrehozott EU-USA ad hoc munkacsoporttól (a továbbiakban: a munkacsoport) származó információkon **alapul**. E közlemény a **Bizottság két értékelő jelentését követi**, amelyek 2002-ben⁸, illetve 2004-ben⁹, a védett adatkikötőre vonatkozó szabályozás kezdeti szakaszában készültek.

⁶ Egyes tanulmányok szerint, ha a kötelező erejű vállalati szabályok, szerződéses rendelkezésminták és a védett adatkikötő alkalmazásának megszűnése következtében zavar keletkezne a szolgáltatásokban és a határokon átnyúló adatáramlásban, az uniós GDP-re gyakorolt kedvezőtlen hatás elérhetné a -0,8 – -1,3 %-ot, az USA-ba irányuló európai uniós szolgáltatásexport pedig 6,7%-kal zuhanna a versenyképesség terén elszenvedett veszteség miatt. Lásd: „The Economic Importance of Getting Data Protection Right” (Az adatvédelemhez való jog érvényesítésének gazdasági jelentősége) a Nemzetközi Politikai Gazdaságtan Európai Központjának 2013. márciusi tanulmánya az Egyesült Államok Kereskedelmi Kamarája számára.

⁷ A Namuri Egyetem Informatikai és Jogi Kutatási Központja (*Centre de Recherche Informatique et Droit*) által, 2008-ban a Bizottság számára készített hatásvizsgálati tanulmány.

⁸ Bizottsági szolgálati munkadokumentum: „The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce” (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 szóló 2000. július 26-i 2000/520/EK bizottsági határozat alkalmazása), SEC (2002) 196, 2002.12.13.

⁹ Bizottsági szolgálati munkadokumentum: „The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce” (Az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló 2000/520/EK bizottsági határozat végrehajtása), SEC (2004) 1323, 2004.10.20.

2. A VÉDETT ADATKIKÖTŐ SZERKEZETE ÉS MŰKÖDÉSE

2.1. A védett adatkikötő szerkezete

A védett adatkikötőhöz csatlakozni kívánó amerikai vállalatoknak: a) meg kell határozniuk nyilvánosan hozzáférhető adatvédelmi politikájukat, amelynek el kell fogadnia az alapelveket, és ténylegesen meg kell felelnie azoknak, valamint b) öntanúsítványt kell adniuk, vagyis nyilatkozniuk kell az alapelvek betartásáról az Egyesült Államok Kereskedelmi Minisztériuma számára. Az öntanúsítványt évente ismételtelen be kell nyújtani. A védett adatkikötőről szóló határozat I. mellékletéhez csatolt, a védett adatkikötőre vonatkozó alapelvek felölelik a személyes adatok anyagi jogi védelmére (az adatok sértetlenségére, biztonságára, megválasztására és harmadik fél számára történő továbbítására vonatkozó elvek), és az érintettek eljárási jogaira (értesítési, betekintési és jogérvényesítési elvek) vonatkozó követelményeket.

Ami a védett adatkikötőre vonatkozó program egyesült államokbeli érvényesítését illeti, ebben két amerikai intézmény – az Egyesült Államok Kereskedelmi Minisztériuma és a Szövetségi Kereskedelmi Bizottság – játszik lényeges szerepet.

A **Kereskedelmi Minisztérium** felülvizsgálja a vállalatoktól kapott, védett adatkikötőre vonatkozó öntanúsítványokat és évente ismételtelen benyújtott tanúsítványokat annak biztosítása érdekében, hogy azok tartalmazzák a programban való részvételhez szükséges valamennyi elemet¹⁰. A Minisztérium naprakésszé teszi azoknak a vállalatoknak a jegyzékét, amelyek benyújtották az öntanúsító levelet, a jegyzéket és leveleket pedig közzéteszi a weboldalán. Emellett figyelemmel kíséri a védett adatkikötő működését, és eltávolítja a jegyzékből azokat a vállalatokat, amelyek nem felelnek meg az alapelveknek.

A **Szövetségi Kereskedelmi Bizottság** fogyasztóvédelmi hatáskörén belül – a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza értelmében – fellép a tisztességtelen vagy csalárd gyakorlatok ellen. A Szövetségi Kereskedelmi Bizottság jogérvényesítési intézkedései kiterjednek a védett adatkikötőhöz való csatlakozással kapcsolatos valótlan nyilatkozatok, illetve azon esetek vizsgálatára, amikor a programban résztvevő vállalatok nem felelnek meg az említett alapelveknek. Az Egyesült Államok Közlekedési Minisztériuma¹¹ az illetékes szerv azokban a konkrét ügyekben, amikor a védett adatkikötőre vonatkozó alapelveket légi fuvarozókkal szemben érvényesítik.

A védett adatkikötőről szóló jelenlegi határozat a tagállami hatóságok által alkalmazandó uniós joganyag részét képezi. A határozat értelmében az EU nemzeti **adatvédelmi hatóságainak** különleges esetekben joguk van felfüggeszteni a védett adatkikötőre vonatkozó tanúsítvánnyal rendelkező vállalatok felé irányuló adattovábbítást¹². A Bizottságnak nincs tudomása arról, hogy a nemzeti adatvédelmi hatóságok akár egyetlen esetben is alkalmazták volna a felfüggesztést a védett adatkikötő 2000. évi létrehozása óta. A védett adatkikötőről szóló határozat alapján az uniós adatvédelmi hatóságokat megillető hatáskörtől függetlenül, e hatóságok akár nemzetközi adattovábbítások esetén is jogosultak közbeavatkozni az 1995. évi adatvédelmi irányelvben meghatározott általános adatvédelmi elvek tiszteletben tartása érdekében.

¹⁰ Amennyiben egy vállalat tanúsítványa vagy ismételt tanúsítványa nem teljesíti a védett adatkikötő követelményeit, a Kereskedelmi Minisztérium értesíti a vállalatot arról, hogy milyen lépéseket kell tennie (pl.: a politika leírásának pontosítása, módosítása), mielőtt véglegesíthetik az adott vállalat tanúsítványát.

¹¹ Az Egyesült Államok Szövetségi Törvénykönyve 49. címének 41712. szakasza alapján.

¹² Közelebbről, abban a két helyzetben kérhető az adattovábbítások felfüggesztése, amikor:

a) az amerikai kormányzati szerv megállapította, hogy a vállalat megsérti a védett adatkikötő adatvédelmi alapelveit; vagy
b) alaposan valószínűsíthető, hogy megsértik a védett adatkikötő adatvédelmi alapelveit; okkal feltételezik, hogy az érintett végrehajtási mechanizmus sem most, sem később nem tesz megfelelő és időszzerű lépéseket az adott eset rendezésére; a folytatódó adattovábbítás az érintettek súlyos károsodásának veszélyével fenyeget; a tagállam illetékes hatóságai a körülményekhez képest elfogadható erőfeszítéseket tettek, hogy a vállalatot értesítsék, és lehetőséget adjanak neki a válaszára.

Amint a védett adatkikötőre vonatkozó jelenlegi határozat hangsúlyozza, a **Bizottság rendelkezik hatáskörrel** arra, hogy – a 182/2011/EU rendeletben meghatározott vizsgálóbizottsági eljárásnak megfelelően eljárva – a határozat végrehajtása során szerzett tapasztalatok fényében kiigazítsa a jogszabályt, vagy bármikor felfüggeszse, illetve korlátozza annak hatályát. Ezt különösen akkor írják elő, ha amerikai oldalon rendszerszintű hiányosság mutatkozik, például amennyiben az Egyesült Államokban a védett adatkikötőre vonatkozó alapelveknek való megfelelés biztosításáért felelős bármely szerv nem hatékonyan tölti be szerepét, illetve ha az Egyesült Államok jogszabályainak követelményei szigorúbbá válnak a védett adatkikötőre vonatkozó alapelveknél. Bármely más bizottsági határozathoz hasonlóan a jogszabály is módosítható, sőt akár hatályon kívül helyezhető, egyéb okok miatt is.

2.2. A védett adatkikötő működése

A **3246¹³ tanúsítással rendelkező vállalat** között egyaránt szerepelnek kis- és nagyvállalatok¹⁴. Jóllehet a Szövetségi Kereskedelmi Bizottság jogérvényesítési hatásköre nem terjed ki a pénzügyi szolgáltatási és távközlési iparágra, amelyeket ezért kizártak a védett adatkikötő szabályozásából, mégis számos iparág és szolgáltatási szektor tartozik a tanúsítással rendelkező vállalatok körébe, köztük jól ismert internetes vállalatok, továbbá különféle iparágak az informatikai és számítógépes szolgáltatásoktól, a gyógyszeriparon, az utazási és üdülési szolgáltatásokon át a gyógykezelési és hitelkártya szolgáltatásokig¹⁵. Ezek főként olyan amerikai vállalatok, amelyek az EU belső piacán nyújtanak szolgáltatásokat. Néhány uniós cég – például a Nokia vagy a Bayer – leányvállalata is szerepel köztük. Ezek 51 %-a európai foglalkoztatottak olyan adatait feldolgozó cég, amelyeket humánerőforrással kapcsolatos megfontolásokból továbbítanak az Egyesült Államokba¹⁶.

Egyes uniós adatvédelmi hatóságok körében **növekvő mértékű aggodalom** nyilvánul meg a védett adatkikötőre vonatkozó jelenlegi program alapján történő adattovábbításokkal kapcsolatosan. Egyes tagállami adatvédelmi hatóságok kritikával illeték az alapelvek rendkívül általános megfogalmazását, valamint az öntanúsítás és az önszabályozás nagymértékű alkalmazását. Hasonló aggodalmak merültek fel az iparági szereplők részéről, amelyek említést tettek arról, hogy a jogérvényesítés hiánya miatt versenytorzulások következnek be.

A védett adatkikötőre vonatkozó jelenlegi szabályozás a vállalatok önkéntes csatlakozásán, e csatlakozó vállalatok öntanúsításán, valamint az öntanúsítványban vállalt kötelezettségek hatósági érvényesítésén alapszik. Ilyen feltételek mellett az átláthatóság és a végrehajtás esetleges hiányosságai aláássák a védett adatkikötőre vonatkozó program alapjait.

Ha amerikai oldalon az átláthatóságot vagy a jogérvényesítést érintő bármely hiányosság mutatkozik, az azt eredményezi, hogy a felelősség az európai adatvédelmi hatóságokat és a programot igénybe vevő vállalatokat terheli. A német adatvédelmi hatóságok 2010. április 29-én kiadott határozta felszólítja az Európából az Egyesült Államokba adatokat továbbító vállalatokat, hogy tevékenyen működjenek közre annak ellenőrzésében, hogy az Amerikába adatokat importáló vállalatok valóban megfelelnek-e a védett adatkikötőre vonatkozó adatvédelmi alapelveknek, továbbá azt ajánlja, hogy „legalább az exportáló vállalat

¹³ 2013. szeptember 26-án **3246 „aktív”**, illetve **935 „nem aktív”** szervezetet tüntettek fel a védett adatkikötő jegyzékén.

¹⁴ A legfeljebb 250 alkalmazottal rendelkező szervezetek aránya 60 % (3246-ból 1925), a legalább 251 alkalmazottal rendelkezőké pedig **40 %** (3246-ból 1295).

¹⁵ Például a MasterCard bankok ezreivel áll üzleti kapcsolatban, és ez a vállalat egyértelmű példája annak, amikor a védett adatkikötő nem helyettesíthető a személyes adatok továbbítására vonatkozó más jogi eszközzel, például kötelező erejű vállalati szabályokkal vagy szerződéses rendelkezésekkel.

¹⁶ A védett adatkikötőt alkalmazó szervezetek **51 %-a** (3246-ból 1671) a humánerőforrás-adatok szervezését is a védett adatkikötőre vonatkozó tanúsítvány alapján végzi (így elfogadta, hogy együttműködik az uniós adatvédelmi hatóságokkal, és eleget tesz azok előírásainak).

győződjön meg arról, hogy továbbra is érvényes-e az importőr védett adatkikötőre vonatkozó tanúsítványa”¹⁷.

Miután napvilágra kerültek az Egyesült Államok hírszerzési programjára vonatkozó értesülések, a német adatvédelmi hatóságok 2013. július 24-én további aggodalmaiknak adtak hangot amiatt, hogy „nagy valószínűség szerint megsértik a Bizottság határozataiban foglalt alapelveket”¹⁸. Egyes esetekben bizonyos adatvédelmi hatóságok (például a brémai adatvédelmi hatóság) felszólítják az amerikai szolgáltatók számára személyes adatokat továbbító vállalatokat, hogy tájékoztassák az adatvédelmi hatóságot arról, hogy az érintett szolgáltatók megakadályozzák-e a Nemzeti Biztonsági Ügynökség adatokhoz való hozzáférését, és milyen módon teszik ezt. Az ír adatvédelmi hatóság arról számolt be, hogy – miután napvilágra kerültek az Egyesült Államok nemzetbiztonsági ügynökségeinek programjaival kapcsolatos értesülések – a közelmúltban két panasz érkezett hozzá a védett adatkikötőre vonatkozó programmal kapcsolatban, azonban elutasította ezek kivizsgálását, arra hivatkozva, hogy a személyes adatok harmadik országba történt továbbítása megfelelt az ír adatvédelmi jog követelményeinek. Egy hasonló panaszt követően a luxemburgi adatvédelmi hatóság megállapította, hogy a Microsoft és a Skype – az Egyesült Államokba történő adattovábbítás során – megfelelt a luxemburgi adatvédelmi törvénynek¹⁹. Azóta azonban az ír Felső Bíróság (*High Court*) helyt adott egy bírósági felülvizsgálati iránti kérelemnek, amelynek alapján felül fogja vizsgálni az ír adatvédelmi biztosnak az amerikai hírszerzési programokkal kapcsolatos passzivitását. A két panasz egyikét az „Európa kontra Facebook (EvF)” elnevezésű diákcsoport nyújtotta be, amely a Yahoo-val szemben is hasonló panasszal élt Németországban. Az érintett adatvédelmi hatóságok jelenleg végzik e panasz feldolgozását.

Az adatvédelmi hatóságoknak a hírszerzéssel kapcsolatos értesülésekre adott elérő válaszai azt tanúsítják, hogy fennáll a valós veszélye a védett adatkikötőre vonatkozó program széttagolódásának, továbbá kérdések merülnek fel a program megvalósulásának mértékével kapcsolatosan.

3. A CSATLAKOZÓ VÁLLALATOK ADATVÉDELMI POLITIKÁJÁNAK ÁTLÁTHATÓSÁGA

A védett adatkikötőről szóló határozathoz csatolt (II. melléklet) 6. gyakran felvetődő kérdés értelmében a védett adatkikötő keretében történő tanúsítás iránt érdeklődő vállalatoknak meg kell küldeniük adatvédelmi politikájukat a Kereskedelmi Minisztérium részére, és nyilvánosságra kell hozniuk azt. E politikának az adatvédelmi elvek elfogadására vonatkozó kötelezettségvállalást kell tartalmaznia. A program működése szempontjából alapvető fontosságú az a követelmény, hogy az öntanúsító vállalatoknak **nyilvánosan hozzáférhetővé kell tenniük adatvédelmi politikájukat**, és az adatvédelmi alapelvek elfogadására vonatkozó nyilatkozatukat.

¹⁷ Lásd a Düsseldorf Kreist 2010. április 28-29-i határozatát. [Lásd: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29 April 2010 in Hannover: \(A legfelsőbb adatvédelmi hatóságok magánszektorbeli adatvédelemre vonatkozó 2010. április 28-29-i, hannoveri határozata\):](http://www.bfdi.bund.de/SharedDocs/Publikationen/Entscheidungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile)
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entscheidungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Ugyanakkor Peter Hustinx, európai adatvédelmi biztos az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottságának 2013. október 7-i meghallgatásán annak a véleményének adott hangot, hogy a védett adatkikötőt illetően „komoly javulás történt, és a legtöbb kérdést mostanra rendezték”:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

¹⁸ Lásd a német adatvédelmi biztosok konferenciájának állásfoglalását, amely azt hangsúlyozza, hogy a hírszerző szolgálatok komoly veszélyt jelentenek a Németország és az Európán kívüli országok közötti adatforgalomra:
http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

¹⁹ Lásd a luxemburgi adatvédelmi hatóság 2013. november 18-i sajtóközleményét.

Ha e vállalatok nem biztosítanak megfelelő hozzáférést adatvédelmi politikájukhoz, az hátrányos azoknak az egyéneknek a számára, akiknek a személyes adatait összegyűjtik és feldolgozzák, valamint az **értesítési elv megsértésének** minősülhet. Ilyen esetekben előfordulhat, hogy azok az egyének, akiknek az adatait továbbítják az Unióból, nincsenek tisztában jogaikkal, valamint az öntanúsító vállalatok kötelezettségeivel.

Ezenfelül a vállalatoknak az adatvédelmi alapelvek betartására vonatkozó kötelezettségvállalása megalapozza a **Szövetégi Kereskedelmi Bizottság arra vonatkozó jogkörét, hogy** – a kötelezettségek megszegése, például tisztességtelen vagy csalárd gyakorlat esetén – **érvényesítse az említett elveket** a vállalatokkal szemben. Az amerikai vállalatok átláthatóságának hiánya megnehezíti a Szövetégi Kereskedelmi Bizottság számára a felügyelet gyakorlását, és rontja a jogérvényesítés hatékonyságát.

Az évek során jelentős számú öntanúsító vállalat nem hozta nyilvánosságra adatvédelmi politikáját és/vagy nem tett közzé nyilvános közleményt az adatvédelmi alapelvek elfogadásáról. A védett adatkikötőre vonatkozó 2004-es jelentés kiemelte annak szükségességét, hogy a Kereskedelmi Minisztérium **aktívabb szerepet játsszon** e követelmény **teljesítésének ellenőrzésében**.

A Kereskedelmi Minisztérium 2004 óta **új informatikai eszközöket** fejlesztett ki abból a célból, hogy segítséget nyújtson a vállalatoknak átláthatósági kötelezettségeik teljesítéséhez. A programra vonatkozó információk hozzáférhetők a Kereskedelmi Minisztérium védett adatkikötővel foglalkozó weboldalán²⁰, amelyre a vállalatok feltölthetik adatvédelmi politikájukat. A Kereskedelmi Minisztérium arról számolt be, hogy a vállalatok kihasználják ezt a lehetőséget, és a védett adatkikötőhöz való csatlakozás iránti kérelmük benyújtásakor közzéteszik adatvédelmi politikáikat a Kereskedelmi Minisztérium weboldalán²¹. Ezenfelül a Kereskedelmi Minisztérium 2009 és 2013 között közzétett egy sor iránymutatást azon vállalatok számára, amelyek csatlakozni kívánnak a védett adatkikötőhöz (például „Öntanúsításra vonatkozó iránymutatás”, valamint „Hasznos tanácsok az öntanúsításnak való megfeleléshez”)²².

A vállalatok különféle mértékben felelnek meg az átláthatósági követelményeknek. Jóllehet egyes vállalatok arra szorítkoznak, hogy az öntanúsítási eljárás keretében közlik adatvédelmi politikájuk leírását a Kereskedelmi Minisztériummal, a többségük saját weboldalán is közzéteszi ezt a politikát, amellet, hogy feltölti azt a Kereskedelmi Minisztérium weboldalára. Ugyanakkor **e politikákat nem minden esetben jelenítik meg fogyasztóbarát és könnyen olvasható formában**. Az adatvédelmi politikákra mutató hivatkozások nem mindig működnek megfelelően, és nem minden esetben a helyes weboldalra mutatnak.

A határozat és mellékletei értelmében az a követelmény, hogy a vállalatoknak nyilvánosságra kell hozniuk adatvédelmi politikájukat, **túlmutat** az öntanúsítványnak a Kereskedelmi Minisztériummal való **pusztá közlésén**. A gyakran felvetődő kérdésekben meghatározottak szerint a tanúsításra vonatkozó követelmény felöleli az adatvédelmi politika leírását, valamint arra vonatkozó átlátható információkat, hogy hol érhető el az adatvédelmi politika a nyilvánosság számára betekintésre²³. Az adatvédelmi nyilatkozatoknak egyértelműnek, és a nyilvánosság számára könnyen hozzáférhetőnek kell lenniük. E nyilatkozatoknak

²⁰ <http://www.export.gov/SafeHarbour/>

²¹ <https://SafeHarbour.export.gov/list.aspx>

²² Az iránymutatás hozzáférhető a program alábbi weboldalán: <http://export.gov/SafeHarbour/> Hasznos tanácsok: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

²³ A Kereskedelmi Minisztérium 2013. november 12-én megerősítette, hogy „A nyilvános weboldallal rendelkező, és fogyasztók/ügyfelek/látogatók adatait kezelő vállalatoknak mostantól meg kell jeleníteniük weboldalukon a védett adatkikötőre vonatkozó alapelveknek megfelelő adatvédelmi politikájukat” („A védett adatkikötő keretének végrehajtására irányuló USA-EU együttműködés” elnevezésű, 2013. november 12-i dokumentum).

tartalmazniuk kell egy hivatkozást a Kereskedelmi Minisztérium védett adatkikötőre vonatkozó, a program összes „aktív” résztvevőjét felsoroló weboldalára, továbbá egy linket az alternatív vitarendezési szolgáltatóhoz. A program 2000 és 2013 közötti résztvevői közül azonban számos vállalat nem teljesítette ezeket a követelményeket. A Bizottsággal folytatott 2013. februári munkamegbeszélések során a Kereskedelmi Minisztérium elismerte, hogy a tanúsítvánnyal rendelkező vállalatok körében akár 10%-ot is elérheti azok aránya, amelyek valójában nem tették fel nyilvános weboldalukra a védett adatkikötő elfogadását megerősítő nyilatkozatot.

A közelmúltbeli statisztikai adatok azt tanúsítják, hogy továbbra is problémát jelentenek a **védett adatkikötő elfogadására vonatkozó hamis állítások**. A védett adatkikötőben való részvételüket állító vállalatok mintegy 10 %-a nem szerepel a Kereskedelmi Minisztériumnak a program aktív résztvevőit tartalmazó jegyzékén²⁴. E hamis állítások az alábbi két forrásból származnak: olyan vállalatoktól, amelyek soha nem vettek részt a védett adatkikötőben, valamint olyan vállalatoktól, amelyek egyszer csatlakoztak a programhoz, később azonban nem nyújtották be évente ismételt öntanúsítványukat a Kereskedelmi Minisztériumnak. Ebben az esetben e vállalatok nevét továbbra is feltüntetik a védett adatkikötőre vonatkozó weboldalon található jegyzékben, de a tanúsítás státusza rovatban a „nem aktív” megjegyzés szerepel, ami azt jelenti, hogy a vállalat tagja a programnak, így változatlanul köteles biztosítani a már feldolgozott adatok védelmét. A Szövetségi Kereskedelmi Bizottság rendelkezik hatáskörrel arra, hogy eljárjon a védett adatkikötőre vonatkozó alapelvekkel kapcsolatos csalárd gyakorlatok és azok megszegése esetén (lásd az 5.1. szakaszt). A „hamis állításokkal” kapcsolatos tisztázatlanság kihat a program hitelességére.

Az Európai Bizottság 2012 és 2013 folyamán, a rendszeres kapcsolattartás során figyelmeztette a Kereskedelmi Minisztériumot, hogy az átláthatósági követelmények teljesítéséhez nem elegendő pusztán az, hogy a vállalatok eljuttatják adatvédelmi politikájuk leírását a Kereskedelmi Minisztériumhoz. Az adatvédelmi nyilatkozatokat nyilvánosan hozzáférhetővé kell tenni. Emellett felkérték a Kereskedelmi Minisztériumot, hogy **erősítse a vállalatok weboldalának rendszeres ellenőrzését** az első öntanúsítási eljárás vagy annak éves megújítása keretében végzett ellenőrzési eljárást követően, továbbá hozzon intézkedéseket azokkal a vállalatokkal szemben, amelyek nem tesznek eleget az átláthatósági követelményeknek.

A **Kereskedelmi Minisztérium** – az uniós aggodalmakra adott első válaszlépésként – **2013 márciusa óta kötelezővé tette** a védett adatkikötőben részt vevő, nyilvános weboldallal rendelkező vállalatok számára, hogy ezen a weboldalon elérhetővé tegyék a fogyasztók/felhasználók adataira vonatkozó adatvédelmi politikájukat. A Kereskedelmi Minisztérium ezzel egyidejűleg megkezdte az összes olyan vállalat felszólítását, amelynek az adatvédelmi politikája még nem tartalmazott hivatkozást a Kereskedelmi Minisztérium védett adatkikötőre vonatkozó weboldalára, hogy tüntessen fel ilyen linket, amely közvetlenül elérhetővé teszi a védett adatkikötő résztvevőinek hivatalos jegyzékét és annak weboldalát a vállalat weboldalára látogató fogyasztók számára. Ez lehetővé teszi az európai adatalanyok számára, hogy – további internetes keresés nélkül – azonnal ellenőrizzék a vállalatnak a Kereskedelmi Minisztériumhoz benyújtott kötelezettségvállalásait. Emellett a Kereskedelmi Minisztérium megkezdte a vállalatok értesítését arról, hogy közzétett adatvédelmi

²⁴

A Galexia elnevezésű ausztrál tanácsadó cég 2013 szeptemberében összehasonlította a védett adatkikötőben meglévő tagságot illetően 2008-ban, illetve 2013-ban tett „hamis állításokat”. A tanulmánynak az a legfontosabb megállapítása, hogy 2008 és 2013 között a védett adatkikötőben résztvevők létszámának (1 109-ről 3 246-ra történő) emelkedésével párhuzamosan a hamis állítások száma 206-ról 427-re növekedett. http://www.galexia.com/public/about/news/about_news-id225.html

politikájukban fel kell tüntetniük a független vitarendezési szolgálható elérhetőségére vonatkozó információkat²⁵.

Ezt a folyamatot fel kell gyorsítani annak érdekében, hogy 2014. márciusig (vagyis a vállalatok évente történő ismételt tanúsítására vonatkozó, az új követelmények 2013. márciusi bevezetésétől számított határidőig) valamennyi tanúsítással rendelkező vállalat maradéktalanul megfeleljen a védett adatkikötőre vonatkozó követelményeknek.

Mindazonáltal továbbra is fennállnak az aggályok azzal kapcsolatban, hogy valamennyi öntanúsító vállalat maradéktalanul eleget tesz-e az átláthatósági követelményeknek. A Kereskedelmi Minisztériumnak szigorúbban kell figyelemmel kísérnie és vizsgálnia, hogy a vállalatok eleget tesznek-e a kezdeti öntanúsítási eljárás és az éves megújítás alkalmával vállalt kötelezettségeknek.

4. A VÉDETT ADATKIKÖTŐRE VONATKOZÓ ALAPELVEK BEÉPÍTÉSE A VÁLLALATOK ADATVÉDELMI POLITIKÁJÁBA

Az öntanúsító vállalatoknak meg kell felelniük a határozat I. mellékletében meghatározott adatvédelmi alapelveknek ahhoz, hogy megszerezzék és megtartsák a védett adatkikötő kedvezményét.

A Bizottság 2004-es jelentésében megállapította, hogy jelentős számú **vállalat nem megfelelően építette be a védett adatkikötőre vonatkozó alapelveket** az adatfeldolgozási politikájába. Például az egyének nem minden esetben kaptak egyértelmű és átlátható tájékoztatást arról, hogy mely célokból dolgozták fel az adataikat, vagy pedig nem tették lehetővé számukra a kívülmaradást, amennyiben az adataikat harmadik fél tudomására hozzák, vagy az eredeti adatgyűjtés céljaival összeegyeztethetetlen célra használják fel. A Bizottság 2004. évi jelentése szerint a Kereskedelmi Minisztériumnak *„aktívabban kell fellépnie a védett adatkikötőhöz való hozzáférés, és az alapelvek tudatosítása tekintetében”*²⁶.

Ebben a tekintetben kevés előrehaladás történt. A Kereskedelmi Minisztériumnak 2009. január 1. óta a megújítást megelőzően értékelnie kell azon vállalatok adatvédelmi politikáját, amelyek meg kívánják újítani a védett adatkikötőre vonatkozó, évente megújítandó tanúsítványukat. Az értékelés köre azonban korlátozott. **Nem kerül sor az öntanúsító vállalatok tényleges gyakorlatának teljes körű értékelésére**, ami jelentősen erősítené az öntanúsítási eljárás hitelességét.

Miután a Bizottság felkérte a Kereskedelmi Minisztériumot, hogy szigorúbban és rendszeresebben ellenőrizze az öntanúsító vállalatokat, **jelenleg több figyelmet szentelnek az új kérelmeknek**. 2010 és 2013 között komoly mértékben növekedett – az ismételten tanúsító vállalatok esetében megduplázódott, a védett adatkikötő új résztvevői esetében pedig háromszorosára nőtt – azoknak az új kérelmeknek a száma, amelyeket nem fogadtak el, hanem az adatvédelmi politika javítása céljából visszaküldtek az érintett vállalatoknak²⁷. A

²⁵

A Kereskedelmi Minisztérium 2013 márciusa és szeptembere között:

- 101 olyan vállalkozást, amely már feltöltötte a védett adatkikötőre vonatkozó alapelveknek megfelelő adatvédelmi politikáját a védett adatkikötővel foglalkozó weboldalra értesített arról, hogy adatvédelmi politikáját a vállalat weboldalára is fel kell tennie;
- 154 olyan vállalatot, amely ezt még nem tette meg, értesített arról, hogy a védett adatkikötővel foglalkozó weboldalra mutató hivatkozást kell feltüntetniük adatvédelmi politikájukban;
- több mint 600 vállalatot értesített arról, hogy a független vitarendezési szolgálható elérhetőségére vonatkozó információkat fel kell tüntetniük adatvédelmi politikájukban.

²⁶

Lásd a 2004. évi jelentés SEC (2004) 1323 8. oldalát.

²⁷

A Kereskedelmi Minisztérium által 2013 szeptemberében szolgáltatott statisztikai adatok szerint a Minisztérium 2010-ban az 512 első alkalommal tanúsító vállalat 18 %-át (93) és az 1 417 ismételt tanúsító 16 %-át (231) hívta fel arra, hogy javítsák adatvédelmi politikájukat és/vagy a védett adatkikötő alkalmazásait. Miután azonban a Bizottság 2013. szeptember közepén

Kereskedelmi Minisztérium arról biztosította a Bizottságot, hogy kizárólag akkor véglegesíthetők a tanúsítványok vagy az ismételt tanúsítványok, ha a vállalat adatvédelmi politikája megfelel valamennyi követelménynek, különösen annak, hogy tartalmazzon kifejezett kötelezettségvállalást a védett adatkikötő megfelelő adatvédelmi alapelveinek elfogadására, továbbá hogy az adatvédelmi politika nyilvánosan hozzáférhető legyen. Az adott vállalat a védett adatkikötő jegyzékében szereplő adatok között köteles meghatározni a vonatkozó adatvédelmi politika elérhetőségének helyét. Továbbá a weboldalán köteles egyértelműen megadni egy alternatív vitarendezési szolgáltató adatait, valamint feltüntetni egy hivatkozást a Kereskedelmi Minisztérium weboldalán található, védett adatkikötőre vonatkozó öntanúsítványra. Becslések szerint azonban a védett adatkikötő résztvevőinek több mint 30 %-a a weboldalán található adatvédelmi politikájában nem nyújt vitarendezésre vonatkozó tájékoztatást²⁸.

A Kereskedelmi Minisztérium az érintett vállalatok többségét az adott vállalat kifejezett kérésére távolította el a védett adatkikötőre vonatkozó jegyzékből (pl. olyan vállalatokat, amelyek beolvadás vagy felvásárlás miatt megszűntek, megváltoztatták vagy megszüntették üzleti tevékenységüket). Kisebb számban töröltek vállalatokra vonatkozó, idejélmúlt bejegyzéseket amiatt, hogy az abban szereplő weboldalak nem látszottak működőnek, és az adott vállalat már évek óta „Nem aktív” tanúsítási státusszal rendelkezett²⁹. Fontos, hogy a jelek szerint a törlésre egyetlen esetben sem amiatt került sor, hogy a Kereskedelmi Minisztérium ellenőrzése megfelelőségi problémák feltárásához vezetett volna.

A védett adatkikötőre vonatkozó jegyzékben szereplő bejegyzés nyilvános értesítésként és a vállalat védett adatkikötőre vonatkozó kötelezettségvállalásainak rögzítésére szolgál. **A védett adatkikötőre vonatkozó alapelvek elfogadásával kapcsolatos kötelezettségvállalás időben nem korlátozott** azon adatok esetében, amelyeket a vállalat abban az időszakban kapott, amikor a védett adatkikötő kedvezményét élvezte, továbbá a vállalatnak mindaddig alkalmaznia kell az alapelveket az adatalanyokra, amíg tárolja, felhasználja vagy közli a szóban forgó adatokat, még abban az esetben is, ha időközben bármilyen okból elhagyja a védett adatkikötőt.

Az alábbiak szerint alakult azoknak a védett adatkikötőben való részvételt **kérelmező** vállalatoknak a száma, amelyek **nem mentek át sikerrel** a Kereskedelmi Minisztérium **adminisztratív felülvizsgálatán**, és ezért sohasem került sor a védett adatkikötőre vonatkozó jegyzékbe való felvételükre: **2010-ben** az első alkalommal tanúsító 513 vállalat mindössze **6 %-át** (33) nem vették fel a védett adatkikötőre vonatkozó jegyzékbe amiatt, hogy nem feleltek meg a Kereskedelmi Minisztérium öntanúsítással kapcsolatos előírásainak. **2013-ban** az első alkalommal tanúsító 605 vállalat **12 %-át** (75) nem vették fel a védett adatkikötőre vonatkozó jegyzékbe amiatt, hogy nem felelt meg a Kereskedelmi Minisztérium öntanúsítással kapcsolatos előírásainak.

A felügyelet átláthatóságának növelésére vonatkozó minimumkövetelményként a Kereskedelmi Minisztériumnak a weboldalán fel kell sorolnia az összes olyan vállalatot, amelyet töröltek a védett adatkikötőből, és indokolnia kell, hogy miért nem újították meg a tanúsítást. A Kereskedelmi Minisztérium védett adatkikötőben résztvevő vállalatokat

többször sürgette az összes kérelem szigorú, körültekintő és rendszeres ellenőrzését, a Minisztérium értesítést küldött a 602 első alkalommal tanúsító vállalat 56 %-ának (340) és az 1 809 ismételt tanúsító 27 %-ának (493), felszólítva őket adatvédelmi politikájuk javítására.

²⁸ Chris Connolly (Galexia) nyilatkozata az Európai Parlament Állampolgári Jogi, Bel- és Igazságügyi Bizottságának 2013. október 7-i meghallgatásán.

²⁹ Az Egyesült Államok Kereskedelmi Minisztériuma 2011 decembere óta 323 vállalatot törölt a védett adatkikötőre vonatkozó jegyzékből: 94 vállalatot töröltek az üzleti tevékenységük megszűnése miatt, 88 vállalatot felvásárlás vagy beolvadás miatt, 95-öt az anyavállalat kérésére, 41 vállalatot, az ismételt tanúsítás kérelmezésének többszöri elmulasztása miatt, további 5 vállalatot pedig különféle egyéb okokból kifolyólag.

felsoroló jegyzékében szereplő „Nem aktív” megjegyzést nem pusztán tájékoztatásnak kell tekinteni, hanem azt arra vonatkozó **egyértelmű** – szóbeli és grafikus – **figyelmeztetésnek** kell kisélnie, hogy az adott vállalat jelenleg nem teljesíti a védett adatkikötő követelményeit.

Ezenfelül egyes vállalatok továbbra sem építették be maradéktalanul a védett adatkikötő alapelveit. A 3. szakaszban tárgyalt átláthatósági problémától eltekintve, az öntanúsító vállalatok adatvédelmi politikája gyakran abban a tekintetben sem egyértelmű, hogy milyen célokból gyűjtik az adatokat, és az érintetteknek joguk van-e megválasztani, hogy az adatok harmadik felek tudomására hozhatók-e vagy sem; ez pedig kérdésessé teszi, hogy betartják-e az értesítés és a választási lehetőség adatvédelmi alapelvét. Az értesítés és a választási lehetőség alapvető fontosságú ahhoz, hogy az adatalanyok ellenőrizhessék, hogy mi történik a személyes adataikkal.

A megfelelési folyamat első fontos lépése – a védett adatkikötőre vonatkozó adatvédelmi alapelveknek a vállalatok adatvédelmi politikájába való beépítése – nem megfelelően biztosított. A Kereskedelmi Minisztériumnak prioritásként kell kezelnie ezt a kérdést, olyan módszereket kidolgozva, amelyek biztosítják a vállalatok működési gyakorlatának és az ügyfelekkel való kapcsolattartásának megfelelőségét. **A Kereskedelmi Minisztériumnak aktívan fel kell lépnie annak érdekében, hogy a védett adatkikötőre vonatkozó alapelveket ténylegesen beépítsék a vállalatok adatvédelmi politikájába, tehát nem hagyatkozhat csupán az egyénektől érkező panaszokra ahhoz, hogy megtegye a jogérvényesítési intézkedéseket.**

5. A HATÓSÁGI VÉGREHAJTÁS

Több mechanizmus áll rendelkezésre a védett adatkikötőre vonatkozó program hatékony végrehajtásához, valamint ahhoz, hogy jogorvoslatot biztosítsanak az egyének számára azokban az esetekben, amikor az adatvédelmi alapelvek be nem tartása a személyes adataikat érinti.

A végrehajtás elve szerint hatékony megfelelési mechanizmusokat kell belefoglalni az öntanúsító szervezetek adatvédelmi politikájába. A 11., 5. és 6. gyakran felvetődő kérdésre adott válaszban tovább pontosított, adatvédelmi végrehajtási elv értelmében e követelmény olyan **független eljárási mechanizmusokhoz** való csatlakozás révén teljesíthető, amelyek esetében nyilvánosan kijelentették, hogy hatáskörrel rendelkeznek arra, hogy eljárjanak az alapelvek betartásának elmulasztásával kapcsolatos egyéni panaszok ügyében. Másik lehetőségként ez úgy is megvalósítható, hogy az adott szervezet kötelezettséget vállal az **európai adatvédelmi bizottsággal** való együttműködésre³⁰. Ezenfelül az öntanúsító vállalatok a Szövetségi Kereskedelmi Bizottság hatáskörébe tartoznak a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza értelmében, amely tiltja a tisztességtelen vagy csalárd kereskedelmi, illetve kereskedelmet érintő cselekményeket vagy gyakorlatokat³¹.

A 2004-es jelentés aggodalmakat fogalmazott meg a védett adatkikötőre vonatkozó program végrehajtása tekintetében, konkrétan azzal kapcsolatban, hogy a Szövetségi Kereskedelmi

³⁰

Az európai adatvédelmi bizottság az illetékes szerv az egyének által benyújtott azon panaszok kivizsgálása és elbírálása tekintetében, amelyek a védett adatkikötőre vonatkozó alapelveknek a védett adatkikötőben részt vevő amerikai vállalatok általi állítólagos megsértésére vonatkoznak. A védett adatkikötőre vonatkozó alapelvek betartását tanúsító vállalatoknak választaniuk kell a független eljárási mechanizmusok teljesítése, illetve az európai adatvédelmi bizottsággal való együttműködés között annak érdekében, hogy orvosolják a védett adatkikötőre vonatkozó alapelvek nem teljesítéséből származó problémákat. Az amerikai vállalatoknak mindazonáltal kötelező együttműködniük az európai adatvédelmi bizottsággal, amennyiben valamely foglalkoztatási jogviszonnyal összefüggésben dolgoznak fel az Unióból származó, emberi erőforrással kapcsolatos személyi adatokat. Ha a vállalat kötelezettséget vállal az európai adatvédelmi bizottsággal való együttműködésre, azt is vállalnia kell, hogy követi a bizottság tanácsait, amennyiben a testület arra az álláspontra helyezkedik, hogy a vállalatnak különleges intézkedéseket – például jogorvoslati vagy kártérítési intézkedéseket – kell tennie a védett adatkikötőre vonatkozó alapelvek teljesítése érdekében.

³¹

A Közlekedési Minisztérium hasonló hatáskörrel rendelkezik az Egyesült Államok Szövetségi Törvénykönyve 49. címének 41712. szakasza szerinti légi fuvarozók esetében.

Bizottságnak aktívabban kell fellépnie a vizsgálatok megindítása és az egyének saját jogaikkal kapcsolatos ismereteinek bővítése terén. Emellett az is aggodalomra adott okot, hogy nem volt egyértelmű a Szövetségi Kereskedelmi Bizottság hatásköre az emberierőforrás-adatokkal kapcsolatos alapelvek érvényesítése tekintetében.

Az emberierőforrás-adatokért felelős fellebbviteli szervhez – az uniós adatvédelmi bizottsághoz – egyetlen emberierőforrás-adatokat érintő panasz érkezett³². A panaszok hiánya alapján azonban nem vonható le olyan következtetés, hogy a program teljes körűen működőképes. A vállalatok megfelelőségére vonatkozó, hivatalból indított vizsgálatokat kell bevezetni az adatvédelmi követelmények tényleges végrehajtásának ellenőrzése érdekében. Az uniós adatvédelmi hatóságoknak szintén intézkedéseket kell hozniuk, hogy felhívják a figyelmet az európai adatvédelmi bizottság létezésére.

Problémákra mutattak rá a végrehajtó szerv szerepét betöltő alternatív eljárási mechanizmusok működési módja tekintetében. Számos ilyen szerv nem rendelkezik megfelelő eszközökkel ahhoz, hogy orvosolja azokat az eseteket, amikor nem teljesítik az alapelveket. Foglalkozni kell ezekkel a hiányosságokkal.

5.1. Szövetségi Kereskedelmi Bizottság

A Szövetségi Kereskedelmi Bizottság jogérvényesítési intézkedéseket hozhat azokban az esetekben, amikor a vállalatok megsértik az általuk vállalt, védett adatkikötőre vonatkozó kötelezettségeket. A Szövetségi Kereskedelmi Bizottság vállalta, hogy amennyiben a védett adatkikötő már létrejött, elsőbbséget biztosít az uniós tagállamok hatóságaitól érkező ügyek felülvizsgálatának³³. Mivel a szabályozás első tíz évére vonatkozóan nem érkezett panasz, a Szövetségi Kereskedelmi Bizottság úgy döntött, hogy az általa lefolytatott valamennyi adatvédelmi és adatbiztonsági vizsgálat során igyekszik feltárni a védett adatkikötő megsértéseit. A Szövetségi Kereskedelmi Bizottság 2009 óta 10 esetben hozott vállalatokkal szembeni jogérvényesítési intézkedést a védett adatkikötő megsértése alapján. Ezek az intézkedések – komoly pénzbüntetés kilátásba helyezése mellett – a jogsértés orvoslására felszólító végzések kiadásához vezettek, amelyek megtiltották az adatvédelemmel – így a védett adatkikötő szabályainak teljesítésével – kapcsolatos félrevezető magatartást, és átfogó adatvédelmi programokat és 20 évre szóló ellenőrzéseket írtak elő a vállalatok számára. A vállalatok kötelesek elfogadni, hogy a Szövetségi Kereskedelmi Bizottság felkérésére független értékelések készülnek az adatvédelmi programjaikról. Ezekről az értékelésekről rendszeresen beszámolnak a Szövetségi Kereskedelmi Bizottság számára. A Szövetségi Kereskedelmi Bizottság végzései azt is megtiltják az említett vállalatoknak, hogy félrevezető állításokat tegyenek az adatvédelmi gyakorlatukat, illetve a védett adatkikötőben vagy más, hasonló adatvédelmi programokban való részvételüket illetően. Ez az eset fordult elő például a Szövetségi Kereskedelmi Bizottság Google-lal, Facebookkal és Myspace-szel szembeni vizsgálatainak során.³⁴ A Google 2012-ben elfogadta, hogy 22,5 millió USD összegű bírságot fizet az egyezséget elrendelő végzés állítólagos megsértésének jóvátétele céljából. A

³² A panasz egy svájci állampolgártól származik, ezért az uniós adatvédelmi bizottság a svájci adatvédelmi hatóság elé utalta azt (az Egyesült Államok védett adatkikötőre vonatkozó külön programmal rendelkezik Svájc vonatkozásában).

³³ Lásd a 2000. július 26-i 2000/520/EK bizottsági határozat V. mellékletét.

³⁴ A Szövetségi Kereskedelmi Bizottság a 2009 és 2012 közötti időszakban tíz intézkedést hozott a védett adatkikötőre vonatkozó kötelezettségek érvényesítésére: FTC kontra Javian Karnani, és Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Lásd: „Federal Trade Commission of Safe Harbour Commitments” (a Szövetségi Kereskedelmi Bizottság védett adatkikötőre vonatkozó kötelezettségvállalásokkal kapcsolatos tevékenysége): http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Lásd továbbá: „Case Highlights” (az ügyek vázlata): <http://business.ftc.gov/us-eu-Safe-Harbour-framework>. A legtöbb említett ügyben olyan vállalatokkal kapcsolatban jelentkeztek problémák, amelyek csatlakoztak a védett adatkikötőhöz, később pedig továbbra is résztvevőnek tüntették fel magukat, anélkül, hogy megújították volna az éves tanúsítást.

Szövetségi Kereskedelmi Bizottság minden adatvédelmi vizsgálat keretében hivatalból megvizsgálja, hogy sor került-e a védett adatkikötő megsértésére.

A Szövetségi Kereskedelmi Bizottság nemrég megerősítette arra vonatkozó nyilatkozatait és vállalását, hogy kiemelten kezeli az adatvédelmi önszabályozó vállalatoktól és uniós tagállamoktól érkező bármely olyan ügy felülvizsgálatát, amely arra vonatkozó állítást tartalmaz, hogy egy adott vállalat nem teljesíti a védett adatkikötővel kapcsolatos alapelveket.³⁵ A Szövetségi Kereskedelmi Bizottság az elmúlt három évben csak néhány utalást kapott az európai adatvédelmi hatóságoktól.

Az utóbbi hónapokban fejlődésnek indult az adatvédelmi hatóságok közötti transzatlanti együttműködés. Például a Szövetségi Kereskedelmi Bizottság és az ír adatvédelmi biztos hivatala 2013. június 26-án egyetértési megállapodást írt alá a személyes adatok védelmét biztosító jogszabályok magánszektorbeli végrehajtásához történő kölcsönös segítségnyújtásról. A megállapodás létrehozta a megerősített, korszerűsített és hatékonyabb adatvédelmi végrehajtási együttműködés keretét³⁶.

A Szövetségi Kereskedelmi Bizottság 2013 augusztusában közölte, hogy tovább erősíti azoknak a vállalatoknak az ellenőrzését, amelyek személyes adatokat tartalmazó nagyméretű adatbázisokat kezelnek. Emellett létrehozott egy internetes portált, ahol a fogyasztók benyújthatják az amerikai vállalatokkal kapcsolatos adatvédelmi panaszaikat³⁷.

A Szövetségi Kereskedelmi Bizottságnak fokoznia kell továbbá a védett adatkikötőhöz való csatlakozásra vonatkozó hamis állítások felderítésére irányuló erőfeszítéseit. Ha egy vállalat a honlapján azt állítja, hogy megfelel a védett adatkikötő követelményeinek, a Kereskedelmi Minisztérium jegyzékében azonban nem szerepel a program „aktív” résztvevői között, akkor félrevezeti a fogyasztókat és visszaél azok bizalmával. A hamis állítások gyengítik a rendszer egészének hitelességét, ezért azokat haladéktalanul törölni kell a vállalatok weboldaláról. A vállalatoknak eleget kell tenniük annak a végrehajtási követelménynek, hogy nem vezetnek félre a fogyasztókat. A Szövetségi Kereskedelmi Bizottságnak továbbra is törekednie kell a védett adatkikötőre vonatkozó olyan hamis állítások azonosítására, mint amely a *Karnani* ügyben került felszínre, ahol a Szövetségi Kereskedelmi Bizottság töröltetett egy kaliforniai honlapot, amelyen a védett adatkikötőben való hamis regisztrációt tüntetettek fel, és az európai fogyasztókkal szembeni, csalárd elektronikus kereskedelmi gyakorlatot folytattak³⁸.

A Szövetségi Kereskedelmi Bizottság 2013. október 29-én azt közölte, hogy „az utóbbi hónapokban számos vizsgálatot” indított „a védett adatkikötő szabályainak teljesítése tekintetében”, és „az elkövetkező hónapokban” további jogérvényesítési intézkedések várhatók ezen a téren. A Szövetségi Kereskedelmi Bizottság azt is megerősítette, hogy „arra törekszik, hogy megtalálja a módját hatékonysága javításának”, és „továbbra is örömmel fogad majd bármely fontos információt, mint például egy fogyasztókat képviselő európai ügyvédől a múlt hónapban érkezett panaszt, amely a védett adatkikötővel kapcsolatos nagyszámú jogsértésre vonatkozó állítást fogalmaz meg”.³⁹ Az ügynökség azt is vállalta, hogy „saját végzéseinkhez hasonlóan rendszeresen figyelemmel kísérjük a védett adatkikötőre vonatkozó végzéseket”.⁴⁰

³⁵ Ezt a vállalatot Julie Brill, a Szövetségi Kereskedelmi Bizottság biztosa, valamint az európai adatvédelmi hatóságok (a 29. cikk szerinti munkacsoport) 2013. április 17-i, brüsszeli megbeszélésén megerősítették.

³⁶ <http://www.dataprotection.ie/viewdoc.aspx?Docid=1317&Catid=66&StartDate=1+January+2013&m=n>

³⁷ A fogyasztók a Szövetségi Kereskedelmi Bizottság panaszkezelő oldalán (<https://www.ftccomplaintassistant.gov/>), a nemzetközi fogyasztók pedig az econsumer.gov (<http://www.econsumer.gov>) weboldalon nyújthatják be panaszaikat.

³⁸ <http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf>

³⁹ <http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf> és

<http://www.ftc.gov/speeches/ramirez/131029tadcremarks.pdf>

⁴⁰ Edith Ramireznek, a Szövetségi Kereskedelmi Bizottság elnökének Viviane Reding alelnökéhez intézett levele.

A Szövetségi Kereskedelmi Bizottság 2013. november 12-én arról tájékoztatta az Európai Bizottságot, hogy **„amennyiben egy vállalat adatvédelmi politikája a védett adatkikötő védelmi szintjének biztosítását ígéri, önmagában az a tény, hogy az említett vállalat nem regisztrált vagy nem tartja fenn a regisztrációját, valószínűleg nem mentesíti a vállalatot a Szövetségi Kereskedelmi Bizottságnak a védett adatkikötőre vonatkozó érintett kötelezettségvállalások teljesítésének kikényszerítésére irányuló intézkedése alól”**⁴¹.

A Kereskedelmi Minisztérium 2013 novemberében arról tájékoztatta az Európai Bizottságot, hogy „annak elősegítése érdekében, hogy a vállalatok ne fogalmazzanak meg »hamis állításokat« a védett adatkikötőben való részvétel tekintetében, a Kereskedelmi Minisztérium egy hónappal az ismételt tanúsítás dátuma előtt felveszi a kapcsolatot a védett adatkikötő résztvevőivel, hogy ismertesse, milyen lépéseket kell tenniük abban az esetben, ha úgy döntenek, hogy nem nyújtanak be ismételt tanúsítványt.” A **Kereskedelmi Minisztérium „figyelmeztetni fogja az e kategóriába tartozó vállalatokat, hogy töröljék a védett adatkikötőben való részvételre vonatkozó valamennyi utalást – többek között kerüljék a Kereskedelmi Minisztérium védett adatkikötőre vonatkozó tanúsítási jelének használatát – az adott vállalat adatvédelmi politikájából és weboldaláról, továbbá egyértelműen értesíti őket arról, hogy a fentiek elmulasztása esetén a Szövetségi Kereskedelmi Bizottság jogérvényesítési intézkedéseket foganatosíthat velük szemben”**⁴².

A védett adatkikötőhöz való csatlakozásra vonatkozó hamis állítások leküzdése érdekében az öntanúsító vállalatok adatvédelmi politikájának minden esetben tartalmaznia kell egy hivatkozást a Kereskedelmi Minisztérium védett adatkikötőre vonatkozó weboldalára, ahol a program összes „aktív” tagjának jegyzéke megtalálható. Ez lehetővé teszi az európai adatalanyok számára, hogy – további internetes keresés nélkül – azonnal ellenőrizzék, hogy a vállalat aktív tagja-e a védett adatkikötőnek. A Kereskedelmi Minisztérium 2013 márciusától igényli ezt a vállalatoktól, de a folyamatot fel kell gyorsítani.

A program megfelelő és hatékony működése szempontjából továbbra is kiemelten fontos, hogy – a Kereskedelmi Minisztérium fentiekben kiemelt intézkedései mellett – a Szövetségi Kereskedelmi Bizottság is folyamatosan figyelemmel kísérje és következetesen kikényszerítse a védett adatkikötőre vonatkozó alapelvek tényleges teljesítését. Különösen szükséges, hogy fokozzák a **hivatalból indított ellenőrzéseket és vizsgálatokat** a védett adatkikötőre vonatkozó alapelvek **vállalatok általi teljesítése** tekintetében. Emellett tovább kell könnyíteni a Szövetségi Kereskedelmi Bizottsághoz intézett, jogsértésekkel kapcsolatos panaszok feltételeit.

5.2. Az európai adatvédelmi bizottság

Az európai adatvédelmi bizottság a védett adatkikötőről szóló határozat alapján létrehozott szerv. Hatáskörrel rendelkezik az egyének által benyújtott, munkaviszonnyal összefüggésben gyűjtött személyes adatokkal kapcsolatos panaszok, valamint az olyan esetek kivizsgálására, amikor a tanúsítással rendelkező vállalatok választották ezt a vitarendezési lehetőséget a védett adatkikötő keretében (az összes vállalat 53%-a). A bizottság a különböző európai adatvédelmi hatóságok képviselőiből áll.

Mostanáig négy panasz érkezett a bizottsághoz (kettő 2010-ben, kettő pedig 2013-ban). A testület a két, 2010. évi panaszt nemzeti adatvédelmi hatóságok (Egyesült Királyság és Svájc) elé utalta. A harmadik és a negyedik panasz vizsgálata jelenleg van folyamatban. A panaszok alacsony számát az magyarázhatja, hogy a bizottság hatásköre – amint már említettünk – elsősorban bizonyos adattípusokra korlátozódik.

⁴¹ Edith Ramireznek, a Szövetségi Kereskedelmi Bizottság elnökének Viviane Reding alelnökhöz intézett levele.

⁴² A védett adatkikötő keretének végrehajtására irányuló USA-EU együttműködés, 2013. november 12.

A bizottság korlátozott ítélkezési gyakorlatát részben az is magyarázhatja, hogy kevesen tudnak a bizottság létezéséről. A Bizottság 2004 óta láthatóbbá tette weboldalán a bizottsággal kapcsolatos információkat⁴³.

A bizottság megfelelőbb igénybevétele érdekében azoknak az amerikai vállalatoknak, amelyek azt választják, hogy együttműködnek a testülettel, és a vonatkozó öntanúsításaikban szereplő személyesadat-kategóriák némelyike vagy mindegyike esetében eleget tesznek a bizottság határozatainak, egyértelműen és jól láthatóan meg kell jeleníteniük ezt az adatvédelmi politikájukban vállalt kötelezettségek között, hogy a Kereskedelmi Minisztériumnak lehetősége legyen annak ellenőrzésére. Minden európai uniós adatvédelmi hatóság weboldalán létre kell hozni egy védett adatkikötővel foglalkozó oldalt az európai vállalatok és adatalanyok védett adatkikötővel kapcsolatos ismereteinek bővítése érdekében.

5.3. A végrehajtás javítása

Az átláthatósággal és a végrehajtással kapcsolatos, fent körvonalazott hiányosságok olyan aggodalmakat keltenek az európai vállalatok körében, hogy a védett adatkikötő program kedvezőtlenül hat az európai vállalatok versenyképességére. Amennyiben egy európai vállalat egy olyan amerikai vállalattal versenyez, amely a védett adatkikötő alapján működik, de a gyakorlatban nem alkalmazza annak alapelveit, akkor a szóban forgó európai vállalat versenyhátrányba kerül az amerikaihoz képest.

Továbbá a Szövetségi Kereskedelmi Bizottság hatásköre kiterjed a tisztességtelen vagy csalárd „kereskedelmi, illetve a kereskedelmet érintő” cselekményekre vagy gyakorlatokra. A Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza – többek között a **távközlés** tekintetében – kivételeket állapít meg a Szövetségi Kereskedelmi Bizottság tisztességtelen vagy csalárd cselekményekre vagy gyakorlatokra vonatkozó jogköre alól. A távközlési vállalatok – amelyek nem tartoznak a Szövetségi Kereskedelmi Bizottság jogérvényesítési hatáskörébe – nem csatlakozhatnak a védett adatkikötőhöz. Mivel azonban a technológiai és szolgáltatási ágazat egyre közelebb kerül egymáshoz, az amerikai IKT-szektorban működő sok közvetlen versenytársuk tagja a védett adatkikötőnek. Egyes európai távközlési szolgáltatókat nyugtalanítja, hogy a távközlési cégeket kizárták a védett adatkikötő program alapján zajló adatcseréből. Az Európai Távközlési Hálózatüzemeltetők Egyesülete (ETNO) szerint „ez egyértelműen ellentétes a távközlési szolgáltatók legfontosabb igényével, amely az egyenlő versenyfeltételek megteremtésére vonatkozik”⁴⁴.

⁴³ A 2004. évi jelentés alapján az uniós adatvédelmi bizottságra vonatkozó, kérdések és válaszok formájában megfogalmazott tájékoztatót tettek közzé a Bizottság (Jogérvényesítési Főigazgatóság) weboldalán azzal a céllal, hogy bővítsék a magánszemélyek ismereteit, és segítsék őket a panasz benyújtásában, amennyiben úgy vélik, hogy a védett adatkikötő megsértésével dolgozták fel a személyes adataikat: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf

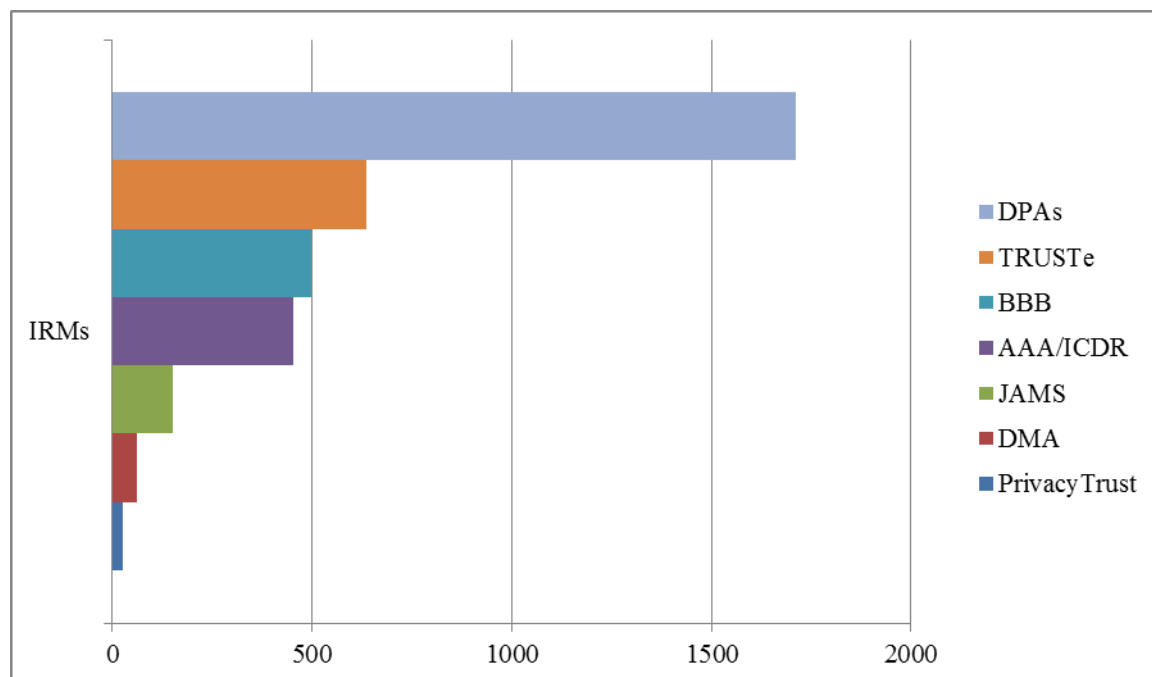
A panasztételi űrlap az alábbi internetcímen érhető el: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf

⁴⁴ A Bizottság szolgálataihoz 2013. október 4-én érkezett „ETNO-megfontolások” emellett az alábbiakat tárgyalják: 1) a személyes adat védett adatkikötőn belüli meghatározása, 2) a védett adatkikötő nyomon követésének hiánya, 3) valamint az, hogy „az amerikai vállalatok európai versenytársaiknál sokkal kevesebb korlátozással továbbíthatnak adatokat”, ami „az európai vállalatokkal szembeni, egyértelmű hátrányos megkülönböztetésnek minősül, és kihat az európai vállalatok versenyképességére”. A védett adatkikötő szabályai szerint az adatok harmadik féllel való közlése érdekében az adott szervezeteknek alkalmazniuk kell az értesítés és a választási lehetőség elvét. Amennyiben a szervezet az információt olyan harmadik félnek kívánja továbbítani, amely közvetítőként jár el, ezt úgy teheti meg, ha először vagy megállapítja, hogy a harmadik fél elfogadja az elveket, vagy az irányelv, illetve más megfelelőségi megállapítás hatálya alá tartozik, vagy ha írásos megállapodást köt az ilyen harmadik féllel arra nézve, hogy a harmadik fél legalább ugyanolyan szintű adatvédelmet biztosít, mint amit a vonatkozó elvek megkövetelnek.

6. A VÉDETT ADATKIKÖTŐRE VONATKOZÓ ADATVÉDELMI ALAPELVEK ERŐSÍTÉSE

6.1. Alternatív vitarendezési eljárások

A végrehajtási elv előírja, hogy „könnyen hozzáférhető és megfizethető független eljárási mechanizmusokat” kell kialakítani, „amelyekkel minden egyes személy panaszait és vitáit meg lehet vizsgálni”. Ezért a védett adatkikötő program létrehozta az alternatív vitarendezés rendszerét, amely független harmadik személy közreműködésével⁴⁵ gyors megoldásokat biztosít az egyének számára. Az eljárási mechanizmusokat biztosító három legfontosabb szerv az európai adatvédelmi bizottság, a BBB (Üzletmenet-fejlesztési Hivatal), és a TRUSTe.



Az alternatív vitarendezési eljárások igénybevétele 2004 óta növekszik, a Kereskedelmi Minisztérium pedig megerősítette az amerikai alternatív vitarendezési szolgáltatók figyelemmel kísérését annak érdekében, hogy világos, hozzáférhető és érthető tájékoztatást nyújtsanak a panaszeljárással kapcsolatban. Mostanáig azonban még nem bizonyosodott be ennek a rendszernek a hatékonysága, mivel az említett szervek eddig nagyon kevés ügyben jártak el⁴⁶.

Jóllehet a Kereskedelmi Minisztérium sikeresen csökkentette az alternatív vitarendezési szolgáltatók által felszámított díjakat, a hét nagy szolgáltató közül kettő továbbra is díjat számít fel az egyéneknek a panaszok benyújtásáért⁴⁷. Ez a védett adatkikötőben résztvevő

⁴⁵ A fogyasztói jogviták alternatív rendezéséről szóló 2013/11/EU uniós irányelv hangsúlyozza a független, pártatlan, átlátható, hatékony, gyors és méltányos alternatív vitarendezési eljárások fontosságát.

⁴⁶ Például az egyik nagy szolgáltató („TRUSTe”) arról számolt be, hogy 2010-ben 881 kérelem érkezett hozzá, de ezek közül csupán három volt elfogadhatónak és megalapozottnak tekinthető, amely alapján az érintett vállalat köteles volt megváltoztatni adatvédelmi politikáját és weboldalát. 2011-ben 879 volt a panaszok száma, és egy ügyben a vállalat köteles volt megváltoztatni adatvédelmi politikáját. A Kereskedelmi Minisztérium szerint az alternatív vitarendezési eljárásban feldolgozott panaszok túlnyomó többsége olyan fogyasztóktól – például felhasználóktól – érkező kérés, akik elfejtették a jelszavukat, és nem tudták azt az internetes szolgáltatás útján megszerezni. A Bizottság kérését követően a Kereskedelmi Minisztérium új statisztikai beszámolósi kritériumokat dolgozott ki, amelyeket valamennyi alternatív vitarendezési szolgáltatónak használnia kell. E kritériumok megkülönböztetik egymástól a puszta kéréseket és a panaszokat, valamint tovább pontosítják a beérkezett panaszok típusait. Az említett új kritériumokat azonban alaposabban is meg kell vitatni annak biztosítása érdekében, hogy az új, 2014-es statisztikai adatok valamennyi alternatív vitarendezési szolgáltatóra vonatkozzanak, összehasonlíthatók legyenek, valamint biztosítsák az eljárási mechanizmusok hatékonyságának értékeléséhez szükséges, alapvető információkat.

⁴⁷ Az International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA), 200 USD, a JAMS pedig 250 USD „benyújtási díjat” számít fel. A Kereskedelmi Minisztérium arról tájékoztatta a Bizottságot, hogy az egyének számára

vállalatok mintegy 20 %-a által igénybe vett szolgáltatóknak felel meg. Az említett vállalatok olyan szolgáltatót választottak, amely panasz-benyújtási díjat számít fel a fogyasztóknak. Az ilyen gyakorlat nem felel meg a védett adatkikötő végrehajtási alapelvének, amely biztosítja, hogy az egyének jogosultak igénybe venni „könnyen hozzáférhető és megfizethető független eljárási mechanizmusokat”. Az Európai Unión belül az európai adatvédelmi bizottság által biztosított független vitarendezési mechanizmus valamennyi adatalany számára díjmentesen igénybe vehető.

A Kereskedelmi Minisztérium 2013. november 12-én megerősítette, hogy „továbbá is fellép az uniós polgárok adatainak védelmében és együttműködik az alternatív vitarendezési szolgáltatókkal annak megállapítása érdekében, hogy a díjaik tovább csökkenthetők-e”.

Ami a szankciókat illeti, nem minden alternatív vitarendezési szolgáltató rendelkezik az adatvédelmi alapelvek megsértése miatt előállt helyzet orvoslásához szükséges eszközökkel. Ezenfelül a meg nem felelésre vonatkozó megállapítások közzététele a jelek szerint nem szerepel az alternatív vitarendezési szolgáltatók által kiszabható szankciók és intézkedések eszköztárában.

A szolgáltatók továbbá kötelesek a Szövetségi Kereskedelmi Bizottság elé utalni az ügyet, amennyiben egy vállalat nem felel meg az alternatív vitarendezési eljárás eredményének, vagy elutasítja a szolgáltató határozatát. Így a Szövetségi Kereskedelmi Bizottság felülvizsgálatot és vizsgálatot végezhet, és adott esetben jogérvényesítési intézkedéseket hozhat. Mostanáig azonban a szolgáltatók egy ügyet sem utaltak a határozat nem teljesítése miatt a Szövetségi Kereskedelmi Bizottság elé⁴⁸.

Az alternatív vitarendezési szolgáltatók a honlapjaikon listát vezetnek azokról a vállalatokról (a vitarendezés résztvevői), akik igénybe vették a szolgáltatásaikat. Ez lehetővé teszi, hogy a fogyasztók könnyen ellenőrizzék – egy vállalattal való jogvita esetén – hogy egyének nyújthatnak-e be panaszt egy meghatározott vitarendezési szolgáltatóhoz. Tehát például a BBB vitarendezési szolgáltató felsorolja a BBB vitarendezési rendszerében részt vevő összes vállalatot. Ugyanakkor sok olyan vállalat van, amely azt állítja magáról, hogy részt vesz egy meghatározott vitarendezési rendszerben, de a szolgáltatók nem sorolják fel őket vitarendezési programjuk résztvevői között⁴⁹.

Az alternatív vitarendezési mechanizmusoknak könnyen hozzáférhetőnek, függetlennek és az egyének számára megfizethetőnek kell lenniük. Az érintettnek túlzott megkötések nélkül képesnek kell lennie arra, hogy panaszt nyújtson be. Valamennyi alternatív vitarendezési testületnek közzé kell tennie weboldalán a kezelt panaszokra vonatkozó statisztikai adatokat, valamint az azok eredményével kapcsolatos konkrét információkat. Végezetül pedig továbbra is figyelemmel kell kísérni az alternatív vitarendezési szervek működését annak biztosítása érdekében, hogy világos és érthető tájékoztatást adjanak az eljárásról és a panasz benyújtásának módjáról, és így a vitarendezés eredményes, hatékony és megbízható mechanizmussá váljon. Ismételten nyomatékosítani kell továbbá, hogy a meg nem felelésre vonatkozó megállapítások közzétételét fel kell venni az alternatív vitarendezési szolgáltatók kötelező szankcióinak katalógusába.

legköltségesebb vitarendezési szolgáltatóval – az AAA-val – együttműködve kifejezetten a védett adatkikötőre vonatkozó programot dolgozott ki, amely több ezer dollárról 200 dolláros átalánydíjra csökkentette a fogyasztók költségét.

⁴⁸ Lásd 11. GYFK.

⁴⁹ Például: Az Amazon arról tájékoztatta a Kereskedelmi Minisztériumot, hogy a BBB-t alkalmazza vitarendezési szolgáltatójaként, azonban a BBB nem sorolja fel az Amazont vitarendezési résztvevői között. Fordított esetben az Arsalon Technologies (www.arsalon.net) nevű számítási felhő tárhely-szolgáltató szerepel a BBB védett adatkikötőre vonatkozó vitarendezési jegyzékén, de a vállalat nincs a védett adatkikötő aktív tagjai között (a 2013. október 1-jei helyzet szerint). A BBB-nek, a TRUSTe-nek és a többi alternatív vitarendezési szolgáltatónak törölniük vagy helyesbíteniük kell a tanúsításra vonatkozó állításait. Eleget kell tenniük annak a kikényszeríthető követelménynek, hogy kizárólag olyan vállalatokra vonatkozóan adhatnak ki tanúsítványokat, amelyek részt vesznek a védett adatkikötőben.

6.2. Adattovábbítás harmadik fél részére

Az adatáramlások exponenciális növekedése szükségessé teszi a személyes adatok folyamatos védelmének biztosítását a feldolgozás összes szakaszában, különösen amikor a védett adatkikötőhöz csatlakozó vállalat továbbítja az adatokat egy **harmadik adatfeldolgozó fél** számára. Ezért a védett adatkikötővel kapcsolatos aggályokat nem csupán a védett adatkikötő résztvevőivel, hanem az alvállalkozókkal szemben is hatékonyabban kell érvényesíteni.

A védett adatkikötőre vonatkozó program lehetővé teszi a megbízottként eljáró harmadik fél számára való adattovábbítást, ha a védett adatkikötőre vonatkozó programban részt vevő vállalat „meggyőződik arról, hogy a harmadik fél elfogadja az elveket, vagy az irányelv, illetve más megfelelőségi megállapítás hatálya alá tartozik, vagy ha írásos megállapodást köt az ilyen harmadik féllel arra nézve, hogy a harmadik fél legalább ugyanolyan szintű adatvédelmet biztosít, mint amit a vonatkozó elvek megkövetelnek”⁵⁰. Például a Kereskedelmi Minisztérium még abban az esetben is szerződéskötésre kötelezi a számításifelhő-szolgáltatót, ha megfelel a „védett adatkikötőnek” és megkapja a feldolgozandó személyes adatokat⁵¹. A védett adatkikötőről szóló határozat II. mellékletében azonban nem egyértelmű ez a rendelkezés.

Mivel az elmúlt évek során – különösen a számítási felhővel összefüggésben – jelentős mértékben növekedett az alvállalkozók igénybevétele, indokolt lenne, hogy a védett adatkikötőben részt vevő vállalatoknak az ilyen szerződések megkötésekor értesíteniük kelljen a Kereskedelmi Minisztériumot, és kötelesek legyenek nyilvánosságra hozni az adatvédelmi biztosítékokat⁵².

A három fenti kérdés – az alternatív vitarendezési mechanizmusok, a megerősített felügyelet és a harmadik félnek történő adattovábbítás – további pontosítást igényel.

7. A VÉDETT ADATKIKÖTŐRE VONATKOZÓ PROGRAM KERETÉBEN TOVÁBBÍTOTT ADATOKHOZ VALÓ HOZZÁFÉRÉS

2013 folyamán az Egyesült Államok hírszerzési programjainak nagyságrendjére és terjedelmére vonatkozó értesülések aggodalmat keltettek a védett adatkikötőre vonatkozó program keretében az Egyesült Államokba törvényesen továbbított személyes adatok védelmének folyamatossága tekintetében. Például a jelek szerint a PRISM programban résztvevő és az amerikai hatóságok számára az Egyesült Államokban tárolt és feldolgozott valamennyi adathoz hozzáférést biztosító valamennyi vállalat rendelkezik védett adatkikötőre vonatkozó tanúsítvánnyal. Ennek alapján a védett adatkikötőre vonatkozó program az egyik olyan csatorna, amelyen keresztül az amerikai hírszerzési hatóságok hozzájuthatnak az eredetileg az Unióban feldolgozott személyes adatokhoz.

A védett adatkikötőről szóló határozat I. melléklete úgy rendelkezik, hogy az adatvédelmi elvek elfogadása korlátozható, ha a nemzetbiztonság, a közérdek vagy a bűnüldözés

⁵⁰ Lásd a 2000/520/EK bizottsági határozat 7. oldalát (adattovábbítás harmadik fél részére).

⁵¹ Lásd: „Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing” (Az USA-EU védett adatkikötőre vonatkozó keretével és a számítási felhővel kapcsolatos pontosítások): http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_ma_in_060351.pdf

⁵² E megjegyzések azokra a számításifelhő-szolgáltatókra vonatkoznak, amelyek nem vesznek részt a védett adatkikötőben. A Galexia tanácsadó cég szerint „a számításifelhő-szolgáltatók között rendkívül magas a védett adatkikötőben tagsággal rendelkezők (és annak megfelelők) aránya. A számításifelhő-szolgáltatók általában többretegű adatvédelemmel rendelkeznek, amely ügyfelekkel kötött közvetlen szerződések és átfogó adatvédelmi politikák kombinációjából áll. A védett adatkikötőben résztvevő számításifelhő-szolgáltatók – egy-két fontos kivételtől eltekintve – eleget tesznek a vitarendezésre és a végrehajtásra vonatkozó legfontosabb előírásoknak. A hamis tagsági nyilatkozatot tevő vállalatok listáján jelenleg egyetlen nagy számításifelhő-szolgáltató sem szerepel.” (Chris Connolly, a Galexia munkatársa nyilatkozata az Állampolgári Jogi, Bel- és Igazságügyi Bizottság előtt „Az uniós polgárok tömeges elektronikus megfigyelésére” vonatkozó vizsgálat keretében).

követelményei, vagy törvény, kormányrendelet illetve az ítélkezési gyakorlat ezt indokolja. Az alapvető jogok gyakorlásának korlátozásai akkor lehetnek jogszerűek, ha szűken értelmezik azokat; a korlátozásokat nyilvánosan hozzáférhető jogszabályban kell meghatározni, és azoknak szükségeseknek és arányosoknak kell lenniük egy demokratikus társadalomban. Először is, a védett adatkikötőről szóló határozat kimondja, hogy a korlátozások csak a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez „szükséges mértékben” lehetségesek⁵³. Jóllehet a védett adatkikötőre vonatkozó program alapján kivételesen lehetőség van a nemzetbiztonság, a közérdek vagy a bűnüldözés céljából történő adatfeldolgozásra, a védett adatkikötő elfogadásának idején nem láthatták előre, hogy a hírszerzési ügynökségek ilyen nagymértékben hozzáférnek a kereskedelmi ügyeltekkel összefüggésben az Egyesült Államokba továbbított adatokhoz.

Továbbá a Kereskedelmi Minisztériumnak – az átláthatósággal és a jogbiztonsággal összefüggő okokból – értesítenie kell az Európai Bizottságot azokról a törvényekről és kormányrendeletekről, amelyek kihathatnak a védett adatkikötőre vonatkozó adatvédelmi alapelvek elfogadására⁵⁴. Gondosan figyelemmel kell kísérni a kivételek alkalmazását, és ezek nem alkalmazhatók olyan módon, amely aláássa az **Alapelvek** által biztosított védelmet⁵⁵. Különösen az veszélyezteti az elektronikus kommunikáció titkosságát, hogy az amerikai hatóságok széles körben hozzáférnek a védett adatkikötőhöz csatlakozott öntanúsító vállalatok által feldolgozott adatokhoz.

7.1. Arányosság és szükségesség

Az EU–USA ad hoc adatvédelmi munkacsoport megállapításai szerint az amerikai jog számos jogalapot biztosít az amerikai székhelyű vállalatok által tárolt vagy más módon feldolgozott személyes adatok széles körű gyűjtésére és feldolgozására. Ez felöllelheti a védett adatkikötőre vonatkozó program keretében az Unióból korábban az Egyesült Államokba továbbított adatokat is, ami felveti a kérdést, hogy továbbra is teljesítik-e a védett adatkikötőre vonatkozó elveket. E programok nagy mérete miatt előfordulhat, hogy az amerikai hatóságok nagyobb mértékben férnek hozzá a védett adatkikötő keretében továbbított adatokhoz és nagyobb mértékben dolgozzák fel azokat, mint ami a védett adatkikötőről szóló határozatban biztosított kivételnek megfelelően feltétlenül szükséges és arányos volna a nemzetbiztonság védelme céljából.

7.2. Korlátozások és jogorvoslati lehetőségek

Az EU–USA ad hoc adatvédelmi munkacsoport megállapításai szerint az amerikai jog szerint nyújtott biztosítékokat főként az amerikai polgárok és honos személyek vehetik igénybe. Továbbá sem az uniós, sem az amerikai érintetteknek nincs lehetőségük betekinteni az

⁵³ Lásd a védett adatkikötőről szóló határozat I. mellékletét: „Az elvek elfogadása korlátozódhat: a) a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben; b) törvény, kormányrendelet vagy precedensjog által, amelyek az elvekkel ellentétes kötelezettségeket vagy kifejezett felhatalmazásokat hoznak létre, feltéve hogy bármilyen ilyen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nem teljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik; vagy c) ha a tagállami jogszabályokra vonatkozó irányelv 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 politikájukban 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 a magasabb szintű védelem választását, ahol lehetséges.”

⁵⁴ A 29. cikk szerinti adatvédelmi munkacsoport 2000. május 16-án elfogadott 4/2000. véleménye a „védett adatkikötőre vonatkozó alapelvek” által biztosított védelmi szintről.

⁵⁵ A 29. cikk szerinti adatvédelmi munkacsoport 2000. május 16-án elfogadott 4/2000. véleménye a „védett adatkikötőre vonatkozó alapelvek” által biztosított védelmi szintről.

adatokba, azok helyesbítését, illetve törlését kérni, vagy közigazgatási, illetve bírósági jogorvoslással élni személyes adataiknak az amerikai hírszerzési programok keretében zajló gyűjtése és további feldolgozása tekintetében.

7.3. Átláthatóság

A vállalatok nem rendszeresen jelölik meg adatvédelmi politikájukban, hogy mikor alkalmazzák az alapelvek alóli kivételeket. Így az egyének és a vállalatok nincsenek tisztában azzal, hogy mi történik az adataikkal. Különösen igaz ez a szóban forgó amerikai hírszerzési programok működése tekintetében. Ennek következtében azok az európaiak, akiknek az adatait a védett adatkikötő alapján az Egyesült Államokba továbbították egy vállalathoz, az érintett vállalatoktól adott esetben nem kapnak értesítést arról, hogy valaki esetleg hozzáfér az adataikhoz⁵⁶. Ez megkérdőjelezi a védett adatkikötő átláthatóságra vonatkozó alapelveinek teljesülését. A lehető legnagyobb mértékű átláthatóságot kell biztosítani a nemzetbiztonság veszélyeztetése nélkül. A vállalatokra vonatkozó azon meglévő követelményen túlmenően, hogy adatvédelmi politikájukban jelezniük kell, hogy a törvény, kormányrendelet vagy ítélkezési gyakorlat alapján milyen esetben kerülhet sor az alapelvek korlátozására, arra is ösztönözni kell a vállalatokat, hogy tüntessék fel adatvédelmi politikájukban, hogy milyen esetekben alkalmazzák az alapelvek alóli kivételeket a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítése céljából.

8. KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

2000. évi elfogadása óta a védett adatkikötő az EU és az USA közötti személyesadat-áramlás csatornájává vált. A digitális gazdaságban központi szerepet játszó adatáramlások exponenciális növekedése, valamint az adatgyűjtés, -feldolgozás és -felhasználás igen jelentős fejlődése miatt megnőtt a hatékony védelem fontossága személyes adatok továbbítása esetén. Az olyan internetes cégek, mint a Google, a Facebook, a Microsoft, az Apple és a Yahoo több száz millió ügyféllel rendelkeznek Európában, és a védett adatkikötő 2000. évi létrehozásakor még elképzelhetetlen mennyiségben továbbítanak személyes adatokat az Egyesült Államokban történő feldolgozás céljából.

A szabályozás átláthatóságának és végrehajtásának hiányosságai miatt továbbra is fennállnak és orvoslásra szorulnak az alábbi problémák:

- a) a védett adatkikötő tagjai adatvédelmi politikáinak átláthatósága,
- b) az adatvédelmi alapelvek amerikai vállalatok általi hatékony alkalmazása, valamint
- c) a végrehajtás hatékonysága.

Ezenfelül az, hogy **a hírszerző szervek széles körben hozzáférnek a védett adatkikötőre vonatkozó tanúsítvánnyal rendelkező vállalatok által az Egyesült Államokba továbbított adatokhoz**, további súlyos kérdéseket vet fel azzal kapcsolatban, hogy az európaiakat továbbra is megilletik-e az adatvédelmi jogok azt követően, hogy adataikat az USA-ba továbbították.

A fentiek alapján a Bizottság a következő **ajánlásokat** fogalmazta meg:

Átláthatóság

⁵⁶

A védett adatkikötőben résztvevő egyes európai vállalatok viszonylag átlátható információkat közölnek ezzel kapcsolatban. Például a Nokia – amely az Egyesült Államokban is tevékenykedik és a védett adatkikötő tagja – a következő tájékoztatást adja adatvédelmi politikájában: „Előfordulhat, hogy törvényi kötelezettség alapján kötelesek vagyunk közölni személyes adatait bizonyos hatóságokkal vagy más harmadik felekkel, például azoknak az országoknak a bűnüldöző szerveivel, ahol mi vagy a nevünkben eljáró harmadik felek működnek.”

- 1) *Az öntanúsító vállalatoknak nyilvánosságra kellene hozniuk adatvédelmi politikájukat.* Nem elegendő, hogy a vállalatok közlik a Kereskedelmi Minisztériummal adatvédelmi politikájuk leírását. Az adatvédelmi politikákat – világos és érthető megfogalmazásban – nyilvánosan hozzáférhetővé kellene tenni a vállalatok weboldalán.
- 2) Az öntanúsító vállalatok weboldalán közzétett adatvédelmi politikának minden esetben tartalmaznia kellene egy hivatkozást a Kereskedelmi Minisztérium védett adatkikötőre vonatkozó weboldalára, amely felsorolja a program összes „aktív” tagját. Ez lehetővé teszi az európai adatalanyok számára, hogy – további internetes keresés nélkül – azonnal ellenőrizzék, hogy a vállalat aktív tagja-e a védett adatkikötőnek. Ez hozzájárulna a program hitelességének erősödéséhez azáltal, hogy csökkentené a védett adatkikötőhöz való csatlakozásra vonatkozó hamis állítások lehetőségét. A Kereskedelmi Minisztérium 2013 márciusától igényli ezt a vállalatoktól, de a folyamatot fel kellene gyorsítani.
- 3) Az öntanúsító vállalatoknak közzé kellene tenniük az alvállalkozókkal – például számításifelhő-szolgáltatókkal – kötött szerződéseikben szereplő adatvédelmi feltételeket. A védett adatkikötő lehetővé teszi, hogy a védett adatkikötőre vonatkozó tanúsítvánnyal rendelkező vállalatok adatokat továbbítsanak megbízottként eljáró harmadik személyek – például számításifelhő-szolgáltatók – számára. Értelmezésünk szerint ilyen esetekben a Kereskedelmi Minisztérium szerződéskötésre kötelezi az öntanúsító vállalatokat. Ilyen szerződés megkötésekor azonban a védett adatkikötőben résztvevő vállalatot kötelezni kellene arra, hogy értesítse erről a Kereskedelmi Minisztériumot, és nyilvánosságra hozza az adatvédelmi biztosítékokat.
- 4) A Kereskedelmi Minisztérium weboldalán világosan meg kellene jelölni minden olyan vállalatot, amely nem aktív tagja a programnak. A Kereskedelmi Minisztériumnak a védett adatkikötő tagjait felsoroló jegyzékében szereplő „Nem aktív” megjelöléshez olyan egyértelmű figyelmeztetést kellene csatolni, miszerint a vállalat jelenleg nem tesz eleget a védett adatkikötő követelményeinek. Mindazonáltal a „Nem aktív” állapotú vállalat a védett adatkikötő keretében megkapott adatokra továbbra is köteles alkalmazni annak követelményeit.

Eljárási mechanizmusok

- 5) A vállalatok weboldalán található adatvédelmi politikáknak az alternatív vitarendezési szolgáltatóra és/vagy az európai adatvédelmi bizottságra való hivatkozást kellene tartalmazniuk. Ez lehetővé tenné, hogy az európai adatalanyok probléma esetén azonnal kapcsolatba lépjenek az alternatív vitarendezési szolgáltatóval vagy az európai adatvédelmi bizottsággal. A Kereskedelmi Minisztérium 2013 márciusától igényli ezt a vállalatoktól, de a folyamatot fel kellene gyorsítani.
- 6) Az alternatív vitarendezésnek könnyen hozzáférhetőnek és megfizethetőnek kellene lennie. A védett adatkikötőre vonatkozó programban résztvevő egyes alternatív vitarendezési szervek továbbra is 200-250 USD összegű díjat számítanak fel az egyéneknek a panasz kezelésért, ami igen költséges lehet egy egyedi felhasználónak. Ezzel szemben Európában a védett adatkikötő keretében érkező panaszok orvoslása érdekében létrehozott európai adatvédelmi bizottság térítésmentesen vehető igénybe.
- 7) A Kereskedelmi Minisztériumnak rendszeresebben kellene figyelemmel kísérnie az alternatív vitarendezési szolgáltatókat a tekintetben, hogy átlátható és hozzáférhető

tájékoztatást nyújtanak-e az általuk alkalmazott eljárás és a panaszok esetében biztosított nyomon követés vonatkozásában. Ennek révén a vitarendezés hatékony, megbízható és eredményes mechanizmussá válik. Ismételten nyomatékosítani kell továbbá, hogy a meg nem felelésre vonatkozó megállapítások közzétételét fel kell venni az alternatív vitarendezési szolgáltatók kötelező szankcióinak katalógusába.

Végrehajtás

- 8) Miután a védett adatkikötő keretében sor kerül a vállalatok tanúsítására vagy ismételt tanúsítására, az említett vállalatok bizonyos százaléka esetében hivatalból indított vizsgálatokat kellene végezni adatvédelmi politikáik hatékony teljesülése tekintetében (a formális követelmények teljesítésének ellenőrzésén túlmenően).
- 9) Amennyiben panaszt vagy vizsgálatot követően az elvek megsértését állapítanak meg, a vállalat esetében 1 év elteltével újabb nyomon követési vizsgálatot kellene végezni.
- 10) A Kereskedelmi Minisztériumnak tájékoztatnia kellene az illetékes európai adatvédelmi hatóságot abban az esetben, ha kétség merül fel a vállalat megfelelőségét illetően, vagy panaszok elbírálása van folyamatban.
- 11) A védett adatkikötőhöz való csatlakozásra vonatkozó hamis nyilatkozatokat továbbra is ki kellene vizsgálni. Ha egy vállalat a honlapján azt állítja, hogy megfelel a védett adatkikötő követelményeinek, azonban nem szerepel a program „aktív” résztvevői között a Kereskedelmi Minisztérium jegyzékében, akkor félrevezeti a fogyasztókat és visszaél azok bizalmával. A hamis állítások gyengítik a rendszer egészének hitelességét, ezért azokat haladéktalanul törölni kell a vállalatok weboldaláról.

Az amerikai hatóságok hozzájárulása

- 12) Az öntanúsító vállalatok adatvédelmi politikáinak arra vonatkozó tájékoztatást kellene tartalmazniuk, hogy az amerikai jog milyen mértékben teszi lehetővé a hatóságok számára a védett adatkikötő keretében továbbított adatok gyűjtését és feldolgozását. A vállalatokat elsősorban arra kellene ösztönözni, hogy adatvédelmi politikájukban tüntessék fel, hogy mikor alkalmazzák az alapelvek alóli kivételeket a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítése céljából.
- 13) Fontos, hogy a védett adatkikötőről szóló határozat által előírt nemzetbiztonsági kivételt kizárólag a feltétlenül szükséges és arányos mértékben alkalmazzák.