32000D0520

A BIZOTTSÁG HATÁROZATA
(2000. július 26.)
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

(az értesítés a C(2000) 2441. számú dokumentummal történt)

(EGT vonatkozású szöveg)

(2000/520/EK)

AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA,

tekintettel az Európai Közösséget létrehozó szerződésre,

tekintettel a személyes adatok kezelése 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,

mivel:

(1) A 95/46/EK irányelv 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.

(2) A Bizottság megállapíthatja, hogy egy harmadik ország megfelelő szintű védelmet biztosít. Ilyen esetben a személyes adatok a tagállamokból anélkül továbbíthatók, hogy további garanciákra lenne szükség.

(3) A 95/46/EK irányelv alapján, az adatvédelem szintjét az adattovábbítási művelet vagy az adattovábbítási műveletsorozat összes körülményének és az adott feltételeknek a figyelembevételével kell értékelni. A fenti irányelv alapján a személyes adatok kezelése vonatkozásában az egyének védelmére létrehozott munkacsoport [2] útmutatást adott ki az ilyen értékelések elkészítéséhez [3].

(4) Mivel a harmadik országok az adatvédelem eltérő megközelítéseit alkalmazzák, a megfelelőség értékelését és a 95/46/EK irányelv 25. cikkének (6) bekezdésén alapuló bármilyen határozatot oly módon kell végrehajtani, hogy az ne tegyen önkényes vagy indokolatlan megkülönböztetést olyan harmadik országokkal szemben vagy azok között, ahol hasonló feltételek uralkodnak, illetve ne képezzen leplezett kereskedelmi akadályt, figyelembe véve a Közösség jelenlegi nemzetközi kötelezettségeit.

(5) Az e határozat által elismert, a Közösségből az Egyesült Államokba történő adattovábbításra vonatkozó megfelelő szintű védelem elérhető, ha a szervezetek teljesítik az Egyesült Államok kormánya által 2000. július 21-én kiadott, az egy tagállamból az Egyesült Államokba továbbított személyes adatok védelmére vonatkozó „biztonságos kikötő” adatvédelmi elveket (a továbbiakban: az elvek) és az elvek végrehajtására vonatkozó útmutatást biztosító, gyakran felvetődő kérdéseket (a továbbiakban: GYFK). Ezenfelül a szervezeteknek nyilvánosságra kell hozniuk adatvédelmi politikájukat, és el kell fogadniuk a Szövetségi Kereskedelmi Bizottság (FTC) joghatóságát a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza alapján, amely megtiltja a tisztességtelen vagy megtévesztő cselekményeket vagy gyakorlatokat a kereskedelemben vagy azzal kapcsolatban, vagy más hatósági szerv joghatóságát, amely hatékonyan biztosítja a gyakran felvetődő kérdésekkel összhangban bevezetett elveknek való megfelelést.

(6) A határozat VII. mellékletében felsorolt egyesült államokbeli kormányzati szervek egyikének joghatósága alá sem tartozó ágazatok és/vagy adatfeldolgozás e határozat hatályán kívül esik.

(7) E határozat megfelelő alkalmazásának biztosítása érdekében szükséges, hogy az elveket és GYFK-t elfogadó szervezetek az érdekelt felek – mint például az érintettek, adatátadók és adatvédelmi hatóságok – által elismerhetőek legyenek. E célból az Egyesült Államok Kereskedelmi Minisztériumának vagy az általa kijelölt szervnek vállalnia kell az olyan szervezetek jegyzékének vezetését és a

[1] HL L 281., 1995.11.23., 31. o.

[2] A munkacsoport internet címe: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

[3] WP 12: Személyes adatok továbbítása harmadik országokba: a munkacsoport által 1998. július 24-én elfogadott EU adatvédelmi irányelv 25. és 26. cikkének alkalmazása.

nyilvánosság számára hozzáférhetővé tételét, amelyek saját maguk tanúsítják a GYFK-val összhangban végrehajtott elvek elfogadását, és az e határozat VII. mellékletében felsoroltak közül legalább egy kormányzati szerv joghatósága alá tartoznak.

(8) Az átláthatóság érdekében és a tagállamok illetékes hatóságainak azon képessége megőrzése céljából, hogy a személyes adatok kezelése vonatkozásában biztosítsa az egyének védelmét, ebben a határozatban pontosan meg kell határozni azokat a rendkívüli körülményeket, amelyek esetén indokolt a meghatározott adatáramlás felfüggesztése, függetlenül attól, hogy a védelmet megfelelőnek találják.

(9) Az elvek és GYFK által létrehozott „biztonságos kikötő" felülvizsgálatra szorulhat, figyelembe véve a tapasztalatokat, az adatvédelem fejlődését, olyan körülmények között, amelyekben a technológia egyre könnyebbé teszi a személyes adatok továbbítását és kezelését, valamint figyelembe véve az érintett végrehajtó hatóságok jelentéseit a megvalósításról.

(10) A 95/46/EK irányelv 29. cikke alapján a személyes adatok kezelése tekintetében az egyének védelmére létrehozott munkacsoport véleményeket nyilvánított az egyesült államokbeli „biztonságos kikötő" elvek által biztosított védelem szintjéről, amelyeket e határozat elkészítésekor figyelembe vettek [1].

(11) Az e határozatban foglalt intézkedések összhangban vannak a 95/46/EK irányelv 31. cikke alapján létrehozott bizottság véleményével.

(12) Az 1999/468/EK tanácsi határozat és különösen annak 8. cikke alapján az Európai Parlament 2000. július 5-én elfogadta az Egyesült Államok Kereskedelmi Minisztériuma által kiadott A5–0177/2000 állásfoglalást a „biztonságos kikötő adatvédelmi elvek" által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló bizottsági határozattervezetről [2]. A Bizottság az állásfoglalás figyelembevételével felülvizsgálta a határozattervezetet, és arra a következtetésre jutott, hogy bár az Európai Parlament kifejezte azt a véleményét, hogy a „biztonságos kikötő elvek" és a kapcsolódó gyakran felvetődő kérdések némi fejlesztésre szorulnak, mielőtt úgy lehetne tekinteni, hogy „megfelelő védelmet" biztosítanak, nem állapította meg, hogy a Bizottság túllépte volna hatáskörét a határozat elfogadásával,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

(1) A 95/46/EK irányelv 25. cikke (2) bekezdésének alkalmazásában, az Egyesült Államok Kereskedelmi Minisztériuma által 2000. július 21-én kiadott, e határozat II. mellékletében meghatározott gyakran felvetődő kérdések (a továbbiakban: GYFK) által biztosított útmutatással összhangban bevezetett, e határozat I. mellékletében meghatározott „biztonságos kikötő adatvédelmi elveket" (a továbbiakban: az elvek) az említett irányelv hatálya alá tartozó összes tevékenységre vonatkozóan úgy tekintik, mint amelyek biztosítják a Közösségből az Egyesült Államokban letelepedett szervezetek felé továbbított személyes adatok megfelelő szintű védelmét, tekintettel az Egyesült Államok Kereskedelmi Minisztériuma által kiadott következő okmányokra:

a) a III. mellékletben ismertetett „biztonságos kikötő" végrehajtási áttekintés;

b) a IV. mellékletben bemutatott, az adatvédelem megsértéséért járó kártérítésről és az amerikai jog kifejezett meghatalmazásairól szóló jegyzet;

c) a Szövetségi Kereskedelmi Bizottságnak az V. mellékletben bemutatott levele;

d) az Egyesült Államok Közlekedési Minisztériumának VI. mellékletben bemutatott levele.

(2) Minden egyes adattovábbítás tekintetében a következő feltételeknek kell teljesülniük:

a) az adatokat fogadó szervezet egyértelműen és nyilvánosan kinyilvánította a GYFK-val összhangban bevezetett elvek teljesítésére vonatkozó kötelezettségvállalását; és

b) a szervezet egy olyan, az e határozat VII. mellékletében felsorolt egyesült államokbeli kormányzati szervnek a törvényben meghatározott hatásköre alá tartozik, amelyet a panaszok kivizsgálására és a tisztességtelen vagy megtévesztő gyakorlatok miatti jóvátétel kieszközlésére, valamint magánszemélyek orvoslására feljogosítottak, azok lakóhely szerinti országától vagy állampolgárságától függetlenül, a GYFK-val összhangban bevezetett elvek nem teljesítése esetén.

(3) A (2) bekezdésben megállapított feltételeket minden egyes szervezet esetében teljesítettnek tekintik, amely önmaga tanúsítja a GYFK-val összhangban végrehajtott elvek betartását, attól az időponttól számítva, amikor a szervezet közli az Egyesült Államok Kereskedelmi Minisztériumával (vagy az általa kijelölt szervvel) a (2) bekezdés a) pontjában említett kötelezettségvállalás nyilvános közzétételét és a (2) bekezdés b) pontjában említett kormányzati szerv kilétét.

---

[1] WP 15: 1/99 vélemény az adatvédelem szintjéről az Egyesült Államokban és az Európai Bizottság és az Egyesült Államok között folyó tárgyalásokról.
WP 19: 2/99 vélemény az Egyesült Államok Kereskedelmi Minisztériuma által 1999. április 19-én kiadott „nemzetközi biztonságos kikötő elvek" megfelelőségéről.
WP 21: 4/99 vélemény az Egyesült Államok Kereskedelmi Minisztériuma által, a javasolt „biztonságos kikötő" elvek a „nemzetközi biztonságos kikötő elveknek" való megfelelőségével kapcsolatban kiadandó gyakran ismétlődő kérdésekről.
WP 23: Munkaanyag a „nemzetközi biztonságos kikötő elvekre" vonatkozóan az Európai Bizottság és az Egyesült Államok kormánya között folyó tárgyalások jelenlegi állásáról.
WP 27: 7/99 vélemény a „biztonságos kikötő" elvek által biztosított adatvédelem szintjéről, amelyet a gyakran ismétlődő kérdésekkel (GYIK) és más kapcsolódó dokumentumokkal együtt az Egyesült Államok Kereskedelmi Minisztériuma tett közzé 1999. november 15–16-án.
WP 31: 3/2000 vélemény a „biztonságos kikötő" rendszerre vonatkozó EU/USA párbeszédről.
WP 32: 4/2000 vélemény a „biztonságos kikötő" elvek által biztosított védelem szintjéről.

[2] Az állásfoglalást a Hivatalos Lapban még nem tették közzé.

2. cikk

Ez a határozat csak a gyakran felvetődő kérdésekkel összhangban bevezetett elvek alapján az Egyesült Államokban nyújtott védelem megfelelőségére érvényes, a 95/46/EK irányelv 25. cikke (1) bekezdése követelményeinek való megfelelés céljából, és nincs hatással az említett irányelv más, a személyes adatok tagállamokon belüli kezelésével kapcsolatos rendelkezéseinek, különösen a 4. cikkének alkalmazására.

3. cikk

(1) A 95/46/EK irányelv 25. cikkétől eltérő rendelkezések alapján elfogadott nemzeti rendelkezéseknek való megfelelés biztosítása érdekében intézkedés megtételére vonatkozó hatáskörük sérelme nélkül, a tagállamok illetékes hatóságai gyakorolhatják meglévő hatáskörüket az olyan szervezet felé irányuló adatáramlás felfüggesztésére, amely önmaga tanúsította a GYFK-val összhangban bevezetett elvek elfogadását, hogy védjék az egyéneket a személyes adatok kezelése tekintetében olyan esetekben, ahol:

a) az e határozat VII. mellékletében említett egyesült államokbeli kormányzati szerv vagy egy független jogorvoslati mechanizmus az e határozat I. mellékletében meghatározott végrehajtási elvről szóló a) levél értelmében megállapította, hogy a szervezet megszegi a GYFK-val összhangban bevezetett elveket; vagy

b) az elvek megszegésének nagy a valószínűsége; okkal feltételezik, hogy az érintett végrehajtási mechanizmus sem most, sem később nem tesz megfelelő és időszerű lépéseket az adott eset rendezésére; a folytatódó adattovábbítás az érintettek súlyos károsodásának veszélyével fenyeget; és a tagállam illetékes hatóságai a körülményekhez képest elfogadható erőfeszítéseket tettek, hogy a szervezetet értesítsék, és lehetőséget adjanak neki a válaszadásra.

A felfüggesztés megszűnik, amint a gyakran felvetődő kérdésekkel összhangban bevezetett elvek teljesítését biztosítják, és arról értesítik a Közösség illetékes hatóságát.

(2) A tagállamok haladéktalanul tájékoztatják a Bizottságot, amikor az (1) bekezdés alapján intézkedéseket fogadnak el.

(3) A tagállamok és a Bizottság egymást is tájékoztatják azokról az esetekről, amikor az Egyesült Államokban a gyakran felvetődő kérdésekkel összhangban bevezetett elveknek való megfelelés biztosításáért felelős szervek intézkedése nem biztosítja az ilyen megfelelést.

(4) Ha az (1), (2) és (3) bekezdés alapján összegyűjtött információk azt bizonyítják, hogy az Egyesült Államokban a gyakran felvetődő kérdésekkel összhangban bevezetett elveknek való megfelelés biztosításáért felelős bármely szerv nem hatékonyan tölti be szerepét, a Bizottság tájékoztatja az Egyesült Államok Kereskedelmi Minisztériumát, és szükség esetén a 95/46/EK irányelv 31. cikkében említett eljárással összhangban intézkedéstervezeteket nyújt be e határozat visszavonása, felfüggesztése vagy hatályának korlátozása céljából.

4. cikk

(1) Ez a határozat bármikor kiigazítható a végrehajtásával kapcsolatos tapasztalat fényében, illetve ha az Egyesült Államok jogszabályainak követelményei szigorúbbá válnak az elvek és a GYFK által biztosított védelmi szintnél.

A Bizottság a tagállamok felé történő értesítése után három évvel minden esetben értékeli e határozat végrehajtását a rendelkezésre álló információk alapján, és beszámol a 95/46/EK irányelv 31. cikke alapján létrehozott bizottságnak bármilyen vonatkozó megállapításról, beleértve az olyan bizonyítékokat, amelyek hatással lehetnek annak értékelésére, hogy az e határozat 1. cikkében meghatározott rendelkezések a 95/46/EK irányelv 25. cikke értelmében megfelelő védelmet biztosítanak, illetve annak bizonyítékát, hogy ezt a határozatot megkülönböztető módon hajtják végre.

(2) A Bizottság szükség esetén intézkedéstervezeteket terjeszt elő a 95/46/EK irányelv 31. cikkében említett eljárásnak megfelelően.

5. cikk

A tagállamok meghozzák azokat az intézkedéseket, amelyek szükségesek ahhoz, hogy ennek a határozatnak legkésőbb a tagállamok felé történő értesítésétől számított 90 napos időszak végéig megfeleljenek.

6. cikk

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2000. július 26-án.

a Bizottság részéről

Frederik BOLKESTEIN

a Bizottság tagja

I. MELLÉKLET

„BIZTONSÁGOS KIKÖTŐ” ADATVÉDELMI ELVEK

kiadta az Egyesült Államok Kereskedelmi Minisztériuma 2000. július 21-én

Az Európai Unió átfogó adatvédelmi jogszabálya, az adatvédelmi irányelv (az irányelv) 1998. október 25-én lépett hatályba. Az irányelv előírja, hogy a személyes adatok továbbítása csak olyan, az EU-ban tagsággal nem rendelkező országokba történhessen meg, amelyek biztosítják a személyiségi jog „megfelelő” szintű védelmét. Bár az Egyesült Államok és az Európai Unió közös célja az állampolgáraik számára az adatvédelem fokozása, az Egyesült Államok az Európai Uniótól eltérően közelíti meg az adatvédelmet. Az Egyesült Államok ágazati megközelítést használ, amely a törvényhozás, a szabályozás és az önszabályozás keverékére támaszkodik. Az említett eltérések miatt az Egyesült Államokban sok szervezet bizonytalanságát fejezte ki az EU által megkívánt, a személyes adatoknak az Európai Unióból az Egyesült Államokba történő továbbítására vonatkozó „megfelelőségi szabvány” hatásával kapcsolatban.

E bizonytalanság csökkentése és az ilyen adattovábbításokra vonatkozó kiszámíthatóbb keret biztosítása érdekében, a Kereskedelmi Minisztérium hatósági jogkörében a nemzetközi kereskedelem támogatása, elősegítése és fejlesztése céljából kiadja ezt a dokumentumot és a gyakran felvetődő kérdéseket („az elveket”). Az elveket az iparral 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 Egyesült Államok olyan szervezeteinek használatára szánták, amelyek az Európai Unióból személyes adatokat fogadnak, a „biztonságos kikötő” és az általa létrehozott „megfelelőségi” minősítés elnyerése céljából. Mivel az elveket kizárólag e különleges cél szolgálatára dolgozták ki, más célokra alkalmatlannak bizonyulhatnak. Az elvek nem használhatók fel a tagállamokban a személyes adatok kezelésére alkalmazandó irányelv végrehajtásához szükséges nemzeti rendelkezések helyettesítésére.

A szervezetek teljesen önkéntes alapon határozhatnak arról, hogy jelentkeznek a „biztonságos kikötő” minősítés elnyeréséért, amelyre különböző módokon tehetnek szert. Azoknak a szervezeteknek, amelyek úgy döntenek, hogy elfogadják az elveket, meg kell felelniük az elveknek annak érdekében, hogy megszerezzék és megtartsák a „biztonságos kikötő” előnyeit, és nyilvánosan ki kell jelenteniük, hogy így tesznek. Ha például egy szervezet csatlakozik egy olyan önszabályozó adatvédelmi programhoz, amely elfogadja az elveket, „biztonságos kikötő” - nek minősül. A szervezetek saját önszabályozó adatvédelmi politikájuk kidolgozásával is ilyennek minősülhetnek, feltéve hogy politikájuk megfelel az elveknek. Ha az elveknek való megfelelésben a szervezet teljes egészében vagy részben az önszabályozásra támaszkodik, az ilyen önszabályozás nem teljesítésének a Szövetségi Kereskedelmi Bizottságról szóló törvény tisztességtelen és megtévesztő cselekedetek tilalmáról szóló 5. szakasza vagy az ilyen cselekedetek tilalmáról szóló más törvény vagy rendelet alapján szintén peresíthetőnek kell lennie. (Lásd a mellékletben az Egyesült Államok az Európai Unió által elismert hatósági szerveinek jegyzékét.) Ezen túlmenően, a hatósági, szabályozó, közigazgatási vagy más jogi szerv (vagy szabályok) hatálya alá tartozó szervezetek, amelyek hatékonyan védik a személyes adatokat, szintén jogot szerezhetnek a „biztonságos kikötő” cím előnyeire. A „biztonságos kikötő” előnyeit minden esetben attól az időponttól biztosítják, amikor a „biztonságos kikötő” minősítést elnyerni kívánó szervezet önmaga tanúsítja a Kereskedelmi Minisztériumnak (vagy az általa kijelölt szervnek), hogy az a gyakran felvetődő kérdésekben ismertetett útmutatással összhangban betartja az elveket.

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.

Gyakorlati vagy más célból a szervezetek esetleg minden adatfeldolgozási műveletükre alkalmazni kívánják az elveket, de csak azokra az adatokra kötelesek alkalmazni, amelyeket a „biztonságos kikötő”-be való belépés után továbbítottak. A „biztonságos kikötő” minősítéshez a szervezetek nem kötelesek ezeket az elveket alkalmazni a személyes adatokra a manuális nyilvántartórendszerekben. Az Európai Unióból származó információk manuális nyilvántartórendszerekben történő fogadása tekintetében „biztonságos kikötő”-nek minősülni kívánó szervezeteknek alkalmazniuk kell az elveket minden olyan információra, amelyet a „biztonságos kikötő”-be való

belépés után továbbítanak. Az a szervezet, amely a „biztonságos kikötő” előnyeit ki kívánja terjeszteni az Európai Unióból továbbított, a munkaviszonnyal összefüggésben felhasználandó, humán erőforrással kapcsolatos személyes információra, ezt jeleznie kell, amikor önmagát tanúsítja a Kereskedelmi Minisztérium (vagy az általa kijelölt szerv) felé, és meg kell felelnie az öntanúsításról szóló a gyakran felvetődő kérdésben meghatározott követelményeknek. A szervezeteknek arra is képesnek kell lenniük, hogy szolgáltassák az irányelv 26. cikke alapján szükséges biztosítékokat, ha az Európai Unióból adatokat továbbító felekkel lényeges adatvédelmi rendelkezésekre vonatkozóan megkötött írásbeli megállapodásokba belefoglalják az elveket, amint az ilyen mintaszerződésekre vonatkozó más rendelkezéseket a Bizottság és tagállamok engedélyezik.

Az értelmezési kérdések és a „biztonságos kikötő” elveinek való megfelelés (beleértve a gyakran felvetődő kérdéseket), valamint és a „biztonságos kikötő” szervezetek adatvédelmi politikáinak tekintetében az Egyesült Államok jogát kell alkalmazni, kivéve ha a szervezetek az európai adatvédelmi hatóságokkal való együttműködés mellett kötelezték el magukat. Más megállapodás hiányában, a „biztonságos kikötő” elvek és a gyakran felvetődő kérdések minden rendelkezését alkalmazni kell, ahol megfelelő.

A „személyes adatok” és a „személyes információ” olyan azonosított vagy azonosítható egyénre vonatkozó adatok, amelyek az irányelv hatálya alá tartoznak, és amelyeket valamely egyesült államokbeli szervezet az Európai Uniótól kapott, és az valamilyen formában rögzített.

ÉRTESÍTÉS

A szervezetnek tájékoztatnia kell az egyéneket azokról a célokról, amelyek érdekében a rájuk vonatkozó információt gyűjti és használja; arról, hogy kérdéseikkel vagy panaszukkal hogyan léphetnek kapcsolatba a szervezettel; a harmadik felek típusairól, amelyeknek átadja az adatokat; valamint a választási lehetőségekről és eszközökről, amelyeket a szervezet az egyéneknek az adatok felhasználásának és nyilvánosságra hozatalának korlátozására felkínál. Ezt a tájékoztatást világos és érthető megfogalmazásban kell megadni, az első alkalommal akkor, amikor az egyéneket felkérik a személyes információ szolgáltatására a szervezetnek, vagy azt követően a lehető leghamarabb, 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, vagy mielőtt harmadik félnek azokat először átadná ([1]).

VÁLASZTÁSI LEHETŐSÉG

A szervezetnek választási lehetőséget (a nem kívánt lehetőségek kizárásával) kell felkínálnia az egyéneknek, hogy személyes adataikat a) átadják-e harmadik félnek ([1]); vagy b) felhasználják-e olyan célra, amely nem összeegyeztethető azzal (azokkal) a céllal (célokkal), amelyre eredetileg gyűjtötték az adatokat, vagy amelyet az egyén a későbbiekben engedélyezett. Az egyének számára egyértelmű és szembetűnő, könnyen hozzáférhető és megfizethető mechanizmusokat kell biztosítani a választási lehetőség gyakorolására.

A különleges adatok tekintetében (ilyenek az orvosi vagy egészségi állapotra, a faji eredetre vagy etnikai hovatartozásra, a politikai véleményre, a vallásos vagy filozófiai meggyőződésre, a szakszervezeti tagságra vagy az egyén szexuális életére vonatkozó személyes adatok), megerősítő vagy kifejezett választási lehetőséget (a kívánt lehetőség kiválasztásával) kell kapniuk, ha az információt harmadik fél számára átadják, vagy a gyűjtés eredeti céljától, illetve az egyén által a választási lehetőségével élve a későbbiekben engedélyezett céltól eltérő célra használják fel. A szervezetnek minden esetben különlegesként kell kezelnie minden olyan, harmadik féltől kapott információt, amelyet a harmadik fél különlegesként határoz meg és kezel.

ADATTOVÁBBÍTÁS HARMADIK FÉL RÉSZÉRE

Ahhoz, hogy az információt harmadik fél számára átadhassák, a szervezeteknek alkalmazniuk kell az értesítés és a választási lehetőség elveit. Amennyiben a szervezet az információt olyan harmadik félnek kívánja továbbítani, amely közvetítőként jár el a lábjegyzetben leírtak szerint, ezt úgy teheti meg, ha először vagy megállapítja, hogy a harmadik fél csatlakozik az elvekhez, 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. Ha szervezet teljesíti ezeket a követelményeket, nem vonható felelősségre (hacsak a szervezet másként nem állapodik meg), ha a harmadik fél, amelynek az ilyen információt továbbítja, azt bármely korlátozással vagy nyilatkozattal ellentétes módon kezeli, kivéve ha a szervezet tudta vagy tudnia kellett volna, hogy a harmadik fél ilyen, az elvekkel ellentétes módon fogja az információt kezelni, és nem tette meg az indokolt lépéseket az ilyen adatfeldolgozás megakadályozására vagy megállítására.

([1]) Nem szükséges értesítést vagy választási lehetőséget biztosítani, amikor az adatátadás a feladato(ka)t a szervezet nevében és útmutatásai alapján végrehajtó, közvetítőként eljáró harmadik fél részére történik. Az ilyen adatátadásra is vonatkozik a harmadik fél részére történő adattovábbítás elve.

BIZTONSÁG

A személyes információt létrehozó, fenntartó, felhasználó vagy terjesztő szervezeteknek megfelelő intézkedéseket kell tenniük, hogy megóvják az információt az elvesztéstől, a hibás felhasználástól és a jogtalan hozzáféréstől, a nyilvánosságra hozataltól, a megváltoztatástól és a megsemmisítéstől.

ADATINTEGRITÁS

Az elvekkel összhangban, a személyes információnak azokra a célokra kell vonatkoznia, amelyre azt fel kívánják használni. A szervezet nem dolgozhat fel személyes információt 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 az adatok a tervezett felhasználás szempontjából megbízhatók, pontosak, teljesek és időszerűek legyenek.

HOZZÁFÉRÉS

Az egyéneknek hozzáféréssel kell rendelkezniük a valamely szervezet birtokában lévő, rájuk vonatkozó személyes információhoz, és lehetőségük kell, hogy legyen a pontatlan információk javítására, módosítására vagy törlésére, kivéve ha az adott esetben a hozzáférés biztosításának terhe vagy költsége nem állna arányban az egyén adatvédelmi jogának a kockázatával, vagy ha ezzel más személy jogait érné sérelem.

VÉGREHAJTÁS

A hatékony adatvédelemnek magában kell foglalnia az elvek teljesítését biztosító mechanizmusokat, a jogorvoslati jogot az elvek nem teljesítése által érintett egyének számára, valamint a szervezetre vonatkozó következményeket, amikor az elveket nem követik. Az ilyen mechanizmusoknak minimumkövetelményként tartalmazniuk kell a) könnyen hozzáférhető és megfizethető független eljárási mechanizmusokat, amelyekkel minden egyes személy panaszait és vitáit meg lehet vizsgálni és megoldani az elvekre hivatkozva, és kártérítést lehet megítélni, ha az érvényes jog vagy a magánszektor kezdeményezései azt előírják; b) eljárásokat annak ellenőrzésére, hogy az üzleti vállalkozások által az adatvédelmi gyakorlataikról készített tanúsítványok és állítások helytállóak-e, és hogy az adatvédelmi gyakorlatokat úgy valósították-e meg, ahogyan azokat benyújtották; és c) az elvek elfogadását kijelentő szervezetek részéről kötelezettséget az elvek nem teljesítéséből adódó problémák jogorvoslatára, valamint az ilyen szervezetekre vonatkozó következményeket. A szervezetek általi teljesítés biztosítása érdekében a szankcióknak kellőképpen szigorúaknak kell lenniük.

Melléklet

Az Egyesült Államok az Európai Unió által elismert hatósági testületeinek jegyzéke

Az Európai Unió az Egyesült Államok következő kormányzati szerveit ismeri el a panaszok kivizsgálására és a tisztességtelen vagy megtévesztő gyakorlatok miatt járó kártérítés kieszközlésére, valamint az egyének jogorvoslatára feljogosított szervekként, a GYFK-val összhangban végrehajtott elvek nem teljesítése esetén:

– a Szövetségi Kereskedelmi Bizottság, a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza szerinti hatásköre alapján,

– a Közlekedési Minisztérium, az Egyesült Államok törvénykönyve 41712. szakaszának 49. címe szerinti hatásköre alapján.

II. MELLÉKLET

GYAKRAN FELVETŐDŐ KÉRDÉSEK (GYFK)

1. GYFK – Különleges adatok

K: *A szervezetnek mindig kifejezett (a kívánt lehetőséget megerősítő) választási lehetőséget kell-e biztosítania a különleges adatokra vonatkozóan?*

V: Nem, az ilyen választási lehetőségre nincs szükség, amennyiben az adatfeldolgozás: (1) az érintett vagy más személy létfontosságú érdekében áll; (2) szükséges a jogszerű követelések vagy a védelem megállapításához; (3) egészségügyi ellátás vagy diagnózis nyújtásához szükséges; (4) politikai, filozófiai, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármilyen más nonprofit szerv törvényes tevékenysége során történik, és azzal a feltétellel, hogy a feldolgozás kizárólag a szervezet tagjaira vagy olyan személyekre vonatkozik, akik annak céljaival összefüggésben rendszeres kapcsolatban állnak vele, és hogy az adatokat nem adják át harmadik félnek az érintettek beleegyezése nélkül; (5) a szervezetnek a foglalkoztatási jog területén fennálló kötelezettségeinek a végrehajtása céljából szükséges; vagy (6) olyan adatokra vonatkozik, amelyeket az egyén egyértelműen nyilvánosságra hozott.

2. GYFK – Újságírói kivételek

K: *Tekintve az Egyesült Államokban a sajtószabadság alkotmányos védelmét és az irányelv alóli mentességet az újságírói anyagra vonatkozóan, érvényesek-e a „biztonságos kikötő" elvek az újságírói célokra összegyűjtött, fenntartott vagy terjesztett személyes információra?*

V: Amennyiben az Egyesült Államok alkotmányának első módosításában szereplő a sajtószabadságra vonatkozó jog ütközik az adatvédelem érdekeivel, az első alkotmánymódosításnak kell szabályoznia ezen érdekek egyeztetését, tekintettel az egyesült államokbeli személyek vagy szervezetek tevékenységére. A közzétételre, rádió- vagy televíziós műsorhoz vagy újságírói anyag nyilvános közlésének más formájához összegyűjtött személyes információkra – akár felhasználják azokat, akár nem –, valamint a korábban közzétett anyagban talált, médiaarchívumból terjesztett információkra a „biztonságos kikötő" elvek követelményei nem vonatkoznak.

3. GYFK – Mögöttes felelősség

K: *Az internetszolgáltatók, a távközlési szolgáltatók vagy más szervezetek felelősek-e a „biztonságos kikötő" elvek alapján, amikor más szervezet nevében csupán közlik, továbbítják, átirányítják vagy tárolják az információt, amely megsértheti feltételeiket?*

V: Nem. Amint maga az irányelv, a „biztonságos kikötő" 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 feldolgozásának céljait és eszközeit, nem felelős.

4. GYFK – Befektetési banktevékenység és könyvvizsgálat

K: *A könyvvizsgálók és befektetési bankárok tevékenységei magukban foglalhatják a személyes adatok feldolgozását az egyén beleegyezése vagy tudta nélkül. Ezt milyen körülmények között teszik lehetővé az értesítésre, a választási lehetőségre és a hozzáférésre vonatkozó elvek?*

V: A befektetési bankárok vagy könyvvizsgálók csak a törvényes vagy közérdekű követelményeknek való megfeleléshez szükséges mértékben és időtartamban dolgozhatnak fel információt az egyén tudta nélkül, és olyan más körülmények között, amelyek esetén ezen elvek alkalmazása hátrányosan befolyásolná a szervezet jogos érdekeit. Ezek a jogos érdekek magukban foglalják a vállalkozások jogi kötelezettségei és törvényes számviteli tevékenységei teljesítésének folyamatos ellenőrzését, és a lehetséges tulajdonszerzésekkel, egyesülésekkel, vegyes vállalkozásokkal vagy a befektetési bankárok vagy könyvvizsgálók által végrehajtott más hasonló ügyletekkel összefüggő titkosság szükségességét.

5. GYFK – Az adatvédelmi hatóságok szerepe [1]

K: *A magukat az Európai Unió adatvédelmi hatóságaival való együttműködés mellett elkötelező vállalkozások hogyan teszik meg a kötelezettségvállalásokat, és hogyan valósítják meg azokat?*

V: A „biztonságos kikötő" alapján az Egyesült Államok az EU-ból személyes adatokat fogadó szervezeteinek kötelezettséget kell vállalniuk a „biztonságos kikötő" elvek teljesítését biztosító hatékony mechanizmusok alkalmazására. Pontosabban, a végrehajtási elvben megállapítottaknak megfelelően biztosítaniuk kell a) a jogorvoslatot azon egyének számára, akikre az adatok vonatkoznak; b) eljárásokat annak ellenőrzésére, hogy az üzleti vállalkozások által az adatvédelmi gyakorlataikról készített tanúsítványok és állítások helytállóak-e; és c) az elvek nem teljesítéséből eredő problémák orvoslására vonatkozó kötelezettségeket, és a következményeket az ilyen szervezetekre nézve. A szervezet eleget tehet a végrehajtási elv a) és c) pontjának, ha elfogadja e GYFK követelményeit az adatvédelmi hatóságokkal történő együttműködésre vonatkozóan.

A szervezet kötelezheti magát az adatvédelmi hatóságokkal történő együttműködésre azáltal, hogy „biztonságos kikötő" tanúsításában bejelenti a Kereskedelemi Minisztériumnak (lásd: öntanúsításról szóló 6. GYFK), hogy a szervezet:

1. elhatározza, hogy az adatvédelmi hatóságokkal történő együttműködés révén eleget tesz a „biztonságos kikötő" végrehajtási elv a) és c) pontjában meghatározott követelménynek;

2. együttműködik az adatvédelmi hatóságokkal a „biztonságos kikötő" hatálya alá tartozó panaszok kivizsgálásában és megoldásában; és

3. megfogad minden, az adatvédelmi hatóságoktól kapott ajánlást, amennyiben az adatvédelmi hatóságok úgy látják, hogy a szervezetnek különleges intézkedést kell hoznia a „biztonságos kikötő" elveknek való megfeleléshez, beleértve a jogorvoslati vagy kártérítési intézkedéseket az elvek nem teljesítése által érintett egyének javára, és írásban erősíti meg az adatvédelmi hatóságok felé az ilyen intézkedés megtörténtét.

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

– Az adatvédelmi hatóságok ajánlását az adatvédelmi hatóságok európai uniós szinten létrehozott nem hivatalos bizottsága kézbesíti, amely többek között segíti az összehangolt és összefüggő megközelítés biztosítását.

– A bizottság ajánlást ad az Egyesült Államok egyénektől származó megoldatlan panaszokban érintett szervezeteinek az EU-ból a „biztonságos kikötő" alapján továbbított személyes információk kezelésére. Ez az ajánlás a „biztonságos kikötő" elvek helyes alkalmazását kívánja biztosítani, és magában foglal bármilyen, az érintett egyén(ekre) vonatkozó jogorvoslatot, amelyet az adatvédelmi hatóságok megfelelőnek tartanak.

– A bizottság ilyen ajánlást válaszként, az érintett szervezetek megkeresésére és/vagy a közvetlenül az egyénektől érkező, olyan szervezetek elleni panaszokra ad, amelyek a „biztonságos kikötő" céljaiból 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.

– Az ajánlást csak azután adják ki, hogy a jogvitában érdekelt mindkét fél megfelelő lehetőséget kapott a magyarázatra és a kívánt bizonyítékok benyújtására. A bizottság törekszik arra, hogy a megfelelő folyamatra vonatkozó követelményhez mérten a lehető leggyorsabban kézbesítse az ajánlást. Általános szabályként, a bizottság arra törekszik, hogy a panasz vagy megkeresés kézhezvételét követő 60 napon belül – illetve, ha lehetséges, ennél gyorsabban – adjon tanácsot.

– A bizottság közzéteszi a hozzá benyújtott panaszok vizsgálatának eredményeit, ha azt helyénvalónak találja.

– Az ajánlás bizottság általi kézbesítése nem hoz létre semmilyen kötelezettséget a bizottságra vagy az egyes adatvédelmi hatóságokra nézve.

[1] E GYFK hozzáadása a csomaghoz az adatvédelmi hatóságok megállapodásától függ. Ezt a szöveget megvitatták a 29. cikk szerinti munkacsoporttal, és többség elfogahatónak találta, de a határozott állásfoglalásra csak a munkacsóport által a végsõ csomagban kiadandó átfogó vélemény összefüggésében készek.

A fentiek szerint a jogviták megoldására ezt a lehetőséget választó szervezeteknek vállalniuk kell, hogy megfogadják az adatvédelmi hatóságok ajánlását. Ha a szervezet a kézbesítésétől számított 25 napon belül nem fogadja meg az ajánlást, és a késedelemre vonatkozóan nem ad kielégítő indoklást, a bizottság értesítést ad a szándékáról, hogy az ügyet megküldje a Szövetségi Kereskedelmi Bizottsághoz vagy az Egyesült Államok más szövetségi vagy állami testületéhez, amely végrehajtó hatáskörrel rendelkezik csalás vagy hamis közlés esetén, vagy hogy megállapítsa, hogy az együttműködési megállapodást súlyosan megszegték, és ezért azt semmisnek kell tekinteni. Utóbbi esetben a bizottság tájékoztatja a Kereskedelmi Minisztériumot (vagy az általa kijelölt szervet), hogy a „biztonságos kikötő" résztvevőinek jegyzékét megfelelően módosíthassák. Az adatvédelmi hatóságokkal történő együttműködési kötelezettségvállalás bármilyen nem teljesítése, valamint a „biztonságos kikötő" elvek nem teljesítése a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza vagy más hasonló törvény alapján megtévesztő gyakorlatként perelhető lesz.

Az ezt a lehetőséget választó szervezeteknek éves díjat kell fizetniük, amely a bizottság működési költségeinek fedezésére szolgál; ezenkívül adott esetben vállalniuk kell a szükséges fordítási költségeket, amelyek a bizottságnál a kérelmek elbírálásából vagy a szervezetekkel szemben felmerülő panaszokból adódnak. Az éves díj nem lépi túl az 500 USD-t, és kisebb vállalkozások esetében ennél kevesebb lesz.

Az adatvédelmi hatóságokkal történő együttműködés lehetősége a „biztonságos kikötő"-höz egy hároméves időtartam folyamán csatlakozó szervezetek számára áll nyitva. Az adatvédelmi hatóságok ennek az időszaknak a vége előtt felülvizsgálják ezt a rendelkezést, ha az egyesült államokbeli szervezetek túl nagy számban választják ezt a lehetőséget.

6. GYFK – Öntanúsítás

K: *Hogyan tudja egy szervezet önmaga tanúsítani, hogy tartja magát a „biztonságos kikötő" elvekhez?*

V: A „biztonságos kikötő" előnyök attól az időponttól érvényesek, amikor a szervezet önmaga tanúsítja a Kereskedelmi Minisztérium (vagy az általa kijelölt szerv) részére, hogy betartja az elveket az alábbi útmutatással összhangban.

A „biztonságos kikötő"-re vonatkozó öntanúsításhoz a szervezet a „biztonságos kikötő"-höz csatlakozó szervezet a nevében eljáró vállalkozás tisztségviselője által aláírt levelet küldhet a Kereskedelmi Minisztériumnak (vagy az általa kijelölt szervnek), amely legalább a következő adatokat tartalmazza:

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

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

3. a szervezet ilyen személyes adatokra vonatkozó adatvédelmi politikájának a leírása, beleértve a következőket: a) hol érhető el az adatvédelmi politika a nyilvánosság számára betekintésre; b) a bevezetés tényleges időpontja; c) a panaszokat, hozzáférési kérelmeket és a „biztonságos kikötő"-vel kapcsolatban felmerülő bármilyen kérdést kezelő kapcsolattartó iroda; d) az adott hatósági szerv, amely joghatósággal bír a szervezettel szemben felmerülő követelések fogadására az esetleges tisztességtelen vagy megtévesztő gyakorlat, valamint az adatvédelmet szabályozó törvények és rendeletek megsértése ügyében (és amely szerv az elvek mellékletében fel van sorolva); e) bármely olyan adatvédelmi program neve, amelynek a szervezet tagja; f) a hitelesítés módszere (pl. házon belül, harmadik fél által) [1]; és g) a független eljárási mechanizmus, amely a megoldatlan panaszok kivizsgálására rendelkezésre áll.

Amennyiben a szervezet a „biztonságos kikötő" előnyeit ki akarja terjeszteni az Európai Unióból átadott, a munkaviszonnyal összefüggésben felhasználásra kerülő humánerőforrás-adatokra, ezt akkor teheti meg, ha van olyan, az elvek mellékletében felsorolt hatósági szerv, amely joghatósággal bír a szervezet ellen humánerőforrás-adatokkal kapcsolatban felmerülő követelések kivizsgálására. Ezen túlmenően a szervezetnek ezt jeleznie kell levelében, és ki kell jelentenie kötelezettségvállalását az együttműködésre az EU érintett hatóságával vagy hatóságaival, az esetnek megfelelően az 5. GYFK-val vagy a 9. GYFK-val összhangban, valamint azt, hogy megfogadja az ilyen hatóságok ajánlását.

A minisztérium (vagy az általa kijelölt szerv) jegyzéket tart fenn az összes olyan szervezetről, amely ilyen levelet nyújt be, ezáltal biztosítva a „biztonságos kikötő" előnyök hozzáférhetőségét, és az éves levelek és a 11. GYFK szerint kapott értesítések alapján frissíti az ilyen jegyzékeket. Az ilyen öntanúsítási leveleket legalább évente meg kell küldeni. Ellenkező esetben a szervezetet törlik a jegyzékből, és a „biztonságos kikötő" előnyöket a továbbiakban nem biztosítják. A jegyzéket és a szervezetek által benyújtott öntanúsítóleveleket egyaránt

[1] Lásd: a hitelesítésről szóló 7. GYFK.

hozzáférhetővé teszik a nyilvánosság számára. Minden olyanszervezetnek, amely a „biztonságoskikötő”-re önmagát tanúsítja, az erre vonatkozóan közzétett adatvédelem-politikai nyilatkozatában szintén ki kell jelentenie, hogy betartja a „biztonságos kikötő” elveket.

A „biztonságos kikötő” elvek betartására vonatkozó kötelezettségvállalást nem kötik időkorlátokhoz az azon idő alatt fogadott adatok tekintetében, amíg a szervezet élvezi a „biztonságos kikötő” előnyeit. A szervezet kötelezettségvállalása azt jelenti, hogy továbbra is alkalmazza az elveket az ilyen adatok esetében addig, amíg tárolja, felhasználja vagy nyilvánosságra hozza azokat, még akkor is, ha a későbbiekben bármilyen okból elhagyja a „biztonságos kikötő”-t.

Annak a szervezetnek, amely egyesülés vagy átvétel eredményeként megszűnik önálló jogi személyként létezni, erről előzetesen értesítenie kell a Kereskedelmi Minisztériumot (vagy az általa kijelölt szervet). Az értesítésben jeleznie kell azt is, hogy az átvevő jogi személy vagy egyesülés eredményeként létrejött jogi személy (1) továbbra is betartja a „biztonságos kikötő” elveket az átvételt vagy egyesülést szabályozó törvény rendelkezése alapján; vagy (2) úgy dönt, hogy önmaga tanúsítja a „biztonságos kikötő” elvek betartását vagy helyükbe más biztosítékokat léptet, mint például egy írásos megállapodást, amely biztosítja a „biztonságos kikötő” elvek betartását. Amennyiben sem az (1), sem a (2) pont nem érvényes, minden, a „biztonságos kikötő” alapján megszerzett adatot haladéktalanul törölni kell.

A szervezetnek nem szükséges alárendelnie az összes személyes adatot a „biztonságos kikötő” elveknek, de a „biztonságos kikötő”-höz való csatlakozása után az EU-ból fogadott minden személyes adatot alá kell rendelni a „biztonságos kikötő” elveknek.

A közvélemény hamis tájékoztatása a szervezet részéről a „biztonságos kikötő” elvek betartása tekintetében perelhető a Szövetségi Kereskedelmi Bizottság vagy más illetékes kormányzati szerv részéről. A Kereskedelmi Minisztériumnak (vagy az általa kijelölt szervnek) adott hamis közlések a hamis nyilatkozatokról szóló törvény (18 U. S. C. § 1001) alapján perelhetők.

7. GYFK – Hitelesítés

K: *Hogyan gondoskodnak a szervezetek megfelelő eljárásokról annak az ellenőrzésére, hogy azok a tanúsítványok és állítások, amelyeket a „biztonságos kikötő” adatvédelmi gyakorlataikról készítenek, igazak-e, és azokat az adatvédelmi gyakorlatokat a bemutatottakkal és a „biztonságos kikötő” elvekkel összhangban valósították-e meg?*

V: Ahhoz, hogy a végrehajtási elv hitelesítési követelményeinek megfeleljen, a szervezet az ilyen tanúsítványokat és állításokat vagy önértékelés, vagy külső megfelelőségi felülvizsgálati eljárások révén hitelesítheti.

Az önértékelési megközelítés keretében az ilyen hitelesítésnek jeleznie kellene, hogy a szervezetnek az EU-ból fogadott, személyes információra vonatkozó közzétett adatvédelmi politikája pontos, átfogó, jól látható módon bemutatott, teljes mértékben végrehajtott és hozzáférhető. Szintén jeleznie kellene, hogy adatvédelmi politikája megfelel a „biztonságos kikötő” elveknek; hogy az egyéneket tájékoztatják a panaszok kezelésére szolgáló bármilyen belső szabályzatról, valamint azokról a független mechanizmusokról, amelyeken keresztül panaszt tehetnek; tartalmaz az alkalmazottak oktatására vonatkozó eljárást a végrehajtást illetően, valamint fegyelmi eljárásokat az adatvédelmi politika követésének elmulasztása esetére; és 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, vagy egy vizsgálattal vagy a teljesítés elmulasztására vonatkozó panasszal összefüggésben hozzáférhetővé kell tennie.

A szervezeteknek meg kell őrizniük a „biztonságos kikötő” adatvédelmi gyakorlataik végrehajtásáról szóló feljegyzéseiket, 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.

Amennyiben a szervezet a külső megfelelőség-felülvizsgálati eljárást választja, az ilyen felülvizsgálati eljárásnak be kell mutatnia, hogy a szervezet adatvédelmi politikája az EU-ból fogadott személyes adatokra vonatkozóan összhangban van a „biztonságos kikötő” elvekkel, azoknak megfelel, valamint az egyéneket tájékoztatták azokról a mechanizmusokról, amelyeken keresztül panaszt tehetnek. A felülvizsgálat módszerei korlátlanul magukban foglalhatják a könyvvizsgálatot, véletlenszerű felülvizsgálatokat, „csapdák” használatát, vagy technikai eszközök használatát, az esetnek megfelelően. A külső megfelelőségi felülvizsgálat sikeres befejezését hitelesítő

nyilatkozatot vagy a felülvizsgálatot végző személynek, vagy avállalkozás 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.

8. GYFK – Hozzáférés

Hozzáférési elv:

Az egyéneknek hozzáféréssel kell rendelkezniük a valamely szervezet birtokában lévő, rájuk vonatkozó személyes információhoz, és lehetőséget kell kapniuk a pontatlan információk javítására, módosítására vagy törlésére, kivéve ha az adott esetben a hozzáférés biztosításának terhe vagy költsége nem állna arányban az egyén személyiségi jogának kockázatával, vagy ha ezzel más személy törvényes jogait érné sérelem.

1. K: *Teljes körű-e a hozzáférési jog?*

1. V: Nem. A „biztonságos kikötő" elvek alapján a hozzáférési jog az adatvédelem alapvető eleme. Különösen azt teszi lehetővé az egyének számára, hogy ellenőrizzék a róluk tárolt információ pontosságát. Mindazonáltal, a szervezet kötelezettsége az egyénre vonatkozóan tárolt információhoz való hozzáférés biztosítására az arányosság és indokoltság elvétől is függ, és ezért bizonyos esetekben mérsékelni kell. Valóban, az 1980-as OECD adatvédelmi iránymutatáshoz készült magyarázó feljegyzés világossá teszi, hogy a szervezet hozzáférésre vonatkozó kötelezettsége nem teljes körű. Sem a túl részletes kutatást nem követeli meg például idézéssel, sem az információ összes lehetséges tárolási formájához való hozzáférést nem írja elő.

Ehelyett a tapasztalat azt mutatta, hogy személyek hozzáférés iránti kérésére reagálva a szervezeteknek először azt kell megtudnia, 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, és/vagy milyen jellegű az információ (vagy felhasználása), amely a hozzáférés iránti kérelem tárgyát képezi. Az egyéneknek azonban nem kell indokolniuk a saját adatokhoz való hozzáférés iránti kérelmüket.

A költség és a teher fontos tényezők, amelyeket figyelembe kell venni, de nem elsődlegesek annak meghatározásában, hogy a hozzáférés biztosítása indokolt-e. Ha például az információt olyan döntésekre használják, amelyek jelentős hatással vannak az egyénre (pl. fontos juttatások megtagadása vagy megadása, mint például biztosítás, jelzálog vagy állás), akkor – e GYFK-k 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 (pl. nem különleges marketingadatok, amelyeket annak eldöntésére használnak, hogy az egyénnek küldjenek-e katalógust), ezzel szemben azonnal hozzáférhető, és biztosítása nem költséges, a szervezetnek kell biztosítania a hozzáférést azokhoz a tényszerű adatokhoz, amelyeket a szervezet az egyénről tárol. Az adott információ tartalmazhat az egyéntől szerzett, egy ügylet során gyűjtött, illetve másoktól szerzett tényeket, amelyek az egyénre vonatkoznak.

A hozzáférés alaptermészetének megfelelően, a szervezeteknek mindig jóhiszemű erőfeszítéseket kell tenniük a hozzáférés biztosítására. Ha például bizonyos információ védelemre szorul, és könnyen elkülöníthető más, a hozzáférés iránti kérelem tárgyát képező 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 meg kell tagadni, a hozzáférést kérő egyén számára magyarázatot kell adnia a döntéséről, és a további megkeresésekhez egy kapcsolattartási pontot kell kijelölnie számára.

2. K: *Mi a bizalmas kereskedelmi információ, és a szervezetek megtagadhatják-e a hozzáférést annak védelme érdekében?*

2. V: A bizalmas kereskedelmi információ (ahogyan ezt a kifejezést a polgári perrendtartás szövetségi szabályaiban a nyilvánosságra hozatalra vonatkozóan használják) olyan információ, amelynek a nyilvánosságra hozataltól való megvédésére a szervezet lépéseket tett, ha annak nyilvánosságra kerülése segítené a piaci versenytársat. Bizalmas kereskedelmi információnak tekinthető például egy bizonyos számítógépes program, amelyet a szervezet használ – így egy modellező program –, vagy a program részletei. Ahol a bizalmas kereskedelmi információ könnyen elkülöníthető más, hozzáférés iránti kérelem tárgyát képező információtól, a szervezetnek

el kell takarnia a bizalmaskereskedelmi adatokat, ésrendelkezésre kell bocsátania a nem bizalmas információt. 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 olyan körülmények között, ahol az ilyen titoktartási kötelezettséget normál esetben vállalnák vagy előírnák.

3. K: *A hozzáférés biztosításakor a szervezet felfedheti az egyének számára az adatbázisaiból származó rájuk vonatkozó személyes információt, vagy magához az adatbázishoz kell hozzáférést biztosítania?*

3. V: A szervezet biztosíthat hozzáférést az egyén számára történő adatátadás formájában; nem követelmény az egyén hozzáférése a szervezet adatbázisához.

4. K: *A szervezetnek át kell szerkesztenie adatbázisait a hozzáférés biztosításához?*

4. V: A hozzáférés biztosítása csak azon a szinten szükséges, ahogyan a szervezet tárolja az információt. Maga a hozzáférési elv nem jelent semmilyen kötelezettséget a személyesadat-állományok megtartására, karbantartására, újjászervezésére vagy átszerkesztésére.

5. K: *Ezekből a válaszokból az tűnik ki, hogy a hozzáférés bizonyos körülmények között megtagadható. Milyen más körülmények között tagadhatja meg a szervezet az egyének számára a rájuk vonatkozó személyes információhoz való hozzáférést?*

5. V: Az ilyen körülmények korlátozottak, és a hozzáférés megtagadására vonatkozó indoknak mindig meghatározottnak kell lennie. A szervezet visszautasíthatja 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:

a) a törvény végrehajtásába vagy érvényesítésébe való beavatkozás, beleértve a bűncselekmények megelőzését, kivizsgálását vagy felderítését, illetve a tisztességes eljáráshoz való jogot;

b) a magánkereseti jogalapokba való beavatkozás, beleértve a jogszerű követelések megelőzését, kivizsgálását vagy kinyomozását, illetve a tisztességes eljáráshoz való jogot;

c) a más egyén(ek)re vonatkozó személyes adatok nyilvánosságra hozatala, amennyiben az ilyen hivatkozásokat nem lehet eltakarni;

d) törvényes vagy más szakmai kiváltság vagy kötelezettség megsértése;

e) jövőbeni vagy folyamatban lévő tárgyalások – mint például a nyilvánosan jegyzett társaságok tulajdonának megszerzésére vonatkozó tárgyalások – szükséges titkosságának megsértése;

f) munkavállalói biztonsági vizsgálatok vagy panaszeljárások hátrányos befolyásolása;

g) a munkavállalói utánpótlás-tervezéssel és a vállalkozás átszervezésekkel kapcsolatos, korlátozott időtartamokra esetlegesen szükséges titkosság hátrányos befolyásolása; vagy

h) a biztos gazdasági vagy pénzügyi irányítással összefüggő folyamatos ellenőrzéssel, felülvizsgálattal vagy szabályozó funkciókkal összefüggésben esetlegesen szükséges titkosság hátrányos befolyásolása; vagy

i) más körülmények, amelyek között a hozzáférés biztosításának terhe vagy költsége aránytalan lenne, vagy mások törvényes jogai vagy érdekei sérülnének.

A kivételre igényt tartó szervezetnek igazolnia kell annak alkalmazhatóságát (rendszerint ez a helyzet). A fentieknek megfelelően az egyének számára meg kell jelölni a hozzáférés megtagadásának vagy korlátozásának indokait és a további megkeresésekhez a kapcsolattartási pontot.

6. K: *Felszámolhat-e díjat a szervezet a hozzáférés költségének fedezésére?*

6. V: Igen. Az OECD-iránymutatás elismeri, hogy a szervezetek felszámíthatnak díjat, feltéve hogy az nem túlzott. Így a szervezetek a hozzáférésért reális díjat számíthatnak fel. Az ismétlődő és zaklató megkeresések visszaszorítása érdekében hasznosnak bizonyulhat a díj felszámítása.

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.

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

7. K: *Köteles-e a szervezet a hozzáférést megadni nyilvános archívumból származó személyes információhoz?*

7. V: Először azt kell tisztázni, hogy a nyilvános archívum azokat a kormányzati ügynökségek vagy bármilyen szintű jogi személyek által fenntartott nyilvántartásokat jelenti, amelyek általában nyitottak a betekintésre a nyilvánosság számára. Az ilyen információra addig nem szükséges a hozzáférési elvet alkalmazni, amíg nem kapcsolódik össze más személyes információval, kivéve ha kis mennyiségű nem nyilvános adatot használnak fel nyilvános archívumok indexálására vagy szervezésére. Tiszteletben kell azonban tartani a betekintésre vonatkozó jogszabályok által meghatározott feltételeket. 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.

8. K: *Kell-e a hozzáférési elvet alkalmazni a nyilvánosan elérhető személyes információra?*

8. V: Ugyanúgy, mint a nyilvános archívumokban tárolt adatok esetében (lásd 7. K.), nem szükséges a nagyközönség számára már elérhető információhoz való hozzáférés biztosítása, amíg azokat nem kapcsolják össze nyilvánosan nem elérhető információval.

9. K: *Hogyan tudja egy szervezet megvédeni magát a hozzáférésre irányuló ismétlődő vagy zaklató kérelmekkel szemben?*

9. V: A hozzáférésre vonatkozó ilyen kérelmekre a szervezetnek nem kell válaszolnia. Ilyen okokból a szervezetek reális díjat számíthatnak fel, és 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 természete.

10. K: *Hogyan tudja egy szervezet megvédeni magát a hozzáférésre irányuló csalárd kérelmekkel szemben?*

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

11. K: *Van-e olyan határidő, amelyen belül választ kell adni a hozzáférés iránti kérelmekre?*

11. V: Igen, a szervezeteknek túlzott késedelem nélkül és elfogadható időn belül válaszolniuk kell. Ez a követelmény különböző módokon teljesíthető, az 1980-as OECD adatvédelmi iránymutatás magyarázó feljegyzésének megfelelően. Például az az adatkezelő, aki rendszeres időközönként információt biztosít az érintettek számára, mentesíthető az egyéni kérelmekre történő azonnali válaszadás kötelezettsége alól.

9. GYFK – Humán erőforrások

1. K: *A munkaviszonnyal kapcsolatban összegyűjtött személyes információ továbbítása az EU-ból az Egyesült Államokba a „biztonságos kikötő" alá tartozik?*

1. V: Igen, amennyiben az EU-ban letelepedett vállalkozás (korábbi vagy jelenlegi) munkavállalóiról a munkaviszonnyal kapcsolatban gyűjtött személyes információt továbbítja a „biztonságos kikötő"-ben részt vevő anya-, leány- vagy hozzá nem tartozó szolgáltatónak az Egyesült Államokba, atovábbítás élvezi a

„biztonságos kikötő” előnyeit. Ilyen esetekben azinformáció gyűjtése és a továbbítást megelőző kezelése annak az EU-országnak a nemzeti joga alá tartozik, ahol azt összegyűjtötték, és a továbbításra vonatkozó feltételeket és korlátozásokat azon jog szerint kell figyelembe venni.

A „biztonságos kikötő” elvek csak akkor érvényesek, amikor egyedileg azonosított adatokat továbbítanak vagy azokhoz hozzáférnek. Az összesített foglalkoztatási adatokra és/vagy a név nélküli vagy álnevesített adatok felhasználására támaszkodó statisztikai jelentés adatvédelmi aggályokra nem ad okot.

2. K: *Hogyan vonatkoznak az ilyen információra az értesítési és választási lehetőség elvek?*

2. V: Bármely egyesült államokbeli szervezet, amely a „biztonságos kikötő” alapján az Európai Unióból munkavállalókra vonatkozó információt kapott, azt csak az értesítési és választási lehetőség elvvel összhangban fedheti fel harmadik fél számára és/vagy használhatja fel különböző célokra. Ha például egy szervezet a munkaviszonyon keresztül összegyűjtött személyes információt nem foglalkoztatással összefüggő célokra – például marketingértesítésekre – szándékozik felhasználni, akkor az egyesült államokbeli szervezetnek választási lehetőséget kell biztosítania az érintett magánszemélyek számára, mielőtt így tenne, kivéve ha azok már engedélyezték az információ ilyen célú felhasználását. Ezenfelül az ilyen választási lehetőségeket tilos a foglalkoztatási alkalmak korlátozására vagy az ilyen alkalmazottakkal szemben bármilyen megtorló intézkedés alkalmazására felhasználni.

Meg kell jegyezni, hogy egyes, a néhány 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.

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

Olyan mértékben és arra az időtartamra, amely annak érdekében szükséges, hogy a szervezet jogos érdekei ne sérüljenek az előléptetések, kinevezések vagy más hasonló foglalkoztatási döntések meghozatala során, a szervezetnek nem szükséges felajánlania az értesítést és a választási lehetőséget.

3. K: *Hogyan érvényesül a hozzáférési elv?*

3. V: A hozzáférésről szóló GYFK 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. A „biztonságos kikötő” megköveteli, hogy az ilyen adatokat az Egyesült Államokban feldolgozó szervezet együttműködjön az ilyen hozzáférés biztosításában vagy közvetlenül, vagy az EU-beli munkaadón keresztül.

4. K: *Hogyan kezelik a „biztonságos kikötő” elvek alapján az alkalmazotti adatokra vonatkozó végrehajtást?*

4. V: Amennyiben az információt csak a munkaviszonnyal összefüggésben használják fel, a munkavállalóval szemben az adatokért az elsődleges felelősség az EU-beli vállalkozásé 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 információ vélelmezett helytelen kezelése az Egyesült Államokban történt, a felelősség azé az egyesült államokbeli szervezeté, amely az információt a munkaadótól kapta, és nem a munkaadóé, ilyenformán inkább a „biztonságos kikötő” elvek vélelmezett megsértését jelenti, mint az irányelvet végrehajtó nemzeti jogszabályokét. Ez lesz a leghatékonyabb módja a helyi munkajog és munkaügyi megállapodások, valamint az adatvédelmi jogszabályok által előírt, egymást gyakran átfedő jogok és kötelezettségek teljesítésének.

Az Egyesült Államokban a „biztonságos kikötő”-ben részt vevő szervezetnek, amely az Európai Unióból továbbított európai unióbeli humánerőforrás-adatokat használ fel a munkaviszonnyal összefüggésben, és amely az ilyen továbbításokat a „biztonságos kikötő” keretébe kívánja helyezni, ezért el kell köteleznie magát az EU illetékes hatóságai által elvégzett vizsgálatokban való együttműködésre,

valamint azok ajánlásainakkövetésére az ilyen esetekben. Azok az adatvédelmi hatóságok, amelyek beleegyeztek az ilyen módon történő együttműködésbe, értesítik az Európai Bizottságot és a Kereskedelmi Minisztériumot. Ha az Egyesült Államokban a „biztonságos kikötő"-ben részt vevő szervezet olyan tagállamból kíván humánerőforrás-adatokat továbbítani, ahol az adatvédelmi hatóság nem így egyezett meg, az 5. GYFK rendelkezései érvényesek.

10. GYFK – A 17. cikk szerinti szerződések

K: *Amikor kizárólag feldolgozás céljából továbbítanak adatokat az Európai Unióból az Egyesült Államokba, szükség van-e szerződésre, tekintet nélkül a feldolgozó részvételére a „biztonságos kikötő" - ben?*

V: Igen. Az Európai Unióban az adatkezelőktől mindig megkövetelik a szerződés megkötését, amikor pusztán feldolgozási célú továbbítás történik, akár az EU-n belül, akár azon kívül végzik el a feldolgozási műveletet. A szerződés célja az adatkezelő – azaz a feldolgozás céljait és eszközeit meghatározó személy vagy szerv, aki/amely az adatokra vonatkozóan az érintett egyén(ek)kel szemben a teljes felelősséget vállalja – érdekeinek védelme. A szerződés ezért pontosan meghatározza az elvégzendő feldolgozást és az adatok biztonságos tárolásának biztosításához szükséges intézkedéseket.

Egy, az Egyesült Államokban a „biztonságos kikötő"-ben részt vevő szervezetnek, amely az Európai Unióból személyes információt csupán feldolgozásra fogad, ezért nem kell alkalmaznia az elveket erre az információra, mivel az egyénnel szemben továbbra is az európai unióbeli adatkezelő a felelős, összhangban a vonatkozó EU-rendelkezésekkel (amelyek szigorúbbak lehetnek, mint az azoknak megfelelő „biztonságos kikötő" elvek).

Mivel a „biztonságos kikötő"-ben részt vevők megfelelő védelmet biztosítanak, a „biztonságos kikötő"-ben részt vevőkkel pusztán feldolgozásra vonatkozóan kötött szerződések előzetes engedélyezésére nincs szükség (vagy az ilyen engedélyt a tagállamok automatikusan megadják), ami egyébként a „biztonságos kikötő"-ben részt nem vevő vagy megfelelő védelmet másként nem biztosító adatátvevőkkel való szerződések esetében szükséges lenne.

11. GYFK – Jogviták megoldása és végrehajtás

K : *Hogyan kell végrehajtani a végrehajtási elv jogviták megoldására vonatkozó követelményeit, és mi a teendő, ha egy szervezet ismételten nem tartja be az elveket?*

V: A végrehajtási elv megállapítja a „biztonságos kikötő" végrehajtására vonatkozó követelményeket. Az elv b) pontja szerinti követelményeknek való megfelelést a hitelesítésről szóló GYFK (7. GYFK) határozza meg. Ez a 11. GYFK az a) és c) ponttal foglalkozik, amelyek közül mindkettőhöz független jogorvoslati mechanizmusra van szükség. Ezek a mechanizmusok különböző formákat ölthetnek, de meg kell felelniük a végrehajtási elv követelményeinek. A szervezetek a követelményeknek a következőkön keresztül tehetnek eleget: (1) magánszektor által kifejlesztett adatvédelmi programok teljesítése, amelyek a „biztonságos kikötő" elveket belefoglalják szabályaikba, és a végrehajtási elvben leírt típusú, hatékony végrehajtási mechanizmusokat tartalmaznak; (2) alkalmazkodás a törvényi vagy szabályozó felügyeleti hatóságokhoz, amelyek rendelkeznek az egyedi panaszok kezeléséről és a jogviták megoldásáról; vagy (3) kötelezettségvállalás az Európai Unióban lévő adatvédelmi hatóságokkal vagy meghatalmazott képviselőikkel való együttműködésre. E felsorolás szándéka a szemléltetés, nem a korlátozás. A magánszektor a végrehajtás biztosítására más mechanizmusokat is tervezhet, amennyiben azok megfelelnek a végrehajtási elv és a GYFK-k követelményeinek. Meg kell jegyezni, hogy a végrehajtási elv követelményei az elvek bevezetésének (3) bekezdésében közzétett, arra vonatkozó követelményeken túl alkalmazandók, hogy az önszabályozói törekvéseknek a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. cikke vagy hasonló alapokmány alapján végrehajthatóknak kell lenniük.

Jogorvoslati mechanizmusok

A fogyasztókat arra kell ösztönözni, hogy szükség esetén az adott szervezettel kapcsolatban emeljenek panaszt azelőtt, hogy a független jogorvoslati mechanizmusokhoz fordulnának. A jogorvoslati mechanizmus függetlensége olyan ténykérdés, amely többféleképpen bemutatható, például átlátható összetétellel és

finanszírozással, vagy egy hitelesített nyomon követőnyilvántartással. A végrehajtási elvbenmegkövetelteknek megfelelően, a magánszemélyek számára rendelkezésre álló jogorvoslatnak könnyen hozzáférhetőnek és megfizethetőnek 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 a „biztonságos kikötő" elvekkel ([1]). Szintén együtt kell működniük az eszközök – mint például formanyomtatványok a panaszokhoz – kidolgozásában, a panaszrendezési eljárás megkönnyítése érdekében.

Jogorvoslatok és szankciók

A jogvitákat eldöntő szerv által nyújtott bármilyen jogorvoslatnak ahhoz kell vezetnie, hogy a nem teljesítés hatását a szervezet megfordítja vagy kijavítja, amennyiben ez megvalósítható, és a szervezet által a jövőben végzett adatfeldolgozás összhangba kerül az elvekkel, valamint – adott esetben – a panaszt tevő egyén személyes adatainak feldolgozása megszűnik. A szankcióknak kellőképpen szigorúaknak kell lenniük ahhoz, hogy biztosítsák a szervezetek megfelelését az elveknek. A változó szigorúságú szankciók skálája a jogvitát eldöntő szervek számára lehetővé teszi a nem teljesítés különböző fokozatainak megfelelő választ. A szankcióknak magukban kell foglalniuk a nem teljesítésre vonatkozó megállapítások közzétételét és bizonyos körülmények között az adatok törlésére vonatkozó követelményt ([2]). Más szankciók magukban foglalhatják a pecsét felfüggesztését és eltávolítását, az egyének ellentételezését a nem teljesítés következtében felmerült veszteségekért és a felfüggesztő végzéseket. A magánfelek jogvitáit eldöntő szerveknek és az önszabályozó szerveknek a szabályaikat megszegő „biztonságos kikötő" szervezetekről értesíteniük kell a megfelelő joghatósággal rendelkező kormányzati szervet vagy a bíróságokat – az esetnek megfelelően –, valamint értesíteniük kell a Kereskedelmi Minisztériumot (vagy az általa kijelölt szervet).

A Szövetségi Kereskedelmi Bizottság (FTC) fellépése

Az FTC elkötelezte magát az adatvédelmi önszabályozói szervezetektől – például a BBBOnline és a TRUSTe – és az EU tagállamaitól érkező, a „biztonságos kikötő" elvek nem teljesítését vélelmező megkeresések soron kívüli kivizsgálására, 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 oka(i) van(nak) azt hinni, hogy az 5. szakaszt megszegték, megoldhatja az ügyet a kifogásolt gyakorlatokat megtiltó, abbahagyásra kötelező közigazgatási utasítással, vagy panasz benyújtásával valamelyik szövetségi kerületi bírósághoz, amelynek az eredménye siker esetén az ugyanolyan irányú szövetségi bírósági végzés lehet. Az FTC az abbahagyásra kötelező közigazgatási utasítás megsértéséért polgári szankciókat eszközölhet ki, míg a szövetségi bírósági végzés megsértéséért polgári vagy bűnvádi engedetlenség címén indíthat pert. Az FTC értesíti a Kereskedelmi Minisztériumot bármilyen ilyen irányú fellépéséről. A Kereskedelmi Minisztérium arra ösztönzi az egyéb kormányzati szerveket, hogy értesítsék az ilyen megkeresésekre vonatkozó végleges intézkedésekről vagy a „biztonságos kikötő" elvekhez való csatlakozást meghatározó más döntésekről.

Ismétlődő nem teljesítés

Ha egy szervezet ismétlődően nem teljesíti az elveket, tovább már nem jogosult a „biztonságos kikötő" előnyeire. Ismétlődő nem teljesítés áll fenn, ha a szervezet, amely önmaga tanúsította megfelelését a Kereskedelmi Minisztériumnak (vagy az általa kijelölt szervnek), megtagadja valamely önszabályozó 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 Kereskedelmi Minisztériumot (vagy az általa kijelölt szervet) az ilyen tényekről. Ellenkező esetben a szervezet a hamis nyilatkozatokról szóló törvény (18 U. S. C. § 1001) alapján perelhető.

A minisztérium (vagy az általa kijelölt szerv) a „biztonságos kikötő" elvekhez való csatlakozást öntanúsító szervezetekről általa fenntartott nyilvános jegyzékben jelzi, ha ismétlődő nem teljesítésre vonatkozóan bármilyen tájékoztatást kap, akár magától a szervezettől, egy önszabályozó szervtől, vagy akár egy kormányzati szervtől, de csak azt követően, hogy a nem teljesítő szervezetnek harminc (30) napos határidőt és válaszadási lehetőséget biztosított. Ennek megfelelően a Kereskedelmi Minisztérium (vagy az általa kijelölt szerv) által fenntartott nyilvános jegyzékből világosan kiderül, hogy mely szervezetek részesülnek, és mely szervezetek nem részesülnek többé a „biztonságos kikötő" előnyeiből.

([1]) A jogvitákat eldöntő szerveknek nem kell megfelelniük a végrehajtási elvnek. Eltérhetnek az elvektől akkor is, ha adott feladataik végrehajtása során egymásnak ellentmondó kötelezettségekkel vagy kifejezett felhatalmazásokkal szembesülnek.

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

A „biztonságos kikötő” újraminősítés céljából egy önszabályozó szervben való részvételért folyamodó szervezetnek a „biztonságos kikötő”-ben való előző részvételéről teljes körűen tájékoztatnia kell az adott szervet.

12. GYFK – Választási lehetőség – A kizáró választás időzítése

K: *A választási lehetőség elve csak a kapcsolat kezdetekor vagy bármikor lehetővé teszi az egyén számára, hogy a választási lehetőséggel éljen?*

V: 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 kizárás érvénybeléptetésére. A szervezet ezenkívül megkövetelheti a kizárást kérő egyéntől az azonosság megállapításához elegendő információ szolgáltatását. Az Egyesült Államokban az egyének ezzel a választási lehetőséggel egy központi „kizárási” 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 „kizárási” 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.

Hasonlóképpen, a szervezet felhasználhatja az információt bizonyos közvetlen értékesítési célokra, olyankor, amikor a gyakorlatban kivitelezhetetlen az egyén számára a kizárási 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. GYFK – Utazással kapcsolatos információ

K: *A légi utasok helyfoglalása és más utazási információi, mint például a törzsutasprogramra vagy a szállodafoglalásra, illetve a különleges kiszolgálási igényekre, mint például a vallásos követelményeknek megfelelő ételekre vagy az esetleges fizikai segítségre vonatkozó információ mikor továbbítható az EU-n kívül található szervezetek részére?*

V: Az ilyen információ továbbítására különböző körülmények között kerülhet sor. Az irányelv 26. cikke alapján a „személyes adatok olyan harmadik országba irányuló továbbítása vagy továbbítássorozata, amely a 25. cikk (2) bekezdése értelmében nem biztosít megfelelő szintű védelmet”, csak a következő feltételek mellett történhet: (1) a továbbítás a fogyasztó által kért szolgáltatások biztosítása, vagy egy megállapodás, mint például a „törzsutasprogram” megállapodás feltételeinek teljesítése érdekében szükséges; vagy (2) a fogyasztó egyértelműen hozzájárulását adta. Az Egyesült Államokban a „biztonságos kikötő”-höz 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 a „biztonságos kikötő” a különleges információk tekintetében különleges szabályokat tartalmaz, az ilyen információt (amelynek összegyűjtésére például a vásárlók fizikai segítségre vonatkozó igényeivel összefüggésben lehet szükség) a „biztonságos kikötő” résztvevői számára történő továbbítások magukban foglalhatják. Az információt továbbító szervezetnek azonban minden esetben tiszteletben kell tartania annak az EU-tagállamnak a jogszabályait, amelyben működik, amelyek többek között különleges feltételeket írhatnak elő a különleges adatok kezelésére vonatkozóan.

14. GYFK – Gyógyszeripari és gyógyászati termékek

1. K: *Ha a személyes adatokat az Európai Unióban gyűjtik össze és gyógyszeripari kutatásra és/vagy más célokból az Egyesült Államokba továbbítják, a tagállam jogszabályait vagy a „biztonságos kikötő” elveket kell alkalmazni?*

1. V: A személyes adatok összegyűjtésére és bármilyen, az Egyesült Államokba történő továbbítást megelőző feldolgozására a tagállami jogszabályokat kell alkalmazni. Amint azokat továbbították az Egyesült Államokba, az adatokra a „biztonságos kikötő” elvek vonatkoznak. A gyógyszeripari kutatásra és más célokra használt adatokat adott esetben anonimizálni kell.

2. K: *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 „biztonságos kikötő”-ben levő szervezetéhez továbbítják, felhasználhatja-e a szervezet az adatokat egy új tudományos kutatási tevékenységhez?*

2. V: Igen, 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. 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 az adatokat eredetileg gyűjtötték, vagy amelyekhez az egyén utóbb hozzájárult, ismét kérni kell a beleegyezését.

3. K: *Mi történik a személy adataival, ha a résztvevő saját elhatározásából vagy a támogató kérésére visszalép a klinikai kísérlettől?*

3. V: A résztvevők bármikor dönthetnek a klinikai kísérletből való visszalépés mellett, illetve felkérhetők a visszalépésre. A visszalépést megelőzően gyűjtött adatokat a klinikai kísérlet részeként gyűjtött más adatokkal együtt még fel lehet dolgozni, de csak abban az esetben, ha ezt az értesítésben egyértelműen a résztvevő tudtára adták, amikor beleegyezett a részvételbe.

4. K: *A gyógyszeripari és orvostechnikai eszközt gyártó vállalkozások számára megengedett, hogy az Egyesült Államok szabályozó hatóságai számára szabályozói 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 engedélyeznek-e hasonló továbbításokat?*

4. V: Igen, az értesítés és választási lehetőség elveivel összhangban.

5. K: *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 kísérletekben részt vevők a kísérlet során hozzáférnek-e a kezelésükre vonatkozó adatokhoz?*

5. V: Nem, ilyen hozzáférést nem kell biztosítani a résztvevő számára, ha ezt a korlátozást elmagyarázták, amikor a résztvevő belépett a kísérletbe, és az ilyen információ felfedése veszélyeztetné a kutatás integritását. 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 vállalkozástól.

6. K: *A gyógyszeripari vagy orvostechnikai eszközt gyártó vállalkozásnak alkalmaznia kell-e a „biztonságos kikötő" elveket az értesítésre, a választási lehetőségre, az adattovábbításra harmadik személynek, és a hozzáférésre vonatkozóan a termékbiztonságot és -hatékonyságot ellenőrző tevékenységeiben, beleértve a negatív események jelentését és a bizonyos gyógyszereket vagy orvostechnikai eszközöket (pl. szívritmusszabályzót) használó betegek/alanyok megfigyelését?*

6. V: Nem, amennyiben az elvek betartása akadályozza a szabályozói 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.

7. K: *A kutatási adatokat a kutatás vezetője egyedülálló 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 a 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 a személyes adatok „biztonságos kikötő" elvek alá tartozó továbbítását képezi?*

7. V: Nem, ez nem képezi személyes adatok olyan továbbítását, amelyre az elvek vonatkoznak.

15. GYFK – Nyilvános nyilvántartás és nyilvánosan hozzáférhető információ

K: *Az értesítés, választási lehetőség és az adattovábbítás harmadik félnek elvét szükséges-e a nyilvános nyilvántartásban lévő információra vagy a nyilvánosan hozzáférhető információra alkalmazni?*

V: Az értesítés, választási lehetőség és az adattovábbítás harmadik félnek 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 adattovábbítás harmadik félnek 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.

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 a „biztonságos kikötő” előnyeire.

III. MELLÉKLET

A „biztonságos kikötő" végrehajtásának áttekintése

Szövetségi és állami „tisztességtelen és megtévesztő gyakorlatok" hatáskör és adatvédelem

Ez a feljegyzés a Szövetségi Kereskedelmi Bizottságról szóló törvény (15 U. S. C. §§ 41-58., módosítva) 5. szakasza alapján behatárolja a Szövetségi Kereskedelmi Bizottság (FTC) arra vonatkozó illetékességét, hogy intézkedést hozzon azok ellen, akik állításaikkal és/vagy az erre irányuló kötelezettségvállalásaikkal ellentétben nem védik meg a személyes információ titkosságát. Tárgyalja továbbá az illetékesség alóli kivételeket, valamint az intézkedési jogosultsággal rendelkező más szövetségi és állami ügynökségeket is, ahol az FTC nem rendelkezik hatáskörrel ([1]).

Az FTC hatásköre tisztességtelen vagy megtévesztő gyakorlat esetén

A Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza kimondja, hogy a „tisztességtelen vagy megtévesztő cselekmények vagy gyakorlat a kereskedelemben vagy azt érintően" törvényellenesek. 15 U. S. C. § 45(a)(1). Az 5. szakasz teljes hatáskörrel ruházza fel az FTC-t az ilyen eljárások és gyakorlatok megakadályozására. 15 U. S. C. § 45(a)(2). Ennek megfelelően, az FTC hivatalos tárgyalás levezetésével abbahagyásra kötelező közigazgatási határozatot adhat ki a törvénysértő magatartás megszüntetése érdekében. 15 U. S. C. § 45(b). Ha a közérdek úgy kívánja, az FTC ideiglenes korlátozó rendelkezést vagy ideiglenes vagy állandó végzést is kérhet az Egyesült Államok kerületi bíróságán. 15 U. S. C. § 53(b). Olyan esetekben, amikor a tisztességtelen vagy megtévesztő eljárások vagy gyakorlat széles körben elterjedt, vagy amennyiben már abbahagyásra kötelező közigazgatási határozatokat adott ki a tárgyban, az FTC az adott cselekményekre vagy gyakorlatokra vonatkozó közigazgatási szabályt léptethet érvénybe. 15 U. S. C. § 57a.

Aki nem tesz eleget az FTC-rendeletnek, 11 000 USD-ig terjedő polgári bírsággal sújtható, és a folyamatos szabálysértés esetén minden nap külön szabálysértésnek minősül ([2]). 15 U. S. C. § 45(1). Hasonlóképpen bárki, aki valamely FTC-szabályt tudatosan megszegi, minden megszegésért 11 000 USD polgári bírsággal sújtható. 15 U. S. C. § 45.(m). Végrehajtási intézkedéseket vagy az Igazságügyi Minisztérium, vagy – ha az visszautasítja – az FTC hozhat. 15 bU. S. C. § 56.

Az FTC hatásköre és az adatvédelem

Az 5. szakasz szerinti hatáskörének gyakorlásában az FTC azon az álláspontonvan, hogy annak hamis beállítása, hogy miért gyűjtik az információt a fogyasztóktól, vagy hogy azt hogyan használják fel, megtévesztő gyakorlatnak minősül ([3]). 1998-ban például az FTC panaszt nyújtott be a GeoCities ellen, mivel az a honlapján korábban gyűjtött információt harmadik félnek üzletszerzés céljából felfedte, előzetes engedély nélkül, és ezzel ellenkező állítása ellenére ([4]). Az FTC munkatársai azt is megerősítették, hogy a gyermekekre vonatkozó személyes információ gyűjtése, és ezen információ értékesítése és nyilvánosságra hozatala a szülők hozzájárulása nélkül valószínűleg szintén tisztességtelen gyakorlatnak minősül ([5]).

([1]) Itt nem tárgyaljuk az összes különféle szövetségi jogszabályt, amely sajátos összefüggésekben foglalkoznak az adatvédelemmel, illetve az állami jogszabályokat és szokásjogot, amelyek alkalmazandók lehetnek. A személyes információ kereskedelmi összegyűjtését és felhasználását szabályozó szövetségi szintű jogszabályok többek között a következők: a kábel távközlési politikáról szóló törvény (47 U. S. C. §551), a gépjárművezetők adatainak védelméről szóló törvény (18 U. S. C. § 2721), az elektronikus távközlési adatvédelmi törvény (18 U. S. C. § 2701 et seq.), az elektronikus pénzátutalási törvény (15 U. S. C. §§ 1693, 1693 m), a tisztességes hitelinformációról szóló törvény (15 U. S. C. § 1681 et seq.), a pénzügyi adatok védelméről szóló törvény (12 U. S. C. § 3401 et seq.), a telefonos fogyasztóvédelmi törvény (47 U. S. C. § 227) és a videokölcsönzési adatok védelméről szóló törvény (18 U. S. C. § 2710). Sok államban hasonló jogszabályok vannak ezeken a területeken. Lásd pl. Mass. Gen. Laws ch. 167B, §16 (amely megtiltja a pénzintézeteknek az ügyfél pénzügyi nyilvántartásainak felfedését harmadik fél előtt az ügyfél beleegyezése vagy törvényes eljárás nélkül), N. Y. Pub. Health Law § 17 (amely korlátozza orvosi vagy mentális egészségügyi nyilvántartások felhasználását és nyilvánosságra hozatalát és betegek számára ahhoz hozzáférési jogot ad).

([2]) Ilyen keresetben az Egyesült Államok kerületi bírósága az FTC végzés végrehajtása érdekében megfelelő elrendelő és méltányos kártérítést is elrendelhet. 15 U. S. C. § 45(1)

([3]) A „megtévesztő gyakorlatot" olyan állításként, mulasztásként vagy gyakorlatként határozzák meg, amely alkalmas arra, hogy jelentős mértékben félrevezesse az értelmes fogyasztókat.

([4]) Lásd:www. FTC.gov/opa/1998/9808/geocitie.htm

([5]) Lásd a Center for Media Educationhöz küldött személyzeti levelet, www.ftc.gov/os/1997/9707/cenmed.htm. Ezen túlmenően, a gyermekek személyiségi jogainak online védelméről szóló 1998. évi törvény az FTC-t külön jogkörrel ruházza fel, hogy szabályozza a gyermekekre vonatkozó személyes információk weboldal- és onlineszolgáltatás-üzemeltetők általi gyűjtését. Lásd 15 U. S. C. §§ 6501-6506. A törvény különösen megköveteli az online üzemeltetőktől, hogy a gyermekekre vonatkozó személyes információ gyűjtése, felhasználása vagy nyilvánosságra hozatala előtt értesítsék a szülőket, és tőlük ellenőrizhető beleegyezést szerezzenek. Id., § 6502(b). A törvény a szülők számára is megadja a hozzáférés jogát és az információ folytatódó felhasználására vonatkozó engedély megtagadásának jogát. Id.

John Mogghoz, az Európai Bizottság főigazgatójához intézett levelében Pitofsky, az FTC elnöke megjegyezte, hogy az FTC adatvédelemre vonatkozó hatásköre korlátozott, amennyiben nincs hamis közlés (vagy egyáltalán nincs közlés) arra vonatkozóan, hogy az összegyűjtött információkat hogyan használják fel. Pitofsky FTC-elnök levele John Mogg részére (1998. szeptember 23.). Azoknak a vállalkozásoknak azonban, amelyek élni kívánnak a javasolt „biztonságos kikötő" - vel, tanúsítaniuk kell, hogy az előírt iránymutatásokkal összhangban megvédik az összegyűjtött információt. Következésképpen, amennyiben egy vállalkozás tanúsítja, hogy biztosítja az információ titkosságát, és utána mégsem így tesz, az 5. szakasz értelmében eljárása hamis közlésnek és „megtévesztő gyakorlatnak" minősül.

Mivel az FTC hatásköre a „kereskedelmi vagy azt érintő" tisztességtelen vagy megtévesztő eljárásokra vagy gyakorlatra terjed ki, az FTC nem rendelkezik joghatósággal a nem kereskedelmi célokra összegyűjtött és felhasznált személyes információ tekintetében, például jótékonysági alap létrehozása esetén. *Lásd* Pitofsky levelét, 3. o. A személyes információ bármilyen kereskedelmi ügyletben történő felhasználása azonban eleget tesz ennek az illetékességi feltételnek. Így például, ha egy munkaadó a munkavállalóira vonatkozó személyes információt közvetlen piaci üzletszerzéssel foglalkozó vállalkozás számára értékesíti, az ügylet az 5. szakasz rendelkezései alá tartozik.

Az 5. szakasz szerinti kivételek

Az 5. szakasz meghatározza az FTC tisztességtelen vagy megtévesztő eljárásokra vagy gyakorlatra vonatkozó hatásköre alóli kivételeket a következők tekintetében:

– pénzintézetek, beleértve a bankokat, a takarék- és hitelintézeteket, és a hitelszövetkezeteket,

– távközlési és államok közötti szállítási fuvarozó vállalkozások,

– légi fuvarozók, és

– konzervgyár- és vágóhíd-üzemeltetők.

Lásd 15 U. S. C. § 45(a)(2). A következőkben az egyes kivételeket és az ezekre vonatkozó szabályozói hatáskört tárgyaljuk.

Pénzintézetek ([1])

Az első kivétel a 18(f)(3) [15 U. S. C. § 57a(f)(3)] szakaszban leírt bankokra, takarék- és hitelintézetekre és a 18(f)(4) [15 U. S. C. § 57a(f)(4)] szakaszban leírt szövetségi hitelszövetkezetekre vonatkozik ([2]). Ezek a pénzintézetek külön-külön inkább a Federal Reserve Board (szövetségi jegybanki tanács), az Office of Thrift Supervision (takarékbetét felügyelet hivatala) ([3]) és a National Credit Union Administration Board (nemzeti hitelszövetkezet vagyonkezelő igazgatóság) által kiadott szabályozások hatálya alá tartoznak. Lásd 15 U. S. C. § 57a(f). Ezeket a szabályozó ügynökségeket utasították az e pénzintézetek tisztességtelen és megtévesztő gyakorlatának megakadályozásához szükséges szabályozások előírására ([4]) és a fogyasztói panaszokat kezelő különálló részleg létrehozására. 15 U. S. C. § 57a(f)(1). Végül, a végrehajtási hatáskör a bankokra és takarék- és hitelintézetekre a szövetségi betétbiztosításról szóló törvény 8. szakaszából (12 U. S. C. § 1818), és a szövetségi hitelszövetkezetekre a szövetségi hitelszövetkezetről szóló törvény 120. és 206. szakaszából ered. 15 U. S. C. § 57a(f)(2)–(4).

Bár a biztosítási üzletág nem szerepel kifejezetten az 5. szakasz kivételeinek jegyzékében, a McCarran–Ferguson-törvény (15 U. S. C. § 1011 *et seq.*) a biztosítási üzletág szabályozását általában az egyes államokra bízza ([5]). Ezenkívül a McCarran–Ferguson-törvény 2(b) szakasza alapján egyetlen szövetségi törvény sem

([1]) 1999. november 12-én Clinton elnök aláírta a Gramm–Leach–Bliley-törvényt (közzétéve L. 106-102, törvénybe iktatás száma: 15 U. S. C. § 6801 et seq.). A törvény korlátozza az ügyfeleikre vonatkozó személyes információ nyilvánosságra hozatalát a pénzintézetek által. A törvény megköveteli, hogy a pénzintézetek – többek között – értesítsék az összes ügyfelet adatvédelmi politikáikról és gyakorlataikról a személyes információ fiókintézetekkel és nem fiókintézetekkel történő megosztása tekintetében. A törvény felhatalmazza az FTC-t, a szövetségi bankfelügyeleteket és más hatóságokat a jogszabály által megkövetelt adatvédelem végrehajtására vonatkozó előírások közzétételére. Az ügynökségek e célból szabályozási javaslatokat adnak ki.

([2]) Feltételei értelmében ez a kivétel nem vonatkozik az értékpapír-ágazatra. Ezért a brókerek, a kereskedők és mások az értékpapír üzletágban a Securities and Exchange Commission (Értékpapír- és Tőzsdei Bizottság) és az FTC párhuzamos hatásköre alá tartoznak a tisztességtelen vagy megtévesztő cselekedetek és gyakorlat tekintetében.

([3]) Az 5. szakaszban meghatározott kivétel eredetileg a Federal Home Loan Bank Boardra (Szövetségi Lakáshitel-intézetek Igazgatósága) vonatkozott, amelyet 1989 augusztusában a pénzintézetek reformjáról, behajtásról és végrehajtásról szóló 1989. évi törvény megszüntetett. Hivatali hatásköreit az Office of Thrift Supervision (Takarék- és Hitelfelügyeleti Hivatal) és a Resolution Trust Corporation (Befektetési Alapot Kezelő Társaság), a Federal Deposit Insurance Corporation (Szövetségi Betétbiztosítási Intézet) és a Housing Finance Board (Lakásépítési Pénzügyi Igazgatóság) vette át.

([4]) Miközben kivonja a pénzintézeteket az FTC hatásköre alól, az 5. szakasz azt is előírja, hogy amikor az FTC tisztességtelen vagy megtévesztő cselekményekre és gyakorlatra vonatkozó szabályt ad ki, a pénzügyi szabályozó igazgatóságoknak 60 napon belül ezzel párhuzamosan szabályozásokat kell kiadniuk. Lásd 15 U. S. C. 57a(f)(1).

([5]) „A biztosítási üzletág és minden azzal foglalkozó személy a különböző államok azon törvényei alá tartozik, amelyek az ilyen üzlet szabályozására vagy adóztatására vonatkoznak." 15 U. S. C. § 1012(a).

érvényteleníti, csorbítja vagy váltja fel az állami szabályozást, „hacsak az ilyen törvény nem kifejezetten a biztosítási üzletágra vonatkozik". 15 U. S. C. § 1012(b). Az FTC törvény intézkedései azonban a biztosítási üzletágra „annyiban vonatkoznak, amennyiben az ilyen üzletágat az állami törvény nem szabályozza". *Id*. Azt is meg kell jegyezni, hogy a McCarran–Ferguson-törvény csak a biztosítási üzletág tekintetében enged szabad kezet az államoknak. Ezért az FTC fenntartja a fennmaradó hatáskörét a biztosító társaságok tisztességtelen vagy megtévesztő gyakorlata tekintetében, amikor nem a biztosítási üzletágban tevékenykednek. Ez magában foglalhatja például azt, amikor a biztosítók a biztosítottakra vonatkozó személyes információkat értékesítenek nem biztosítási termékek közvetlen piaci értékesítésével foglalkozó szakemberek számára ([1]).

Közhasznú fuvarozó vállalkozások

Az 5. szakasz második kivétele azokra a közhasznú fuvarozó vállalkozásokra terjed ki, amelyek „a kereskedelmet szabályozó törvények alá tartoznak". 15 U. S. C. § 45(a)(2). Ebben az esetben a „kereskedelmet szabályozó törvények" az Egyesült Államok törvénykönyve 49. címének IV. alcímére és az 1934. évi távközlési törvényre utalnak (47 U. S. C. § 151. *et seq*.) (Távközlési Törvény). *Lásd* 15 U. S. C. § 44.

A 49 U. S. C., IV. alcím (államok közötti szállítás) magában foglalja a vasúti fuvarozókat, a közúti fuvarozókat, a vízi fuvarozókat, az alkuszokat, a teherszállítmányozókat és a csővezetéken keresztül fuvarozókat. 49 U. S. C. § 10101 *et seq*. Ezek a különféle közhasznú fuvarozók a Közlekedési Minisztériumon belül független ügynökség, a Surface Transportation Board (Felszíni Közlekedési Igazgatóság) szabályozása alá tartoznak. 49 U. S. C. § 10501, 13501 és 15301. A fuvarozó számára minden egyes esetben tilos az olyan, a rakománya jellegére, rendeltetési helyére és más szempontjaira vonatkozó információ felfedése, amelyeket a szállítmányozó sérelmére használhatnak fel. *Lásd* 49 U. S. C. § 11904, 14908 és 16103. Megjegyezzük, hogy ezek az intézkedések a szállítmányozó rakományára vonatkozó információra utalnak, és így látszólag nem terjednek ki a szállítmányozóra vonatkozó személyes információra, amely nem kapcsolódik a szóban forgó szállítmányhoz.

A távközlési törvény értelmében az „államok közötti és külkereskedelem a vezetékes és rádió távközlésben" szabályozását a Szövetségi Távközlési Bizottság (Federal Communications Commission – FCC) látja el. Lásd 47 U. S. C. §§ 151. és 152. A közhasznú távközlési adattovábbítási szolgáltató vállalkozásokon kívül a távközlési törvény olyan vállalkozásokra is vonatkozik, mint például a televíziós és rádiós műsorszóró vállalkozások, és olyan kábelszolgáltatókra, amelyek nem közhasznú fuvarozó vállalkozások. Mint olyanok, utóbbi vállalkozások az FTC törvény 5. szakasza alapján nem minősülnek kivételnek. Így az FTC hatáskörrel rendelkezik e vállalkozások esetleges tisztességtelen és megtévesztő gyakorlatának vizsgálatára, míg az FCC párhuzamos joghatósággal bír független hatáskörének érvényesítésére ezen a területen, az alább leírtaknak megfelelően.

A távközlési törvény alapján „minden távközlési adattovábbítási vállalkozásnak", beleértve a helyi adatátviteli központokat, kötelessége megvédeni az ügyfél saját információjának titkosságát ([2]). 47 U. S. C. § 222(a). Ezen az általános adatvédelmi hatáskörön kívül a távközlési törvényt módosította a kábeltávközlési politikáról szóló 1984. évi törvény (a kábeltörvény), 47 U. S. C. § 521 *et seq*., amely kifejezetten kötelezővé teszi a kábelüzemeltetők részére, hogy a kábel-előfizetőkre vonatkozó „személyes azonosításra alkalmas információ" titkosságát megvédjék. 47 U. S. C. § 551. ([3]) A kábeltörvény korlátozza a személyes információ a kábelüzemeltető általi gyűjtését, és megköveteli, hogy a kábelüzemeltető értesítse az előfizetőt az összegyűjtött információ természetéről és jövőbeni felhasználásáról. A kábeltörvény megadja az előfizetőknek a róluk szóló információkba való betekintés jogát, és előírja, hogy a kábelüzemeltetők semmisítsék meg az információkat, ha azokra a továbbiakban már nincs szükség.

A távközlési törvény feljogosítja az FCC-t, hogy vagy saját kezdeményezésére vagy külső panaszra reagálva végrehajtsa ezt a két adatvédelmi intézkedést ([4]). 47 U. S. C. 205, 403; *id*. § 208. Ha az FCC megállapítja, hogy a távközlési adattovábbító (beleértve a kábelüzemeltetőt) megszegte a 222. vagy 551. szakasz adatvédelmi rendelkezéseit, három

---

([1]) Az FTC különböző összefüggésekben gyakorolt hatáskört a biztosítótársaságok felett. Egy esetben az FTC megtévesztő hirdetés miatt pert indított egy cég ellen egy olyan államban, amelyben számára nem engedélyezték az üzleti tevékenységet. Az FTC illetékességét azon az alapon hagyták helyben, hogy nem volt hatékony állami szabályozás, mert a cég ténylegesen az állam hatáskörén kívül esett. Lásd FTC v. Travelers Health Association, 362 U. S. 293 (1960).
Ami az államokat illeti, 17 elfogadta a biztosítási megbízottak nemzeti egyesülete (NAIC) által elkészített „biztosítási információról és adatok védelméről szóló" mintatörvényt. A törvény az értesítésre, a felhasználásra és nyilvánosságra hozatalra, valamint a hozzáférésre vonatkozó rendelkezéseket tartalmaz. Szintén majdnem az összes állam elfogadta a NAIC „tisztességtelen biztosítási gyakorlatokról szóló törvény" modelljét, amely kifejezetten a tisztességtelen kereskedelmi gyakorlatra vonatkozik a biztosítási üzletágban.

([2]) Az „ügyféltulajdonú hálózati információ" kifejezés olyan információt jelent, amely az ügyfél által használt „távközlési szolgáltatás mennyiségére, műszaki összeállítására, típusára, rendeltetési helyére és a használat összegére", valamint távbeszélő számlázási információra vonatkozik. 47 U. S. C. 222(f)(1). Ez a kifejezés azonban nem tartalmazza az előfizetői jegyzék információt. Id.

([3]) A jogszabály nem határozza meg kifejezetten a „személyes azonosításra alkalmas információt".

([4]) Ez az illetékesség felöleli az adatvédelem megsértéséért a kárpótláshoz való jogot a távközlési törvény 222. szakasza alapján, vagy kábel-előfizetőkre vonatkozóan, a törvényt módosító kábeltörvény 551. szakasza alapján egyaránt. Lásd még 47 U. S. C. 551(f)(3) („a kábel-előfizető számára rendelkezésre álló bármely más törvényes jogorvoslaton kívül" a polgári per a szövetségi kerületi bíróságon egy nem kizárólagosan felkínált jogorvoslat).

alapvető eljárással élhet. Először, a jogsértés megvizsgálása és meghatározása után, a Bizottság elrendelheti, hogy az adattovábbító vállalkozás fizessen a *pénzügyi károkért* [1]. 47 U. S. C. 209. Másik megoldásként az FCC utasíthatja az adattovábbító vállalkozást, hogy *hagyjon fel* a jogsértő gyakorlattal vagy mulasztással. 47 U. S. C. § 205(a). Végül, a Bizottság arra is utasíthatja a jogsértő adattovábbító vállalkozást, hogy „*alkalmazzon és tartson be [minden olyan] előírást vagy gyakorlatot*", amelyet az FCC előír. *Id*.

Azok a magánszemélyek, akik úgy gondolják, hogy a távközlési adattovábbító vagy a kábelüzemeltető vállalkozás megszegte a távközlési törvény vagy a kábeltörvény vonatkozó rendelkezéseit, panaszt tehetnek az FCC-nél, vagy benyújthatják kereseteiket a szövetségi kerületi bírósághoz. 47 U. S. C. § 207. Annak a panaszosnak, aki a szövetségi bíróságnál a távközlési adattovábbító vállalkozással szemben a távközlési törvény 222. szakaszának szélesebb értelmében a fogyasztói adatvédelem elmulasztásában indított keresetben megnyeri a pert, a tényleges károsszeget és az ügyvéd díjának megtérítését ítélhetik meg. 47 U. S. C. § 206. Annak a panaszosnak, aki a kábeltörvény kábelre vonatkozó 551. szakasza alapján a személyiségi jog megsértése miatt indít pert, a tényleges kártérítésen és a jogi képviselők díján kívül büntető kártérítést és az indokolt perköltség megtérítését is megítélhetik. 47 U. S. C. § 551(f).

Az FCC részletes szabályokat fogadott el a 222. szakasz végrehajtására. Lásd a CFR 47. cím 64.2001-2009. A szabályok különös jogi biztosítékokat határoznak meg az ügyféltulajdonú hálózati információhoz való illetéktelen hozzáférés ellen. A szabályzat megköveteli a távközlési adattovábbítóktól, hogy:

– szoftverrendszereket fejlesszenek ki és vezessenek be, amelyek „jelzik" a fogyasztó értesítési/jóváhagyási állapotát, amikor az ügyfélszolgálati nyilvántartás először megjelenik a képernyőn,

– elektronikus „ellenőrzési nyomvonalat" tartsanak fenn a vásárló nyilvántartásához való hozzáférés követése céljából, beleértve azt is, hogy a fogyasztó nyilvántartását ki és milyen céllal nyitotta meg,

– képezzék ki személyzetüket az ügyféltulajdonú hálózati információ engedélyezett felhasználására, a megfelelő fegyelmi eljárásokkal,

– hozzanak létre felügyeleti felülvizsgálati eljárást a megfelelés biztosítására, amikor kimenő értékesítést folytatnak, és

– éves alapon igazolják az FCC-nek, hogyan teljesítik ezeket az előírásokat.

Légi fuvarozók

Az Egyesült Államok és a külföldi országok légi fuvarozói, amelyek az 1958. évi szövetségi légügyi törvény hatálya alá tartoznak, szintén mentesülnek az FTC törvény 5. szakasza alól. Lásd 15 U. S. C. § 45(a)(2). Ez magában foglal bárkit, aki áruk vagy utasok államok közötti vagy külföldi szállítását végzi, vagy aki postai küldeményeket repülőgépen fuvaroz. Lásd 49 U. S. C. § 40102. A légi fuvarozók a Közlekedési Minisztérium hatásköre alá tartoznak. Ebben a tekintetben a közlekedési miniszter rendelkezik hatáskörrel, hogy intézkedést hozzon „a tisztességtelen, megtévesztő, erőszakos vagy versenyellenes légi szállítási gyakorlatok megelőzésére". 49 U. S. C. § 40101(a)(9). Ha a közérdek úgy kívánja, a közlekedési miniszter kivizsgálhatja, hogy az Egyesült Államok vagy külföldi ország légi fuvarozója vagy jegyügynöke tisztességtelen vagy megtévesztő gyakorlatot folytat-e. 49 U. S. C. § 41712. Meghallgatás után a közlekedési miniszter utasítást adhat ki a jogellenes gyakorlat beszüntetésére. *Id*. Tudomásunk szerint, a közlekedési miniszter nem gyakorolta ezt az hatáskört a légitársaságok ügyfeleire vonatkozó személyes információ titkosságának megvédése ügyében [2].

A személyes információ titkosságának megvédésére két rendelkezés létezik, amelyek a légi fuvarozókra sajátos összefüggésekben vonatkoznak. Először, a szövetségi légügyi törvény megvédi a repülőgép-vezetői állásra jelentkezők adatainak védelmét. *Lásd* 49 U. S. C. § 44936(f). Miközben lehetővé teszi a légi fuvarozók számára, hogy hozzájussanak a kérvényező személyi iratanyagához, a törvény biztosítja a kérelmezőnek a jogot, hogy értesítést kapjon az iratanyag kéréséről, és ahhoz beleegyezését adja, a pontatlanságokat kijavítsa és az iratanyag kiadását csak a foglalkoztatásra vonatkozó döntésben érintettek számára engedélyezze. Másodszor, a DOT (Közlekedési Minisztérium) rendeletei előírják a légi katasztrófa esetén kormányzati felhasználásra összegyűjtött utaslistaadatok „bizalmas kezelését, amely csak az Egyesült Államok Külügyminisztériuma, az országos szállítási igazgatóság (az NTSB kérésére) (Nemzeti Közlekedés-biztonsági Felügyelet) és az Egyesült Államok Közlekedési Minisztériuma részére adható ki". 14 CFR 243. rész, § 243.9(c) (kiegészíti: FR 63., 8258).

---

(1) A panaszos közvetlen kárának hiánya azonban nem jogalap a panasz elutasítására. 47 U. S. C. § 208(a).

(2) Úgy tudjuk, hogy az iparágon belül vannak folyamatban lévő erőfeszítések az adatvédelmi kérdés megoldására. Az iparág képviselői megtárgyalták a javasolt „biztonságos kikötő" alapelveket és lehetséges alkalmazásukat a légi fuvarozók tekintetében. A megbeszélés egy iparági adatvédelmi politika elfogadására irányuló javaslatot tartalmazott, amely szerint a részt vevő cégek magukat kifejezetten a DOT illetékességének vetnék alá.

Konzervgyártók és vágóhidak

Tekintettel a konzervgyártásról és vágóhidakról szóló 1921. évi törvényre (7 U. S. C. § 181. *et seq.*), a törvény megtiltja minden konzervgyártónak az élőállat-állomány, húsok, hústermékek vagy feldolgozatlan állati termékek tekintetében, illetve az élőbaromfi-kereskedőknek bármilyen élő baromfi tekintetében, hogy tisztességtelen, igazságtalanul megkülönböztető vagy megtévesztő gyakorlatot folytasson vagy ilyen eszközt használjon. 7 U. S. C. § 192.(a); lásd még 7 U. S. C. § 213(a) (amely megtiltja a „tisztességtelen, igazságtalanul megkülönböztető vagy megtévesztő gyakorlatot vagy eszközt" az állatállománnyal összefüggésben). A mezőgazdasági miniszter elsődlegesen ezen intézkedések végrehajtásáért felelős, ugyanakkor az FTC hatásköre megmarad a kiskereskedelmi és baromfiipart érintő ügyletek esetében. 7 U. S. C. § 227(b)(2).

Nem világos, hogy a mezőgazdasági miniszter „megtévesztő" gyakorlatként értelmezi-e a konzervgyártásról és vágóhidakról szóló törvény alapján, ha a konzervgyárak vagy vágóhidak nem felelnek meg a személyes adatok védelme tekintetében kinyilvánított politikájuknak. Az 5. szakaszban meghatározott kivétel azonban csak annyiban vonatkozik a személyekre, társulásokra vagy vállalkozásokra, „amennyiben azok a konzervgyártásról és vágóhidakról szóló törvény hatálya alá tartoznak". Ezért ha a személyes adatok védelmét a konzervgyártásról és vágóhidakról szóló törvény rendelkező része nem tartalmazza, akkor az 5. szakaszban meghatározott kivétel semmiképpen nem érvényes, és a konzervgyárak és vágóhidak ebben a tekintetben az FTC hatásköre alá tartoznak.

A „tisztességtelen és megtévesztő gyakorlat" esetében hatáskörrel rendelkező állami hatóságok

Az FTC munkatársai által elkészített elemzésnek megfelelően „mind az 50 állam, valamint Washington szövetségi főváros, Guam, Puerto Rico és Egyesült Államok Virgin-szigetek a Szövetségi Kereskedelmi Bizottságról szóló törvényhez (" FTCA „) többé-kevésbé hasonló törvényeket rendeltek el, hogy megakadályozzák a tisztességtelen vagy megtévesztő kereskedelmi gyakorlatokat. FTC-adatlap:" Fogyasztóvédelmi megjegyzések: A tisztességtelen és megtévesztő gyakorlatokról szóló állami törvények gyakorlati hatékonysága „(Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation), *Tul. 59., L. Rev. 427*(1984). Minden esetben valamely végrehajtási ügynökség rendelkezik hatáskörrel" vizsgálatok folytatására idézések vagy polgári jogi vizsgálati felszólítások alkalmazásával, az önkéntes teljesítés tanúsító okiratainak beszerzésére, abbahagyásra kötelező közigazgatási határozatok kiadására vagy a tisztességtelen, lelkiismeretlen vagy megtévesztő kereskedelmi gyakorlatok alkalmazását megelőző bírósági határozatok kérésére. *Id.* 46 állam joga lehetővé teszi magánkeresetek indítását tényleges, kétszeres, háromszoros vagy büntető kártérítésre vonatkozóan, és néhány esetben, a költségek és ügyvédi díjak megtérítésére. *Id.*

Florida „megtévesztő és tisztességtelen kereskedelmi gyakorlatokról" szóló törvénye például felhatalmazza a főállamügyészt, hogy kivizsgálja a „tisztességtelen versenymódszerek, tisztességtelen, lelkiismeretlen vagy megtévesztő kereskedelmi gyakorlatát" és keresetet indítson, beleértve a hamis vagy megtévesztő reklámot, félrevezető franchise vagy üzleti lehetőségeket, csalárd távértékesítést és piramisrendszereket. Lásd még: N. Y. General Business Law (általános üzlet törvény) § 349 (amely tiltja az üzletmenet során végrehajtott tisztességtelen eljárásokat és megtévesztő gyakorlatot).

A főállamügyészek nemzeti szövetségének (National Association of Attorneys General – NAAG) ez évi vizsgálata megerősíti ezeket a megállapításokat. A választ adó 43 állam mindegyike rendelkezik „mini-FTC" törvényekkel vagy más, hasonló védelmet biztosító jogszabályokkal. Szintén az NAAG-vizsgálat szerint 39 állam jelezte, hogy rendelkeznek a nem letelepedett személyek panaszainak kivizsgálására vonatkozó illetékességgel. Különösen a fogyasztói adatvédelem tekintetében, a választ adó 41 államból 37 azt jelezte, hogy válaszol az azt állító panaszokra, hogy az illetékességük alá tartozó vállalkozás nem tartotta be az önmaga által bejelentett adatvédelmi politikáját.

IV. MELLÉKLET

Kártérítés az adatvédelmi jog megsértése esetén, jogi meghatalmazások, egyesítés és átvétel az amerikai jogban

Ez a fejezet választ ad arra a kérdésre, amelyben az Európai Bizottság kérte az amerikai jog tisztázását a következők tekintetében: a) kártérítési igény az adatvédelem megsértése miatt; b) „kifejezett meghatalmazások" az amerikai jogban a személyes információnak a „biztonságos kikötő" elvekkel ellentétes felhasználására; és c) az egyesülés és az átvétel hatása a „biztonságos kikötő" elvek alapján vállalt kötelezettségekre.

A. **Kártérítés az adatvédelem sérelme esetén**

A „biztonságos kikötő" elvek nem teljesítése az adott körülményektől függően számos magánkeresetnek adhat alapot. A „biztonságos kikötő" szervezetek különösen hamis közlésért vonhatók felelősségre, hogy a bejelentett adatvédelmi politikáikat nem tartják be. A szokásjog alapján is lehet indítani magánkeresetet kártérítésre, a személyiségi jogok (a magánélet) megsértése miatt. Az adatvédelemre vonatkozó számos szövetségi és állami jogszabály szintén rendelkezik kártérítésről magánszemélyek részére jogsértés esetén.

A kártérítésre való jog személyiségi jogok megsértése esetén jól megalapozott az Egyesült Államokban érvényes szokásjog alapján.

A személyes információ a „biztonságos kikötő" elvekkel ellentétes felhasználása számos különböző jogelmélet alapján hozhat létre jogszabályon alapuló kötelezettséget. Például mind az adattovábbító adatkezelő, mind az érintett magánszemély perelheti azt a „biztonságos kikötő" szervezetet, amely nem tartja tiszteletben a „biztonságos kikötő" kötelezettségvállalásait a hamis közlésre vonatkozóan. A Restatement of the Law, Second, Tort (A második jogszabály-összefoglaló, károkozások [1]) alapján:

> Az a személy, aki csalárd módon tényre, véleményre, szándékra vagy a jogra vonatkozóan tudatosan hamis közlést tesz, azzal a céllal, hogy egy másik személyt rávegyen arra, hogy erre támaszkodva cselekedjen vagy tartózkodjon a cselekvéstől, ezzel a személlyel szemben csalárd megtévesztés miatt felelős az anyagi veszteségért, amit ennek a személynek okozott, azzal, hogy az indokoltan támaszkodott a hamis közlésre.

Restatement, § 525. A hamis közlés akkor „csalárd", ha annak tudatában vagy abban a hitben tették, hogy hamis. *Id.* § 526. Általános szabályként, az a személy, aki csalárd módon hamis közlést tesz, azzal a személlyel szemben, akivel a hamis közlést elhiteti vagy el akarja hitetni, felelős lehet minden anyagi veszteségért, amit az illető emiatt elszenved. *Id.* 531. Ezenkívül az a fél, aki mással csalárd módon hamis közlést közöl, felelős egy harmadik féllel szemben is, amennyiben a törvényellenes cselekmény elkövetője számít arra, illetve elvárja, hogy hamis közlését megismétlik a harmadik fél felé, és az ezt követően annak megfelelően cselekszik. *Id.* § 533.

A „biztonságos kikötő"-vel összefüggésben a megfelelő közlés a szervezet arra irányuló nyilvános nyilatkozata, hogy tartja magát a „biztonságos kikötő" elvekhez. Ilyen kötelezettségvállalás esetén az elvek tudatos be nem tartása jogalapot adhat hamis közlésre vonatkozó keresetre azok részéről, akik a hamis állításra támaszkodtak. Mivel az elvekhez való ragaszkodásra vonatkozó kötelezettségvállalást a nyilvánosság felé tették meg, azok az egyének, akik ilyen információ alanyai, valamint az az európai adatkezelő, amely személyes információt továbbít az egyesült államokbeli szervezetnek, kereseti jogalapokkal rendelkezhet az egyesült államokbeli szervezet ellen hamis állítás miatt [2]. Ezenfelül az egyesült államokbeli szervezet marad felelős irányukba az „ismétlődő hamis állításra" vonatkozóan addig, amíg hátrányukra a hamis állításra támaszkodnak. Restatement, § 535.

---

[1] Második jogszabály-összefoglaló – Magánjogi jogsértések; American Law Institute (1997).

[2] Ez az eset állhat fenn például akkor, ha az egyének az egyesült államokbeli szervezet „biztonságos kikötő" – re vonatkozó kötelezettségvállalására támaszkodva adták beleegyezésüket az adatkezelőnek személyes adataik továbbításához az Egyesült Államokba.

Azok, akik egy csalárd hamis állításra támaszkodnak, kártérítésre jogosultak. A Restatement értelmében:

> A csalárd hamis állítás címzettje jogosult a csalás elkövetője elleni kártérítési keresetében a számára okozott olyan pénzbeli veszteség behajtására, amelynek a törvényes oka a hamis állítás.

Restatement, 549. A megengedhető kártérítés tartalmazza a tényleges készkiadási veszteséget, valamint a kereskedelmi ügylet „üzleti hasznának" elmaradását. *Id*.; *lásd pl*. Boling kontra Tennessee State Bank, 890 S. W.2d 32 (1994) (a bank a hitelfelvevőkkel szemben 14 825 USD tényleges kár megtérítésére kötelezett a hitelfelvevők személyes adatainak és üzleti terveinek felfedéséért a bankelnök előtt, akinek ellentétes érdekei voltak).

Bár a csalárd hamis állításhoz vagy az állítás hamisságának a tényleges ismerete, vagy legalább az arról való meggyőződés szükséges, a gondatlan hamis közlés is felelősségre vonáshoz vezethet. A Restatement értelmében, aki üzleti tevékenysége, hivatása vagy munkaviszonya során vagy bármilyen pénzügyletben hamis nyilatkozatot tesz, felelősségre vonható, „ha nem tanúsít kellő gondosságot vagy szakértelmet az információ megszerzése vagy közlése során". Restatement, § 552(1). A csalárd hamis állításokkal ellentétben a gondatlan hamis állításra vonatkozó kártérítés a készkiadási veszteségre korlátozódik. *Id*., § 552B (1).

Egy nemrég lefolytatott eljárásban például Connecticut állam legfelsőbb bírósága úgy vélte, hogy az a tény, hogy egy áramszolgáltató vállalkozás nem adott tájékoztatást az ügyfelek befizetéseiről nemzeti hitelintézetek számára, hamis közlésre vonatkozó kereseti jogalapot képez. Lásd Brouillard kontra United Illuminating Co., 1999 Conn. Super. LEXIS 1754. Ebben az eljárásban a felperes követelését elutasították, mert az alperes a számla dátumát követő harminc napon belül nem teljesített fizetéseket „elkésettként" jelentette. A felperes azt állította, hogy nem tájékoztatták erről a politikáról, amikor alperesnél az áramszolgáltatás kifizetésére lakossági folyószámlát nyitott. A bíróság kifejezetten úgy ítélte meg, hogy „a gondatlan hamis közlésre vonatkozó kereset alapulhat az alperes nyilatkozattételének elmaradásán, ha az erre kötelezett." Ez az eset is azt jelzi, hogy a tudatos vagy csalárd szándék nem szükségszerű eleme a gondatlan hamis állításra vonatkozó kereseti jogalapnak. Így az az egyesült államokbeli szervezet, amely gondatlanul elmulasztja teljes mértékben nyilvánosságra hozni, hogy miként fogja felhasználni a „biztonságos kikötő" alapján fogadott személyes információt, hamis állításért felelősségre vonható.

Amennyiben a „biztonságos kikötő" alapelveinek megsértése személyes információval történő visszaéléssel jár, ez az érintettnek a személyiségi jogainak (magánéletének) megsértése miatti károkozás tárgyában a szokásjog alapján indított keresetét is alátámasztaná. Az amerikai jog régóta elismeri a magánélet megsértésére vonatkozó kereseti jogalapokat. Egy 1905-ös ügyben ([1]) Georgia állam legfelsőbb bírósága elismerte a magánélet védelmének jogát, amely a természetes jog és a szokásjog rendelkezéseiben gyökerezik, egy magánállampolgár számára, akinek a fényképét tudta és beleegyezése nélkül egy életbiztosító egy reklámhirdetésben illusztrációként használta fel. A bíróság a magánélet védelemére vonatkozó amerikai jogtudományban ma már megszokott álláspontra helyezkedve úgy ítélte meg, hogy a fénykép felhasználása „rossz szándékú" és „helytelen" volt, és arra irányult, hogy „a felperest köznevetség tárgyává tegye" ([2]). A *Pavesich* határozat alapjai, jelentéktelen eltérésekkel, e témában az amerikai jog alapjává váltak. Az egyes államok bíróságai a személyiségi jogok megsértése esetében a kereseti jogalapokat következetesen támogatták, és most legalább 48 szövetségi állam bíróságilag elismer néhányat az ilyen kereseti jogalapok közül ([3]). Ezenfelül legalább 12 szövetségi állam rendelkezik alkotmányos rendelkezésekkel a polgárai magánéletének tolakodó cselekményekkel szembeni védelmére ([4]), ahol is ez a védelem néhány esetben a személyiségi jogok nem kormányzati szervek általi megsértésére is kiterjedhet. *Lásd pl.:* Hill kontra NCAA, 865 P.2d 633 (Ca. 1994); lásd még S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the age of the Internet, 34 S. D. L. Rev. 1153 (1997). („Néhány állam alkotmánya a magánélet olyan jogi védelmét tartalmazza, amely felülmúlja az Egyesült Államok alkotmányában meghatározott, a magánélet tiszteletben tartásához való jogra alapozott védelmet. Alaszka, Arizona, Kalifornia, Florida, Hawaii, Illinois, Louisiana, Montana, Dél-Karolina, és Washington a magánélet szélesebb körű védelmével rendelkezik.")

A Second Restatement of Torts (A magánjogi jogsértések második jogszabály-összefoglalója) ezen a területen mérvadó jogi áttekintést nyújt. A szokásos bírói gyakorlat bemutatásával a Restatement elmagyarázza, hogy a „magánélethez való jog" négy elkülönült kereseti jogalapot ölel fel az ebbe a kategóriába tartozó károkozásokra. Lásd: Restatement, § 652A. Először, a „betolakodás"-ra vonatkozó kereseti jogalap megállhat egy alperessel szemben, aki szándékosan, testileg vagy más módon beleavatkozik a másik személy magányába vagy visszavonultságába, illetve annak magánügyeibe vagy érdekeltségébe ([5]). Másodszor a „jogtalan felhasználás" esete akkor állhat fenn, ha valaki más nevét

([1]) Pavesich kontra New England Life Ins. Co. 50. S. E. 68 (Ga. 1905).

([2]) Id., a 69.-nél.

([3]) A WESTLAW adatbázis elektronikus kutatása 2 703 bejelentett, állami bíróságokhoz benyújtott, személyiségi jogvédelemre vonatkozó polgári peres esetet talált 1995 óta. Előzőleg átadtuk e vizsgálat eredményeit a Bizottságnak.

([4]) Lásd pl. a következő államok alkotmányát: Alaszka 1. cikk 22. szakasz; Arizona 2. cikk 8. szakasz; Kalifornia 1. cikk 1. szakasz; Florida 1. cikk 23. szakasz; Hawaii 1. cikk 5. szakasz; Illinois 1. cikk 6. szakasz; Louisiana 1. cikk 5. szakasz; Montana 2. cikk 10. szakasz; New York 1. cikk 12. szakasz; Pennsylvania 1. cikk 1. szakasz; Dél-Carolina 1. cikk 10. szakasz és Washington 1. cikk 7. szakasz.

([5]) Id., 28. fejezet, 62B szakasz.

vagy hasonlóságát saját céljára vagy saját hasznára használja fel (1). Harmadszor a „magánadatok nyilvánosságra hozatala" perelhető, ha a nyilvánosságra hozott ügy, természeténél fogva egy átlagember számára kifejezetten sértő, és jogszerűen nem tartozik a nyilvánosságra (2). Végül, a „nyilvánosan hamis színben való feltüntetés"-ért a kereset akkor helytálló, ha az alperes egy másik személyt tudatosan vagy nemtörődöm módon hamis színben tüntet fel a nyilvánosság előtt, és ez egy átlagember számára kifejezetten sértő (3).

A „biztonságos kikötő" alapelveinek keretrendszerével összefüggésben, a „betolakodás" magában foglalhatja a személyes információ jogosulatlan összegyűjtését, míg a személyes információ kereskedelmi célokra történő illetéktelen felhasználása a jogtalan felhasználás címén adhat keresetre alapot. Hasonlóképpen, a pontatlan személyes információ felfedése a „nyilvánosan hamis színben való feltüntetés" alapján alapozza meg a keresetet, ha az információ megfelel az „átlagember számára kifejezetten sértő" kritériumnak. Végezetül a magánélet megsértése, amely érzékeny személyes információ felfedéséből származik, a „magánadatok nyilvánosságra hozatala" címén teremtheti meg a kereseti jogalapot. (Lásd alább a szemléltető példákat.)

A károkozás tekintetében a személyiségi jogok megsértése a sértett fél számára a következő esetekben adja meg a kártérítés jogát:

a) a sértett fél személyiségi jogainak megsértéséből eredő érdeksérelme;

b) a sértett fél bizonyítottan elszenvedett lelki sérelme, ha az olyan jellegű, amely ilyen jogsértésből rendesen származhat; és

c) különleges kár, amelynek jogalapja a jogsértés.

Restatement, § 652H. Tekintve a magánjogi jogsértésekre vonatkozó szabályok általános alkalmazhatóságát és a személyiségi jogi érdekek különböző szempontjaira vonatkozó kereseti jogalapok sokféleségét, a pénzügyi kártérítés valószínűleg rendelkezésre áll azok számára, akik személyiségi jogi érdekeik sérelmét szenvedik el a „biztonságos kikötő" elvek be nem tartása következtében.

Valóban, az államok bíróságai előtt nagy számban vannak olyan ügyek, amelyekben a személyiségi jogok megsértését vélelmezik hasonló helyzetekben. Az *Ex Parte* AmSouth Bancorporation *et al*., 717 So. 2d 357, ügy például egy csoport nevében indított keresetet tartalmaz, amelyben azt állították, hogy az alperes „kihasználta a bankban elhelyezett bizalmi letéteket, bankbetétesekre és számláikra vonatkozó bizalmas információk kiadásával", lehetővé téve a bank fiókintézetének, hogy kölcsönös pénzalapokat és más befektetéseket értékesítsenek. A kártérítést az ilyen esetekben gyakran megítélik. A Vassiliades kontra Garfinckel's, Brooks Bros ügyben, 492 A.2d 580 (D. C. App. 1985), a fellebbviteli bíróság megváltoztatta az elsőfokú bíróság ítéletét, arra az álláspontra helyezkedve, hogy a felperes plasztikai műtét „előtti" és „utáni" fényképének felhasználása egy nagyáruházban megrendezett bemutató során a személyiségi jogok megsértését valósította meg a magánadatok közzététele alapján. A Candebat kontra Flanagan esetben, 487 So. 2d 207(Miss. 1986) az alperes biztosítótársaság egy reklámkampányban felhasznált egy balesetet, amelyben a felperes felesége súlyos sérüléseket szenvedett. A felperes pert indított a magánéletének megsértése címén. A bíróság úgy ítélt, hogy a felperes a neki okozott érzelmi szenvedésért és személyazonosságának felhasználásáért kártérítésre jogosult. A jogellenes felhasználásra vonatkozó keresetek akkor is fenntarthatók, ha a felperes nem híres személy. *Lásd pl*.: Staruski kontra Continental Telephone Co., 154 Vt. 568(1990) (az alperesnek kereskedelmi haszna származott a munkavállaló nevének és fényképének újsághirdetésben való felhasználásából). A Pulla kontra Amoco Oil Co., 882 F. Supp. 836 (S. D Iowa 1995) ügyben, a munkaadó beavatkozott a felperes munkavállaló magánéletébe azáltal, hogy egy másik alkalmazottal lenyomoztatta annak hitelkártya-nyilvántartásait, betegszabadságának ellenőrzése céljából. A bíróság helybenhagyta az esküdtek ítéletét, amely 2 USD tényleges kártérítést és 500 000 USD büntető kártérítést ítélt meg. Egy másik munkaadót azért vontak felelősségre, mert a vállalkozás újságjában közzétett egy történetet egy olyan alkalmazottról, akit személyi iratanyagának állítólagos meghamisítása miatt elbocsátottak. *Lásd* Zinda kontra Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis. App. 1987). A történet magántermészetű ügy közzétételével megsértette a felperes személyiségi jogait, mivel az újságot a közösségben terjesztették. Végezetül egy főiskolát, amely a hallgatókon HIV-teszteket végzett, azt állítva nekik, hogy a vérvizsgálat csak rubeolára vonatkozik, magánéletbe való jogtalan betolakodás miatt vontak felelősségre. *Lásd* Doe kontra High-Tech Institute, Inc., 972 P.2d 1060 (Colo. App. 1998). (A további jelentett esetekre vonatkozóan *lásd* az Restatement, § 652H, függelék.)

Az Egyesült Államokat gyakran bírálják azért, hogy túlságosan sok a peres eljárás, de ez egyszersmind azt is jelenti, hogy a magánszemélyek ténylegesen érvényt szerezhetnek a törvényes jogorvoslatnak – és meg is teszik –, ha úgy vélik, hogy hátrány érte őket. Az Egyesült Államok igazságszolgáltatási rendszere sok szempontból megkönnyíti a

(1) Id., 28. fejezet, 652C szakasz.
(2) Id., 28. fejezet, 652D szakasz.
(3) Id., 28. fejezet, 652E szakasz.

felperesek számára kereset benyújtását, akár egyénileg, akár egy csoport nevében. Az ügyvédi kamara, amely nagyobb, mint a legtöbb más országban, könnyen elérhető szakmai képviseletet biztosít. A „felperesek jogtanácsosa", aki magánszemélyeket magánkeresetekben képviseli, tipikusan részesedési alapon dolgozik, ezáltal lehetővé téve még a szegény vagy rossz anyagi körülmények között élő felperesek számára is, hogy jogorvoslatot keressenek. Ez fontos tényezőre mutat rá – az Egyesült Államokban jellemzően mindkét fél fedezi saját ügyvédeinek díját és más költségeket. Ez ellenkezik azzal az Európában uralkodó szabállyal, amely szerint a vesztes félnek meg kell térítenie a másik fél költségeit. A két rendszer viszonylagos érdemeinek vitatása nélkül, az Egyesült Államok szabálya valószínűleg kevésbé riasztja el azokat a magánszemélyeket a kereset indításától, akik nem lennének képesek mindkét fél költségeinek megtérítésére, ha veszítenének.

Magánszemélyek kárpótlásért pert indíthatnak még akkor is, ha követeléseik viszonylag kismértékűek. Az Egyesült Államok legtöbb, ha nem az összes államának igazságszolgáltatási rendszerében vannak az úgynevezett „kis ügyek" bíróságai, amelyek egyszerűsített, kevésbé költséges eljárásokkal döntenek a törvényes határokat meg nem haladó jogvitákban ([1]). A büntető kártérítés lehetősége pénzbeli térítést is kínál azon egyének számára, akik csekély közvetlen sérelmet szenvedtek ahhoz, hogy elítélendő meg nem engedett magatartás miatt pert indítsanak. Végül, azok a magánszemélyek, akik ugyanolyan módon szenvedtek sérelmet, egyesíthetik forrásaikat és követeléseiket, hogy közös polgári peres eljárást indítsanak.

Jó példa magánszemélyek kártérítés célú perindítási lehetőségére az Amazon.com ellen indított függő jogvita a személyiségi jogok megsértéséért. Az Amazon.com, a nagy online kereskedelmi vállalkozás ellen közös kereset indult, amelyben a felperesek azt állítják, hogy őket nem tájékoztatták arról, ilyenformán nem is adták beleegyezésüket a rájuk vonatkozó személyes információ gyűjtéséhez, amikor az Amazon tulajdonában lévő, „Alexa" nevű szoftverprogramot használták. Az esetben a felperesek a tárolt üzeneteihez való jogtalan hozzáférés miatt a számítógépes csalásról és visszaélésről szóló törvény megsértését, és az elektronikus és vezetékes kommunikációjuk jogellenes lehallgatása miatt az elektronikus hírközlés titkosságáról szóló törvény megsértését állították. A szokásjog alapján a magánéletük megsértése miatt is perelnek. Ez egy internetbiztonsági szakértő által decemberben benyújtott panaszból származik. A pert indítók személyenként 1 000 USD kártérítést és az ügyvédi díj, valamint a jogsértés eredményeként elért haszon megfizetését kérik. Tekintettel arra, hogy a közös keresetben részt vevők száma milliós nagyságrendű lehet, a kártérítés összege több milliárd dollárra rúghat. Az FTC is vizsgálja a vádakat.

A szövetségi és állami adatvédelmi törvény gyakran magánkereseti jogalapokat biztosít a pénzbeli kártérítésre.

A magánjogi jogsértésekre vonatkozó törvényi szabályokon alapuló polgári jogi felelősségen kívül a „biztonságos kikötő" elvek nem teljesítése a több száz szövetségi és állami adatvédelmi törvény valamelyikét is megszegheti. Ezek a törvények, amelyek a személyes információ kezelését tárgyalják mind az állami, mind a magánszektorban, sok esetben lehetővé teszik magánszemélyek számára kártérítési per indítását jogsértés esetén. Például:

Az 1986. évi törvény az elektronikus hírközlés titkosságáról (ECPA). Az ECPA megtiltja a mobiltelefon-beszélgetések és számítógépről számítógépre történő átvitelek illetéktelen lehallgatását. A jogsértések a jogsértés minden egyes napjára vonatkozóan legalább 100 USD polgári jogi kártérítési kötelezettséget eredményezhetnek. Az ECPA védelme a tárolt elektronikus közleményekhez való illetéktelen hozzáférésre és azok felfedésére is kiterjed. A jogsértők felelnek az okozott kárért, illetve a jogsértésből származó nyereség elkobozható.

Az 1996. évi távközlési törvény. A 702. szakasz alapján az ügyféltulajdonú hálózati információ (CPNI) a távközlési szolgáltatások nyújtásán kívül semmilyen más célra nem használható fel. A szolgáltatás előfizetői panaszt tehetnek a szövetségi távközlési bizottságnál, vagy pert indíthatnak a szövetségi kerületi bíróságon kártérítés és az ügyvédi díjak behajtása céljából.

A fogyasztói hitelinformáció jelentésének reformjáról szóló 1996. évi törvény. Az 1996. évi törvény módosította a tisztességes hitelinformációról szóló törvényt (FCRA) a hitelinformáció alanyai részére az értesítés és a hozzáférési jog továbbfejlesztése céljából. A reformtörvény a fogyasztói hitelinformáció viszonteladóira új korlátozásokat is bevezetett. A fogyasztók a jogsértésekért kártérítést és az ügyvédi díjakat hajthatják be.

([1]) Korábban tájékoztatást adtunk a Bizottság részére a kis összegű követelés keresetekről.

Az állami törvények számos területen szintén biztosítják a személyes adatok védelmét. Az államok intézkedést hoztak többek között a banki nyilvántartások, kábeltelevízió-előfizetések, hitelinformáció, munkaügyi nyilvántartások, kormányzati nyilvántartások, genetikai és egészségügyi nyilvántartások, biztosítási nyilvántartások, iskolai nyilvántartások, elektronikus közlemények és videokölcsönzések területén ([1]).

B. **Kifejezett, jogszabályon alapuló meghatalmazások**

A „biztonságos kikötő" elvek tartalmaznak egy kivételt, amennyiben a jogszabály, szabályozás vagy a precedensjog „ellentmondó kötelezettségeket vagy kifejezett meghatalmazásokat hoz létre, feltéve hogy a szervezet bármilyen ilyen meghatalmazás gyakorlása során ki tudja mutatni, hogy az elvek nem teljesítése arra a mértékre korlátozódik, ami az ilyen meghatalmazás által elősegített uralkodó jogos érdekeknek való megfeleléshez szükséges". Nyilvánvaló, hogy ahol az Egyesült Államok jogszabályai ellentmondó kötelezettségeket szabnak, az Egyesült Államok szervezeteinek – akár a „biztonságos kikötő"-ben, akár nem – be kell tartania a jogszabályokat. Ami a kifejezett meghatalmazásokat illeti – bár a „biztonságos kikötő" elvek célja a különbségek áthidalása az Egyesült Államok és Európa kormányzati rendszere között az adatvédelem tekintetében – tiszteletben kell tartanunk választott törvényhozóink jogalkotói előjogait. A „biztonságos kikötő" elvek szigorú betartása alóli korlátozott kivétel egyensúlyt próbál teremteni a jogos érdekek egyeztetésére mindkét oldalon.

A kivétel olyan esetekre korlátozódik, ahol kifejezett meghatalmazás van. Ezért kiindulásként a vonatkozó jogszabálynak, szabályozásnak vagy bírósági határozatoknak megerősítően engedélyeznie kell a „biztonságos kikötő" szervezetek kifejezett magatartását ([2]). Más szóval, a kivétel nem érvényes, amennyiben jogszabály nem rendelkezik erről. Ezen túlmenően, a kivétel csak akkor érvényes, ha a kifejezett meghatalmazás ellentétben áll a „biztonságos kikötő" elvek betartásával. Még abban az esetben is, a kivétel „az ilyen meghatalmazás által elősegített uralkodó jogos érdekeknek való megfeleléshez szükséges mértékre korlátozódik". Például ha jogszabály egyszerűen felhatalmaz egy vállalkozást, hogy személyes információt adjon át kormányzati hatóságoknak, a kivétel nem lenne érvényes. Ha ellenben a törvény kifejezetten felhatalmazza a vállalkozást, hogy személyes információt adjon át kormányzati ügynökségeknek a személy beleegyezése nélkül, ez „kifejezett meghatalmazást" jelent egy olyan eljárásra, amely ellentétes a „biztonságos kikötő" elvekkel. Viszont az értesítés és a hozzájárulás követelmények alóli egyedi kivételek a kivétel alá tartoznának (mivel az egyenértékű lenne a kifejezett meghatalmazással az információ előzetes értesítés és hozzájárulás nélküli felfedésére). Az olyan jogszabály például, amely engedélyezi az orvosok számára a betegeik egészségügyi adatainak közlését az egészségügyi hatóságokkal a betegek előzetes beleegyezése nélkül, kivételt tehet lehetővé az értesítési és választási lehetőség elvek alól. Ez a meghatalmazás nem engedélyezné az orvos számára ugyanazon egészségügyi adatok közlését egészségügyi üzemeltető szervezetekkel vagy kereskedelmi gyógyszerészeti kutatólaboratóriumokkal, amely túllépne a törvény által engedélyezett célokon, és ezért a kivételek körén kívül esne ([3]). A szóban forgó törvényes hatáskör lehet „egyszeri" meghatalmazás valamilyen művelet elvégzésére a személyes információval, de – ahogyan az alábbi példák mutatják – ez rendszerint kivétel a személyes információ gyűjtését, felhasználását vagy nyilvánosságra hozatalát tiltó jogi szabályok alól.

Az 1996. évi távközlési törvény

A legtöbb esetben az engedélyezett felhasználások vagy összhangban vannak az irányelv és az elvek követelményeivel, vagy azokat az engedélyezett kivételek valamelyike engedélyezné. Például a távközlési törvény 702. szakasza (törvénybe iktatva 47 U. S. C. § 222) kötelezi a távközlési adatátviteli szolgáltatókat az ügyfeleik számára nyújtott szolgáltatások során birtokukba jutott személyes információ titkosságának megőrzésére. Ez az intézkedés kifejezetten megengedi a távközlési adattovábbítási szolgáltatók számára, hogy:

1. ügyfél-információt használjanak fel távközlési szolgáltatás nyújtására, beleértve az előfizetői névjegyzékek közzétételét;

2. az ügyfél írásos kérésére mások számára ügyfél-információt adjanak; és

3. ügyfél-információt adjanak összesített formában.

([1]) A WESTLAW adatbázis közelmúltban történt elektronikus kutatása 994 kártérítésre és a magánélet megsértésére vonatkozó jelentett állami esetet tárt fel.

([2]) A tisztázás céljából, a vonatkozó törvényes hatóságnak nem kell kifejezetten hivatkoznia a „biztonságos kikötő" elvekre.

([3]) Hasonlóképpen, ebben a példában az orvos nem támaszkodhatna a törvényes felhatalmazásra, hogy érvénytelenítse az egyénnek a 12. GYFK által előírt, a közvetlen üzletszerzésből kizárásra vonatkozó választási lehetőségét. A „kifejezett felhatalmazás" alóli kivétel hatálya szükségszerűen a felhatalmazás tárgyára korlátozódik a vonatkozó jogszabályok alapján.

Lásd 47 U. S. C.§ 222(c)(1)–(3). A törvény a távközlési adattovábbítási szolgáltatók számára kivételt is megenged, hogy az ügyfél-információt felhasználják:

1. szolgáltatásaik bevezetésére, nyújtására, számlázására és díj beszedésére;

2. védekezésre a csalárd, sértő vagy jogellenes magatartással szemben; és

3. telemarketing-, közvetítő- vagy ügyviteli szolgáltatás nyújtására az ügyfél által kezdeményezett beszélgetés folyamán ([1]).

Id., § 222(d)(1)–(3). Végül, a távközlési adattovábbítási szolgáltatóknak a telefonkönyv-kiadók részére biztosítaniuk kell az előfizetők jegyzékét, amely csak a neveket, címeket, telefonszámokat és kereskedelmi ügyfelek esetében az üzletágat tartalmazhatja. *Id.*, § 222(e).

A „kifejezett meghatalmazások" kivétel akkor érvényesülhet, ha a távközlési adattovábbítási szolgáltató a CPNI-t csalás vagy más jogellenes magatartás megakadályozására használja. Még itt is, az ilyen intézkedések „közérdekű" – nek minősülhetnek, és ezért ezeket az elvek engedélyezhetik.

Az Egészségügyi és Szociális Minisztérium által javasolt szabályok

Az Egészségügyi és Szociális Minisztérium (HHS) szabályokat javasolt az egyedileg azonosítható egészségügyi információ adatvédelmi szabványai tekintetében. *Lásd* 64 Fed. Reg. 59.918 (1999. november 2.) (törvénybe iktatandó 45 C. F. R. 160-164. pont alatt). A szabályok végrehajtanák az egészségbiztosítás hordozhatóságáról és elszámolási kötelezettségéről szóló 1996. évi törvény adatvédelemre vonatkozó követelményeit, kiad. L. 104-191. A javasolt szabályok általában megtiltanák, hogy az érintett jogi személyek (pl. egészségügyi tervek, egészséggondozási elszámolási helyek és olyan egészségügyi szolgáltatók, amelyek egészségügyi információt továbbítanak elektronikus formában) védett egészségügyi információt használjanak fel vagy adjanak át egyedi meghatalmazás nélkül. *Lásd* a javasolt 45 C. F. R. §164.506. A javasolt szabályok a védett egészségügyi információ felfedését csak két célra követelnék meg: 1. hogy magánszemélyek betekinthessenek a róluk szóló egészségügyi információkba, és arról másolatot készíthessenek, *lásd id.* §164.514; és 2. hogy a szabályokat végrehajtsák, *lásd id.* §164.522.

A javasolt szabályok engedélyeznék a védett egészségügyi információk felhasználását vagy átadását, az egyén külön felhatalmazása nélkül, korlátozott körülmények között. Ilyen körülmények például az egészségügyi rendszer ellenőrzése, a bűnüldözés és a szükséghelyzetek. *Lásd id.* §164.510. A javasolt szabályok részletesen megállapítják az ezekre a felhasználásokra és adattovábbításokra vonatkozó korlátozásokat. Ezenfelül a védett egészségügyi információk engedélyezett felhasználását vagy közlését a szükséges legkisebb információmennyiségre korlátoznák. *Lásd id.* §164.506.

A javasolt szabályozások által kifejezetten engedélyezett megengedő felhasználások általában összhangban vannak a „biztonságos kikötő" elvekkel, vagy azokat más kivétel másképpen engedi meg. A jogérvényesítés és a bírósági eljárás során engedélyezett, miként az orvosi kutatás is. Más felhasználások, mint például az egészségügyi ellátó rendszer ellenőrzése, a közegészségügyi feladatok és az állami egészségügyi adatrendszerek, a közérdeket szolgálják. Az adatátvitelre az egészségügyi kifizetések és támogatások kezeléséhez szükség van az egészségügyi szolgáltatás nyújtása érdekében. A felhasználás szükséghelyzetben – a legközelebbi hozzátartozóval a kezelésre vonatkozó konzultáció céljából, ha „a beteg beleegyezése gyakorlatilag vagy ésszerűen nem szerezhető meg", vagy az elhunyt személyazonosságának vagy a halál okának meghatározására – megvédi az érintett és mások létfontosságú érdekeit. Magánszemélyek aktív katonai szolgálatú és más különleges csoportjainak igazgatására vonatkozó felhasználások segítik a katonai feladat vagy hasonló válsághelyzetek megfelelő végrehajtását, és az ilyen felhasználások minden esetben általában kismértékben – vagy egyáltalán nem – érintik az ügyfeleket.

Ez csak azt engedi meg, hogy a személyes információt egészségügyi szervezetek a betegek névjegyzékeinek összeállítására használják fel. Bár az ilyen felhasználás nem éri el a „létfontosságú" érdek szintjét, a névjegyzékek hasznosak a betegek és barátaik, illetve rokonaik számára. Ezenkívül az ilyen engedélyezett felhasználás területe

([1]) E kivétel terjedelme nagyon korlátozott. Feltételei értelmében a távközlési adatátviteli szolgáltató a CPNI-t csak az ügyfél által kezdeményezett hívás folyamán használhatja fel. Ezenkívül az FCC arról tájékoztatott bennünket, hogy a távközlési adatátviteli szolgáltató nem használhatja fel a CPNI-t az ügyfél érdeklődését meghaladó piaci szolgáltatásokra. Végül, mivel az ügyfélnek jóvá kell hagynia a CPNI e célra történő felhasználását, ez a rendelkezés tulajdonképpen egyáltalán nem „kivétel".

eredendően korlátozott. Ezért az elvek alóli kivételre való támaszkodás a törvény által e célból kifejezetten engedélyezett felhasználással minimális veszélyt jelent a betegek személyiségi jogaira.

A tisztességes hitelinformációról szóló törvény

Az Európai Bizottság aggodalmát fejezte ki, hogy a „kifejezett meghatalmazások" kivétele „ténylegesen létrehozza a megfelelőség ténymegállapítását" a tisztességes hitelinformációról szóló törvényhez (FCRA). Ez nem fog megtörténni. A tisztességes hitelinformációról szóló törvény (FCRA) sajátos megfelelőségi ténymegállapítása hiányában, azoknak az egyesült államokbeli szervezeteknek, amelyek másként egy ilyen ténymegállapításra támaszkodnának, ígéretet kell tenniük arra, hogy minden tekintetben betartják a „biztonságos kikötő" elveit. Ez azt jelenti, hogy amennyiben az FCRA-követelmények túllépik az elvekben megfogalmazott védelmi szintet, az egyesült államokbeli szervezeteknek csak az FCRA-nak kell alávetniük magukat. Fordított esetben, amennyiben az FCRA kevésnek bizonyulna, akkor a fenti szervezeteknek tájékoztatási gyakorlataikat az elvekkel kell összhangba hozniuk. A kivétel nem módosítaná ezt az alapvető értékelést. Feltételei értelmében, a kivétel csak akkor érvényes, ha a vonatkozó törvény kifejezetten engedélyezi az olyan magatartást, amely összeegyeztethetetlen lenne a „biztonságos kikötő" elvekkel. A kivétel nem terjedne ki arra, ha az FCRA követelményei egyszerűen csak nem felelnek meg a „biztonságos kikötő" elveknek ([1]).

Más szóval, nem áll szándékunkban olyan értelmet rendelni a kivételhez, hogy amit nem követel meg, az ilyenformán „kifejezetten engedélyezve" van. Ezen túlmenően a kivétel csak akkor érvényes, amikor az, amit az Egyesült Államok joga kifejezetten engedélyez, ellenkezik a „biztonságos kikötő" elvek követelményeivel. A vonatkozó jognak e két elem mindegyikének meg kell felelnie, mielőtt az elvek nem teljesítését engedélyeznék.

Az FCRA 604. szakasza például kifejezetten engedélyezi a fogyasztói tájékoztató ügynökségek számára, hogy fogyasztói jelentéseket adjanak ki különféle, ott felsorolt helyzetekben. *Lásd* FCRA, §604. Ha ennek során a 604. szakasz engedélyezi a hitelinformációs ügynökségeknek, hogy a „biztonságos kikötő" elvekkel szemben járjanak el, akkor a hitelinformációs ügynökségeknek a kivételre kell támaszkodniuk (természetesen hacsak nem voltak érvényben más kivételek). A hitelinformációs ügynökségeknek alá kell vetniük magukat a bírósági határozatoknak és vádesküdtszéki idézéseknek, és a hitelbeszámolók felhasználása kormányzati engedélyezési, szociális és gyermektámogatási végrehajtási ügynökségek által közcélt szolgál. *Id.*, §604(a)(1), (3)(D) és (4). Következésképpen a hitelinformációs ügynökségnek nem kell a „kifejezett meghatalmazás" kivételére támaszkodnia ezekre a célokra. Ha a fogyasztó írásos utasításával összhangban jár el, a fogyasztói tájékoztató ügynökség teljes mértékben teljesíti a „biztonságos kikötő" elveket. Id., 604(a) (2) §. Hasonlóképpen, a fogyasztói jelentések foglalkoztatási célra csak a fogyasztó írásbeli meghatalmazásával szerezhetők be. (*id.*, §§604(a)(3)(B) és (b)(2)(A)(ii)), olyan hitel- vagy biztosítási ügyletekre vonatkozóan pedig, amelyeket nem a fogyasztó kezdeményezett, csak akkor, ha a fogyasztó nem zárta ki magát az ilyen kérelmezésekből (*id.*, 604(c)(1)(B)). Az FCRA továbbá tiltja a hitelinformációs ügynökségeknek orvosi információ kiadását foglalkoztatási célokra a fogyasztó beleegyezése nélkül. *Id.*, §604(g). Az ilyen felhasználások összeegyeztethetők az értesítési és választási lehetőség elvekkel. A 604. szakasz által engedélyezett más célok együtt járnak a fogyasztót érintő ügyletekkel, és ezért az elvek által engedélyezettek lehetnek. *Lásd id.*, §604(a)(3)(A) és(F).

A 604. szakasz által „engedélyezett" fennmaradó felhasználás a másodlagos hitelpiacokra vonatkozik. *Id.*, §604(a)(3)(E). A fogyasztói jelentések e célból történő felhasználása és a „biztonságos kikötő" elvek önmagukban még nem állnak ellentétben. Tény, hogy az FCRA nem követeli meg például a hitelinformációs ügynökségektől, hogy figyelmeztessék a fogyasztókat és a beleegyezésüket kérjék, amikor e célból jelentéseket adnak ki. Ismételten hangsúlyozzuk azonban azt, hogy egy követelmény hiánya nem jelent „kifejezett meghatalmazást" a követelménytől eltérő eljárásra. Hasonlóképpen, a 608. szakasz lehetővé teszi, hogy a hitelinformációs ügynökségek személyes információt adjanak ki kormányzati ügynökségeknek. Ez a „felhatalmazás" nem mentesíti a hitelinformációs ügynökséget, ha az figyelmen kívül hagyná a „biztonságos kikötő" elvek betartására vállalt kötelezettségét. Ez szemben áll más példáinkkal, ahol a megerősítő értesítés és a választási lehetőség követelményei alóli kivételek úgy működnek, hogy kifejezetten engedélyezik a személyes információ felhasználását értesítés és választási lehetőség nélkül.

Összefoglalás

E törvények még oly korlátozott áttekintéséből is kibontakozik egy pontosan érthető séma:

– A jogszabályban a „kifejezett meghatalmazás" általában engedélyezi a személyes információ felhasználását vagy nyilvánosságra hozatalát a személy előzetes beleegyezése nélkül; így a kivétel az értesítési és választási lehetőség elvekre korlátozódna.

([1]) A fenti eszmefuttatás nem tekintendő annak beismerésének, hogy az FCRA nem biztosít „megfelelő" védelmet. Az FCRA bármilyen megítélésekor a jogszabály által biztosított védelmet egészében kell tekintetbe venni, nem csak kivételekre összpontosítva, ahogy ebben az esetben mi tettük.

– A legtöbb esetben a jogszabály által engedélyezett kivételek részletesen meghatározottak, adott helyzetekben adott célokra. Minden esetben a jogszabály egyébként tiltja olyan személyes információ illetéktelen felhasználását vagy nyilvánosságra hozatalát, amely nem tartozik e korlátok közé.

– A legtöbb esetben, törvényhozói jellegét tükrözve, az engedélyezett felhasználás vagy adattovábbítás a közérdeket szolgál.

– Az engedélyezett felhasználás majdnem minden esetben vagy teljes mértékben összhangban van a „biztonságos kikötő" elvekkel, vagy más engedélyezett kivételek közé tartozik.

Végeredményben a „kifejezett meghatalmazásokra" vonatkozó kivétel, a törvényben, természeténél fogva, valószínűleg igen korlátozott hatályú lesz.

C. **Egyesülés és átvétel**

A 29. cikk szerinti munkacsoport aggodalmát fejezte ki az olyan helyzetekkel kapcsolatban, ahol a „biztonságos kikötő" alá tartozó szervezetet olyan vállalkozás vette át, illetve a szervezet olyan vállalkozásokkal egyesült, amely nem kötelezte magát a „biztonságos kikötő" elvek elfogadására. Úgy tűnik azonban, a munkacsoport feltételezte, hogy az átvevő vállalkozás nem lenne köteles a „biztonságos kikötő" elveket alkalmazni az átvett vállalkozás tulajdonában lévő személyes információra vonatkozóan, de az Egyesült Államok joga szerint nem szükségszerűen ez a helyzet. Az Egyesült Államokban az egyesüléssel és átvétellel kapcsolatban az általános szabály az, hogy az a vállalkozás, amelyik egy másik társaság kibocsátott részvényeit megszerzi, általában magára vállalja a megvásárolt vállalkozás kötelezettségeit és tartozásait. *Lásd 15 Fletcher Cyclopedia of the Law of Private Corporations* §7117 (1990); *lásd még Model Bus. Corp. Act* §11. 06 (3) (1979) (a megmaradó társaság viseli az egyesüléshez csatlakozó minden egyes fél összes kötelezettségét). Más szóval, a megmaradó vállalkozást, amely ezzel a módszerrel egy „biztonságos kikötő" szervezettel egyesül vagy olyat vesz át, az utóbbi „biztonságos kikötő" kötelezettségvállalásai kötelezik.

Ezenfelül, még akkor is, ha az egyesülés vagy átvétel a vagyontárgyak tulajdonszerzésén keresztül menne végbe, a megszerzett vállalkozás kötelezettségei bizonyos körülmények között mégis kötelezhetik a megszerző vállalkozást. 15 *Fletcher*, §7122. Még akkor is azonban, ha a kötelezettségek nem élnék túl az egyesülést, érdemes megjegyezni, hogy egy olyan egyesülést sem élnének túl, ha szerződés alapján adatokat továbbítanának Európából – amely a „biztonságos kikötő" egyetlen életképes alternatívája az Egyesült Államokba történő adatátvitelre. Ezen túlmenően, a „biztonságos kikötő" okiratok átdolgozott formájukban most megkövetelik bármely „biztonságos kikötő" szervezettől, hogy értesítsék a Kereskedelmi Minisztériumot bármilyen átvételről, és csak akkor engedélyezzék a további adatátvitelt a jogutód szervezet felé, ha a jogutód szervezet csatlakozik a „biztonságos kikötő"-höz. *Lásd 6. GYFK.* Az Egyesült Államok most valóban felülvizsgálta a „biztonságos kikötő" keretrendszert, hogy megkövetelje az egyesült államokbeli szervezetektől, hogy ilyen helyzetben töröljék a „biztonságos kikötő" keretében kapott információt, ha a „biztonságos kikötő"-re vonatkozó kötelezettségvállalásaik nem folytatódnak, vagy más megfelelő biztosítékokat nem vezetnek be.

V. MELLÉKLET

John Mogg
Igazgató, DG XV
Európai Bizottság
C 107–6/72 Iroda
Rue de la Loi/Wetstraat 200
B–1049 Brüsszel

2000. július 14.

Tisztelt Mogg úr!

Úgy értesültem, hogy a 2000. március 29-i levelemmel kapcsolatban számos kérdés merült fel. Annak érdekében, hogy egyértelművé tegyem a hatáskörünket a felmerült kérdésekhez kapcsolódó területeken, ezt a levelet küldöm, amely a további hivatkozások megkönnyítése érdekében a korábbi levelezést is kiegészíti, illetve összegzi.

Hivatalunkban tett látogatása alkalmával és levélváltásunkban számos kérdést vetett fel a United States Federal Trade Comission (Egyesült Államok Szövetségi Kereskedelmi Bizottsága) hatáskörével kapcsolatban az online adatvédelem terén. Hasznosnak tartom a korábbi válaszaim összefoglalását az FTC ezen a területen végzett tevékenységeire vonatkozóan, kiegészítve további információval az ügynökség hatásköréről a legutóbbi levelében említett fogyasztói adatvédelmi ügyekben. Konkrétan a következő kérdéseket tette fel: (1) hatáskörrel rendelkezik-e az FTC a foglalkozatással kapcsolatos adatok átadásának kérdésében, ha az átadás a „biztonságos kikötő" amerikai elveit sérti; (2) hatáskörrel rendelkezik-e az FTC a „bizalompecséttel" rendelkező nonprofit programok felett; (3) egyaránt érvényes-e az FTC-ről szóló törvény az offline és az online forgalomra; (4) mi történik, ha az FTC hatásköre átfedésbe kerül más végrehajtó hatóságéval?

Az FTC-ről szóló törvény alkalmazása az adatvédelemre

Mint tudja, az elmúlt öt év során az FTC vezető szerepet vállalt az amerikai ipari és fogyasztói csoportok arra irányuló erőfeszítéseinek elősegítésében, hogy átfogó választ adjanak a fogyasztói adatvédelmi kérdésekre, beleértve a személyes információ az interneten keresztül történő gyűjtését és felhasználását. Nyilvános műhelymunkák és az iparág tagjaival, fogyasztói képviselőkkel és a Kereskedelmi Minisztériumban és az Egyesült Államok kormányában dolgozó kollégáinkkal folytatott folyamatos konzultáció révén segítettünk a kulcsfontosságú politikai kérdések meghatározásában és ésszerű megoldások kifejlesztésében.

A Szövetségi Kereskedelmi Bizottság jogi illetékességét ezen a területen a Szövetségi Kereskedelmi Bizottságról szóló törvény („FTC törvény") 5. szakasza szabályozza, amely tiltja a „tisztességtelen vagy félrevezető cselekményeket vagy gyakorlatot" a kereskedelemben vagy azt érintően [1]. A félrevezető gyakorlatot úgy határozza meg, hogy az olyan nyilatkozat, mulasztás vagy gyakorlat, amely jelentős mértékben félre tudja vezetni az értelmes fogyasztót. Tisztességtelen a gyakorlat, ha a felhasználónak jelentős kárt okoz, vagy valószínűleg okozhat, ami ésszerűen nem elkerülhető, és a fogyasztót vagy a versenyt kiegyenlítő előnyökkel nem kárpótolja [2].

Bizonyos információgyűjtési gyakorlatok megsérthetik az FTC törvényt. Ha például egy honlap tévesen azt állítja, hogy megfelel egy kinyilvánított adatvédelmi politikának vagy önszabályozási iránymutatásnak, a FTC törvény 5. szakasza jogalapot biztosít, hogy az ilyenfajta hamis nyilatkozat – mint félrevezető – kifogásolható legyen. Ezen elv megalapozására valóban sikeresen hajtottuk végre a törvényt [3]. Ezen túlmenően a Bizottság arra az álláspontra helyezkedett, hogy a különösen súlyos adatvédelmi gyakorlatot az 5. szakasz értelmében tisztességtelenként üldözi, amennyiben az gyerekekkel vagy rendkívül érzékeny adatokkal – pl. pénzügyi beszámolók [4] vagy orvosi adatok – kapcsolatos. A Szövetségi Kereskedelmi Bizottság a múltban is élt ilyen jogérvényesítési intézkedésekkel, és ezt megteszi a jövőben is, saját aktív ellenőrzési és vizsgáló tevékenységünkön, illetve az olyan eseteken keresztül, amelyekre önszabályozó szervek és más szervek, köztük az Európai Unió tagállamai hívják fel figyelmét.

---

(1) 15 U. S. C. § 45. A tisztességes hitelinformációról szóló törvény szintén vonatkozna az internetes adatgyűjtésre és értékesítésre, amennyiben megfelelnek a törvényileg meghatározott „fogyasztói jelentés" és „fogyasztói tájékoztatási ügynökség" fogalmának.

(2) 15 U. S. C. § 45(n).

(3) Lásd GeoCities, Docket No. C-3849 (jogerős végzés 1999. feb. 12.) (a www.ftc.gov/os/1999/9902/9823015d %26o.htm honlapon); Liberty Financial Cos., Docket No. C-3891 (jogerős végzés 1999. aug. 12.) (a www.ftc.gov/opa/1999/9905/young investor.htm honlapon). Lásd még a Children's Online Privacy Protection Act Rule (COPPA – Gyermekek személyes adatainak online védelméről szóló törvény), 16 C. F. R. 312. rész (a www.ftc.gov/opa/1999/9910/childfinal.htm honlapon). A COPPA törvény, amely a múlt hónapban lépett hatályba, megköveteli a 13 évnél fiatalabb gyermekeknek szóló vagy ismerten 13 évnél fiatalabb gyermekek személyes adatait gyűjtő weboldalak üzemeltetőitől, hogy bevezessék a tisztességes információgyűjtési gyakorlatnak a törvényben megfogalmazott normáit.

(4) Lásd FTC kontra Touch Tone, Inc., 99-WM-783 számú polgári per (D. Co.) (benyújtva 1999. április 21-én) a www.ftc.gov/opa/1999/9904/touchtone.htm honlapon. Staff Opinion Letter, 1997. július 17., válaszul a Center for Media Education által benyújtott petícióra a www.ftc.gov/os/1997/9707/cenmed.htm honlapon.

FTC-támogatás az önszabályozásnak

Az FTC hosszú ideje támogatja az ipar azon erőfeszítéseit, hogy hatékony önszabályozói programokat fejlesszen ki az interneten a fogyasztók adatvédelmének biztosítása érdekében. Ezen erőfeszítések sikerességéhez azonban az iparág tagjainak széles körű részvételére van szükség. Ugyanakkor az önszabályozásnak a jogérvényesítésre kell támaszkodnia. Az FTC ezért az önszabályozói iránymutatásoknak való megfelelés a BBBOnline, a TRUSTe és hasonló szervezetek által bejelentett eseteit kiemelten fogja kezelni. Ez az eljárás összhangban lenne a Better Business Bureau-nál (Üzletmenet-fejlesztési Hivatal) működő, National Advertising Review Boardhoz (NARB – Nemzeti Reklámfelügyeleti Testület) fűződő sokéves kapcsolatunkkal is, amely a reklámmal kapcsolatos panaszokat az FTC-hez irányítja. A NARB-n belül a National Advertising Division (NAD) (Nemzeti Reklámosztály) döntőbírói eljárással szabályozza a belföldi reklámmal kapcsolatos panaszokat. Ha valamelyik fél elutasítja a NAD döntését, az esetet az FTC elé terjesztik. Az FTC munkatársai elsőbbségi alapon felülvizsgálják a kifogásolt reklámot annak a megállapítására, hogy sérti-e az FTC-törvényt, és ezzel gyakran sikerül véget vetniük a kifogásolt magatartásnak, vagy a felet rávenni a NARB-eljáráshoz való visszatérésre.

Az FTC hasonlóképpen elsőbbséggel kezeli az EU-tagállamokból a „biztonságos kikötő” elveinek nem teljesítésével kapcsolatban érkező megkereséseket. Az Egyesült Államok önszabályozó szerveitől érkező megkereséseket illetően munkatársaink minden olyan információt megvizsgálnak, amely felvilágosítást adhat arról, hogy a panaszolt magatartás sérti-e az FTC-törvény 5. szakaszát. Ez az elkötelezettség ezenkívül a „biztonságos kikötő” elveiben is megtalálható a végrehajtásról szóló gyakran felvetődő kérdésnél (11. GYFK).

GeoCities: az FTC első online adatvédelmi esete

A Szövetségi Kereskedelmi Bizottság első internetes adatvédelmi esete, a GeoCities, a Bizottság hatáskörén alapult az 5. szakasz szerint ([1]). Abban az esetben az FTC azt állította, hogy a GeoCities felnőtteket és gyerekeket egyaránt félretájékoztatott arról, hogy személyi adataikat hogyan használja fel. A Szövetségi Kereskedelmi Bizottság panaszának állítása szerint a GeoCities úgy nyilatkozott, hogy bizonyos, a honlapjukon keresztül gyűjtött személyazonosító adatokat csak belső célokra vagy a fogyasztók felé reklámajánlatok megtételére, általuk kért termékek és szolgáltatások biztosítására használnak, és a további „nem kötelező” információt a fogyasztó hozzájárulása nélkül nem adják ki harmadik félnek. Ezt az információt valójában mégis átadták harmadik félnek; akik azt üzleti célú megkereséshez tagok kiválasztásához használták fel, túl azon tagok körén, akik ebbe beleegyeztek. A panasz azzal vádolta továbbá a GeoCitiest, hogy félrevezető gyakorlatot alkalmazott az adatok megszerzéséhez gyermekektől. Az FTC panasza értelmében a GeoCities azt állította, hogy honlapján egy gyereksarkot működtet, és hogy az ott megszerzett adatokat a GeoCities kezeli. Valójában a GeoCities honlapjának ezt a részét harmadik felek működtették, és ők gyűjtötték és kezelték az adatokat.

Az egyezség megtiltja a GeoCitiesnek, hogy hamisan tüntesse fel azt a célt, amihez a vállalkozás a személyazonosító adatokat a fogyasztóktól és a fogyasztókról – a gyerekeket is beleértve – gyűjti és felhasználja. A végzés előírja, hogy a vállalkozás egyértelmű és jól látható adatvédelmi értesítést helyezzen el a honlapján, tájékoztatva a fogyasztókat, hogy milyen adatot kérnek és milyen célból, ezeket kinek adják tovább, és hogy a fogyasztó hogyan tud az adatokhoz hozzáférni, illetve azokat eltávolítani. A szülői felügyelet biztosítására a megállapodás ezen túlmenően előírja, hogy a GeoCities szerezze meg a szülők beleegyezését azelőtt, hogy a 12 éves, illetve annál fiatalabb gyermekektől személyazonosító adatokat kér. A végzés értelmében a GeoCities köteles a tagjait értesíteni és lehetőséget biztosítani számukra adataik törlésére a GeoCities és a harmadik felek adatbázisaiból. Az egyezség különösen megköveteli, hogy a GeoCities értesítse a 12 éves és fiatalabb gyermekek szüleit, és törölje adataikat, amennyiben a szülő azok tárolásához és használatához kifejezetten nem járul hozzá. Végül a GeoCities köteles ezenkívül felvenni a kapcsolatot a harmadik féllel, akivel előzőleg az adatokat közölte, és felszólítani, hogy szintén törölje ezeket az adatokat ([2]).

ReverseAuction.com

Nemrégen ez az ügynökség keresetet indított, amelyben egy másik online társaság állítólagos adatvédelmi jogsértését kifogásolta. 2000 januárjában a Bizottság helyt adott a panasznak a ReverseAuction.com online aukciós oldallal szemben, és jóváhagyta a megegyezéses megállapodást a vállalkozással, amely állítólag egy versenytárs weboldaláról (eBay.com) szerezte meg a fogyasztók azonosítható személyi adatait, akiknek ezután kéretlenül, félrevezető e-mail üzeneteket küldött, és üzleti adataikat kérdezte ([3]). Panaszunk azt állította, hogy a ReverseAuction megszegte az

([1]) GeoCities, Docket No. C-3849 (jogerős végzés 1999. feb. 12.) (a www.ftc.gov/os/1999/9902/9823015d %26o.htm honlapon).

([2]) A Bizottság ezután még egy ügyben hozott határozatot gyermekek személyes adatainak online gyűjtéséről. A Liberty Financial Companies Inc. üzemeltette a Young Investor weboldalt, amely gyermekeknek és tizéveseknek szólt, pénzzel, illetve befektetéssel kapcsolatos témákról. A Bizottság szerint a weboldal hamisan állította, hogy gyerekek körében végzett felmérés keretében gyűjtött adatok névtelenek maradnak, és a résztvevőknek e-mail hírlevelet, illetve nyereményeket küldenek. Valójában a gyermekre és a család pénzügyi helyzetére vonatkozó adatok azonosíthatóak maradtak, és sem hírlevelet, sem nyereményeket nem küldtek. A megegyezéses megállapodás a jövőben megtiltja az ilyen jellegű hamis állításokat, és előírja a Liberty Financial számára, hogy gyermekeknek szóló weboldalakon adatvédelmi értesítést helyezzen el, valamint kérje a szülők bizonyítható beleegyezését az előtt, hogy a gyermekektől személyazonosító adatokat kér. Liberty Financial Cos., Docket No. C-3891 (jogerős végzés 1999. aug. 12.) (a www.ftc.gov/opa/1999/9905/younginvestor.htm honlapon).

([3]) Lásd ReverseAuction.com, Inc., 000032 számú polgári per (D. D. C.) (iktatás dátuma: 2000. január 6.). (Sajtóközlemény és perbeszédek a www.ftc.gov/opa/2000/01/reverse4.htm honlapon.)

FTC-törvény 5 szakaszát a személyesen azonosítható információ, köztük az eBay-felhasználók e-mail címeinek és felhasználói azonosítóinak megszerzésével, valamint a félrevezető e-mail üzenetek elküldésével.

Amint az a panaszban szerepel, a ReverseAuction az információk megszerzése előtt először eBay felhasználóként regisztrálta magát, és vállalta, hogy elfogadja az eBay felhasználói megállapodását és adatvédelmi politikáját. Ez a megállapodás és politika védi a fogyasztók személyiségi jogait azáltal, hogy megtiltja, hogy eBay felhasználók személyazonosító adatokat nem engedélyezett célra – pl. kéretlen, reklámcélú e-mail üzenetek elküldésére – megszerezzenek és felhasználjanak. Ezért panaszunkban először is azt állítottuk, hogy a ReverseAuction hamisan nyilatkozta, hogy elfogadja az eBay felhasználói megállapodását és adatvédelmi politikáját, ami az 5. szakasz értelmében félrevezető gyakorlat. Másik megközelítésben a panasz azt állította, hogy az információ felhasználása a ReverseAuction által kéretlen e-mail üzenetek küldésére megsérti a felhasználói megállapodást és adatvédelmi politikát, ami az 5. szakasz értelmében tisztességtelen kereskedelmi gyakorlat.

Másodszor a panasz azt állította, hogy a fogyasztóknak küldött e-mail üzenet egy félrevezető tárgysort tartalmazott, amelyben azt közölték, hogy eBay-felhasználói azonosítójuk érvényessége „hamarosan lejár". Végezetül, a panasz azt állította, hogy az e-mail üzenetekben hamisan közölték, hogy az eBay közvetve vagy közvetlenül átadta a ReverseAuction részére az eBay-felhasználók azonosítható személyes adatait, vagy más módon vett részt a kéretlen e-mail üzenetek terjesztésében.

Az FTC által elért egyezség megtiltja a ReverseAuctionnak az ilyen fajta törvénysértéseket a jövőben. Ezenkívül kötelezi a ReverseAuctiont, hogy értesítse azokat a felhasználókat, akik a ReverseAuction e-mail üzenetére válaszként a ReverseAuctionnál nyilvántartásba vetették magukat vagy ezt ezután fogják megtenni. Az értesítés továbbá tájékoztatja a felhasználókat, hogy eBay felhasználói azonosítójuk érvényessége nem jár le hamarosan, valamint hogy az eBay nem tudott arról, hogy a ReverseAuction kéretlenül e-mail üzeneteket küldött és erre nem hatalmazta fel. Az értesítéssel meg kell teremteni továbbá a fogyasztók számára annak lehetőségét, hogy nyilvántartásukat a ReverseAuctionnál érvényteleníthessék és személyes adataikat a ReverseAuction adatbázisából töröltethessék. Ezen túlmenően a végzés kötelezi a ReverseAuction vállalkozást, hogy törölje az összes olyan e-Bay-tag személyes adatát, és tartózkodjon ezek használatától vagy továbbításától, akik ugyan megkapták a ReverseAuction e-mailjét, de nem kérték regisztrálásukat a ReverseAuctionnél. Végezetül a megállapodás a hivatalunk által elért korábbi adatvédelmi végzéseknek megfelelően megköveteli a ReverseAuction vállalkozástól, hogy adatvédelmi politikáját hozza nyilvánosságra az internetes honlapján, továbbá átfogó nyilvántartási rendelkezéseket tartalmaz, amelyek biztosítják az FTC számára a rendelkezések betartásának felügyeletét.

A ReverseAuction esete mutatja, hogy az FTC elkötelezetten használja a jogérvényesítési lehetőségeket, hogy támogassa az iparág önszabályozási erőfeszítéseit az online fogyasztói adatvédelem területén. Ez az eset közvetlenül egy olyan magatartást kifogásolt, amely aláássa a fogyasztók személyiségi jogait védő adatvédelmi politikát, illetve az erre vonatkozó felhasználói megállapodást, és ezáltal megrendítheti a fogyasztóknak az online vállalkozások adatvédelmi intézkedéseibe vetett bizalmát. Mivel ebben az esetben egy vállalkozás egy másik vállalkozás adatvédelmi politikája által védett felhasználói adatokat használt fel jogellenesen, az eset különös jelentőséggel bírhat a különböző országok vállalkozásai közötti adatátvitellel kapcsolatos adatvédelmi aggályok szempontjából.

Az FTC jogérvényesítési intézkedései ellenére a GeoCities, a Liberty Financial Cos. és a ReverseAuction esetében, az ügynökség hatásköre az online adatvédelem néhány területén korlátozottabb. Amint fent már említettük, a személyes információ gyűjtése és felhasználása az érintett hozzájárulása nélkül vagy tisztességtelen, vagy félrevezető gyakorlatot kell hogy képezzen ahhoz, hogy ez az FTC-törvény hatálya alá tartozzon. Így az FTC-törvény valószínűleg nem vonatkozik az olyan honlapra, amely a fogyasztóktól azonosítható személyes adatokat kér, de nem tesz hamis állítást az adatgyűjtés céljáról, és nem használja vagy hozza nyilvánosságra az információt olyan módon, ami a fogyasztóknak jelentős kárt okozhatna. Lehet, hogy az FTC hatásköre nem terjed ki arra, hogy széles körben megkövetelje az interneten keresztül adatokat gyűjtő szervezetektől egy bizonyos vagy bármilyen adatvédelmi politika követését [1] [2]. Amint azonban fent már említettük, ha egy vállalkozás nem követi a kinyilvánított adatvédelmi politikát, az valószínűleg félrevezető gyakorlatnak tekinthető.

---

[1] Ebből az okból kifolyólag a Szövetségi Kereskedelmi Bizottság a Kongresszus előtt kijelentette, hogy további jogszabályokra van szükség, amelyek az Egyesült Államokban minden, a fogyasztókat célzó kereskedelmi weboldal számára korrekt tájékoztatási gyakorlatot írnak elő. „Consumer Privacy on the World Wide Web" (fogyasztóvédelem a világhálón), a Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce United States House of Representatives, (távközlési albizottság, kereskedelmi házbizottság kereskedelem- és fogyasztóvédelme, Egyesült Államok képviselőháza) előtt, 1998. július 21. (lásd www.ftc.gov/os/9807/privac98.htm). Az FTC átmenetileg eltekintett az ilyen jogszabályok követelésétől, hogy az önszabályozási törekvések bizonyíthassanak a széles körű, korrekt tájékoztatási gyakorlat megvalósításával a weboldalakon. A Szövetségi Kereskedelmi Bizottság a Kongresszusnak az online adatvédelemről adott 1998. júniusi jelentésében – „Privacy Online: A Report to Congress" (Online személyiségi jogvédelem: a Szövetségi Kereskedelmi Bizottság jelentése a Kongresszus részére), (lásd www.ftc.gov/reports/privacy3/toc.htm) az FTC olyan jogszabályokat javasolt, amelyek szerint a kereskedelmi weboldalaknak meg kell szerezniük a szülők beleegyezését, mielőtt 13 évesnél fiatalabb gyermekektől azonosítható személyes adatokat gyűjtenek. Lásd a fenti 3. lábjegyzetet. Tavaly a Bizottság jelentésében – „Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress" (Önszabályozás és online személyiségi jogvédelem, a Szövetségi Kereskedelmi Bizottság jelentése a Kongresszus részére), 1999. július; (lásd www.ftc.gov/os/1999/9907/index.htm#13) – úgy találta, hogy az önszabályozás megfelelő előrehaladást ért el, és ezért akkor nem tett jogszabályi javaslatot. A Bizottság az elkövetkező hetekben újabb jelentést küld a Kongresszusnak az önszabályozás előrehaladásáról.

[2] 2000 májusában az FTC egy harmadik jelentést nyújtott be a Kongresszusnak „Privacy Online: Fair Information Practices in the Electronic Marketplace" (Online adatvédelem: tisztességes tájékoztatási gyakorlatok az elektronikus kereskedelemben) (lásd www.ftc.gov/os/2000/05/index.htm#22). Ebben az FTC a kereskedelmi weboldalakkal kapcsolatos legújabb vizsgálatait értelmezi, és azt a kérdést, hogy mennyiben használnak ezek a weboldalak tisztességes tájékoztatási gyakorlatokat. A jelentésben (az FTC-tagok többsége) azt ajánlja, hogy a Kongresszus fogadjon el egy törvényt, amely a fogyasztóorientált kereskedelmi weboldalak számára előírja a magánszféra alapvető védelmét.

Ezen túlmenően az FTC hatásköre ezen a területen csak azokra a tisztességtelen és félrevezető cselekményekre és gyakorlatokra vonatkozik, amelyek a „kereskedelemben történnek, vagy érintik a kereskedelmet". A termékeket és szolgáltatásokat reklámozó kereskedelmi vállalkozások adatgyűjtése, beleértve a kereskedelmi célú információgyűjtést és felhasználást, feltehetően kimeríti a „kereskedelem" kritériumát. Másrészről lehetséges, hogy sok személy vagy vállalkozás kereskedelmi cél nélkül gyűjt információt online módon, ami ezáltal kívül esik a Szövetségi Kereskedelmi Bizottság illetékességén. Erre a korlátozásra a „csevegő szobák" (chat rooms) szolgálnak például, ha azokat nem kereskedelmi vállalkozások – pl. jótékonysági szervezetek – működtetik .

Végezetül az FTC kereskedelmi gyakorlattal kapcsolatos alaphatásköréből bizonyos tevékenységek teljesen vagy részben törvényileg ki vannak zárva, ami korlátozza az FTC átfogó válaszadási lehetőségeit az internetes adatvédelmi kérdésekben. Ezek közé tartoznak a kivételek számos nagy információigényű fogyasztói üzletág, mint pl. bankok, biztosítótársaságok és légitársaságok esetében. Amint tudja, e jogi személyek felett szövetségi és állami szinten más intézmények rendelkeznek illetékességgel, így pl. a szövetségi bankügynökségek vagy a Közlekedési Minisztérium.

Azokban az esetekben, ahol az FTC az illetékes, fogadja a levélben vagy telefonon és újabban honlapján keresztül ([1]) a Consumer Response Centerbe (CRC – fogyasztói panaszközpont) érkező fogyasztói panaszokat, és a forrásokhoz mérten eljár azok ügyében. A CRC minden fogyasztó panaszát fogadja, az Európai Unió egyik tagállamában állandó lakhellyel rendelkezőkét is. Az FTC törvény megfelelő hatáskört biztosít a Szövetségi Kereskedelmi Bizottságnak, hogy az FTC törvény jövőbeni megsértései ellen jóvátételt rendeljen el, és kárpótolja a károsult fogyasztókat. Azt kívánjuk azonban vizsgálni, hogy a vállalkozás nem megfelelő magatartást tanúsított-e, mivel egyéni fogyasztói vitákban nem döntünk. A múltban a Szövetségi Kereskedelmi Bizottság kárpótlást biztosított az Egyesült Államok és más országok polgárainak egyaránt ([2]). Az FTC a megfelelő esetekben tovább gyakorolja hatáskörét, hogy kárpótlást biztosítson más országok olyan polgárainak, akiket a joghatóságán belül megtévesztő gyakorlattal megkárosítottak.

Foglalkoztatási adatok

Ön a legutóbbi levelében a foglalkoztatási adatok terén az FTC illetékességének további tisztázását kérte. Először azt kérdezte, hogy az FTC az 5. szakasz értelmében eljárhat-e egy olyan vállalkozás ellen, amely úgy nyilatkozik, hogy elismeri az amerikai „biztonságos kikötő" elveket, mégis olyan módon ad át vagy használ fel foglalkoztatási adatokat, amivel megsérti ezeket az elveket. Biztosítani szeretnénk Önt arról, hogy gondosan felülvizsgáltuk az FTC illetékességére vonatkozó jogszabályokat, a kapcsolódó dokumentumokat, illetve a vonatkozó precedensjogot, és arra a következtetésre jutottunk, hogy az FTC a foglalkoztatási adatok terén ugyanolyan illetékességgel bír, mint általában az FTC törvény 5. szakasza értelmében ([3]). Azaz ha egy eset megfelel az adatvédelmi jogérvényesítési intézkedésekhez szükséges jelenlegi kritériumoknak (tisztességtelenség vagy félrevezetés), akkor a foglakoztatási adatokkal kapcsolatos helyzetben is intézkedhetünk.

El szeretnénk oszlatni minden olyan nézetet, hogy az FTC lehetőségei az adatvédelmi jogérvényesítési intézkedésekben az olyan helyzetekre korlátozódnak, ahol egy vállalkozás egyéni fogyasztókat vezetett félre. Valójában, amint azt a Bizottság nemrégiben tett intézkedése a ReverseAuction ([4]) ügyben is igazolja, az FTC az olyan, adatok vállalkozások közötti átadásával kapcsolatos helyzetekben is tehet adatvédelmi jogérvényesítési intézkedéseket, ahol az állítás szerint az egyik vállalkozás egy másik vállalkozással szemben törvénytelenül jár el, amivel potenciálisan károsítja mind a fogyasztót, mind a vállalkozást. Várhatóan a foglalkoztatási adatok kérdése nagy valószínűséggel ebben a helyzetben merül fel, amikor európai vállalkozások európai állampolgárok foglalkoztatási adatait adják át olyan amerikai vállalkozásoknak, amelyek elkötelezték magukat a „biztonságos kikötő" elvek követése mellett.

Meg szeretnénk azonban említeni egy olyan körülményt, amikor az FTC fellépése behatárolt. Ez azokban a helyzetekben fordulhat elő, ha az ügyet hagyományos munkajogi vitarendezés keretében már tárgyalják, a legjellemzőbben sérelem/döntőbírósági kereset vagy tisztességtelen foglalkoztatási gyakorlat miatti panasz nyomán a National Labor Relations Board (Nemzeti Munkaügyi Testület) keretében. Ez akkor fordulhatna elő, ha például egy

([1]) Lásd a Szövetségi Kereskedelmi Bizottság online panaszűrlapját a http://www.ftc.gov/ftc/complaint.htm címen.

([2]) Például egy nemrégiben történt, egy internetes piramisrendszerrel kapcsolatos esetben a Bizottság 15 622 ügyfél számára nyert visszafizetést összesen körülbelül 5,5 millió USD értékben. A fogyasztók lakhelye az Egyesült Államokban, illetve 70 külföldi államban volt. Lásd www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm.

([3]) Az FTC jogosultságát meghatározó törvényben kifejezetten kizárt esetektől eltekintve az FTC illetékessége az FTC-törvény értelmében a „kereskedelmi vagy azt érintő" gyakorlat tekintetében ugyanolyan terjedelmű, mint a Kongresszus alkotmányos hatásköre a Kereskedelmi Záradék értelmében, Egyesült Államok kontra American Building Maintenance Industries, 422 U. S. 271, 277 n. 6 (1975)). Eszerint az FTC illetékessége felöleli a vállalkozások és iparág foglalkoztatásra vonatkozó gyakorlatát is a nemzetközi kereskedelemben.

([4]) Lásd „Online Auction Site Settles FTC Privacy Charges", az FTC sajtóközleménye (2000. január 6.) a http://www.ftc.gov/opa/2000/01/reverse4.htm honlapon.

munkáltató egy kollektív bértárgyalási megállapodásban a személyes adatok felhasználása tekintetében kötelezettséget vállalt, és a munkavállaló vagy szakszervezet állítása szerint ezt a megállapodást megszegte. Az FTC az ilyen eljárásba valószínűleg nem avatkozna bele ([1]).

Illetékesség a „bizalompecsétes" programoknál

Másodszor, Ön azt kérdezte, hogy az FTC illetékes-e a „bizalompecsétes" programok esetében, amelyek az Egyesült Államokban vitarendezési eszközöket kínálnak, és szerepüket a „biztonságos kikötő" elveinek érvényesítésénél és magánszemélyek panaszainak kezelésénél hamisan tüntették fel, akkor is, ha az ilyen szervezetek gyakorlatilag nem nyereségorientáltak. Annak megállapításában, hogy olyan szervezetek esetében illetékesek vagyunk-e, akik magukat nonprofitnak tüntetik fel, a Bizottság alaposan elemzi, hogy ezek a szervezetek, ha maguk nem is nyereségszerzők, de elősegítik-e tagjaik nyereségszerzését. A Bizottságnak sikerült hatáskört szereznie az ilyen szervezetekkel kapcsolatban, és 1999. május 24-én a California Dental Association kontra Szövetségi Kereskedelmi Bizottság ügyben az Egyesült Államok Legfelsőbb Bírósága egyhangúlag jóváhagyta a Bizottság illetékességét a helyi fogorvosi társaságok önkéntes nonprofit szövetsége felett egy trösztellenes ügyben. A bíróság álláspontja szerint:

> Az FTC-törvény nemcsak olyan szervezeteket kíván hatásköre alá vonni, amelyek „arra szerveződtek, hogy nyereségszerzés céljából üzleti tevékenységet folytassanak" (15 U. S. C. § 44.), hanem olyan szervezeteket is, amely üzleti tevékenységét „tagjai" nyeresége érdekében folytatja. … Ténylegesen aligha feltételezhető, hogy a Kongresszus egy titkosan támogató szervezet fogalmát ennyire korlátozottan kívánta volna megszabni, ezzel lehetőségét teremtve a hatáskör megkerülésére ott, ahol az FTC törvény céljai éppen ennek a hatáskörnek a biztosítását követelik.

Összefoglalva, egy bizonyos, bizalompecsét programot végrehajtó, nem nyereségorientált szervezettel kapcsolatban az illetékesség megadásának meghatározásához először tényszerűen fel kell mérni, hogy a szervezet nyereségorientált tagjainak milyen mértékű gazdasági előnyöket biztosít. Ha egy ilyen szervezet a bizalompecsét programját oly módon működteti, hogy azzal tagjainak gazdasági előnyt teremt, akkor az FTC valószínűleg érvényre juttatja illetékességét. Emellett az FTC valószínűleg az olyan csaló bizalompecsét programok esetében is illetékes, amelyek hamisan tüntetik fel magukat nonprofit szervként.

Adatvédelem az offline világban

Ön harmadsorban megjegyezte, hogy korábbi levelezésünk az online adatvédelemre összpontosított. Bár az elektronikus kereskedelem fejlődésének kritikus összetevőjeként az FTC valóban kiemelt figyelmet fordított az online adatvédelemre, maga az FTC-törvény 1914-ben készült, és az offline világban éppúgy érvényes. Így perbe foghatjuk azokat az offline vállalkozásokat, amelyek tisztességtelen vagy félrevezető gyakorlatot folytatnak a fogyasztói adatvédelem tekintetében ([2]). A Bizottság által múlt évben indított egyik keresetben – FTC kontra TouchTone Information Inc. ([3]) – egy „adatbróker vállalkozást" azzal vádoltak, hogy a fogyasztóktól jogellenesen személyükre vonatkozó pénzügyi adatokhoz jutott és ezeket értékesítette. A Bizottság azt állította, hogy a TouchTone „félrevezetéssel" fért hozzá a fogyasztók adataihoz, amely kifejezést a magánnyomozó szakma mesterségesen hozta létre annak a gyakorlatnak a megnevezésére, amikor csalárd fondorlattal személyes információt szereznek meg másokról, rendszerint telefonon keresztül. Az eset, amelyet 1999. április 21-én nyújtottak be Colorado állam szövetségi bíróságán, egy tiltó végzésre és minden jogszerűtlenül szerzett nyereség elkobzására irányul.

A hatáskörök átfedése

Végül Ön az FTC hatáskörének a más jogérvényesítő hatóságok illetékességével való kölcsönhatásáról kérdezett, különösen olyan esetekben, amikor a hatáskörök átfedésbe kerülhetnek. Szoros munkakapcsolatot teremtettünk sok

---

([1]) Annak eldöntése, hogy egy magatartás „tisztességtelen munkaügyi gyakorlatnak" vagy kollektív bértárgyalási megállapodás megszegésének minősül-e, technikai jellegű, amit rendszerint fenntartanak a panaszt megvizsgáló szakértő munkaügyi bíróságnak, tehát a döntőbíróságnak és az NLRB-nek.

([2]) Ahogy korábbi tárgyalásokból már tudja, a tisztességes hitelinformációról szóló törvény hatáskört biztosít az FTC-nek a fogyasztók pénzügyi adatainak védelmére a törvény hatályán belül, és a Bizottság erre a kérdésre vonatkozóan nemrég egy határozatot adott ki. Lásd In the Matter of Trans Union, Docket No. 9255 (2000. március 1.) (Sajtóközlemény és vélemény a www.ftc.gov/os/2000/03/index.htm honlapon).

([3]) 99-WM-783 polgári per (D. Colo.) (a http://www.ftc.gov/opa/1999/9904/touchtone.htm címen) (előzetes helybenhagyás végzésig)

más jogérvényesítő hatósággal, többek között a szövetségi banknyomozókkal és a főállamügyészekkel. A vizsgálatokat rendszerint összehangoljuk, hogy erőforrásainkat a hatáskörök átfedése esetén a legnagyobb mértékben kihasználhassuk. Ezenkívül a vizsgálandó ügyeket gyakran az illetékes szövetségi vagy állami ügynökséghez irányítjuk.

Remélem, hasznosnak találta ezt az áttekintést. Kérem, értesítsen, ha további információkra van szüksége.

Szívélyes üdvözlettel:

Robert Pitofsky

VI. MELLÉKLET

John Mogg
Igazgató, DG XV
Európai Bizottság
C 107–6/72 iroda
Rue de la Loi/Wetstraat 200
B–1049 Brüsszel

Tisztelt Mogg főigazgató úr!

Ezt a levelet az Egyesült Államok Kereskedelmi Minisztériumának kérésére küldöm el Önnek, hogy ismertessem a Közlekedési Minisztérium szerepét a fogyasztók légitársaságoknak megadott adatai védelme terén.

A Közlekedési Minisztérium támogatja az önszabályozást mint a fogyasztók által a légitársaságoknak megadott adatok védelme biztosításának legkevésbé tolakodó, mégis leghatékonyabb eszközét, és ennek megfelelően támogatja a „biztonságos kikötő" rendszer létrehozását, amely lehetővé tenné, hogy a légitársaságok megfeleljenek az Európai Unió adatvédelmi irányelve követelményeinek az Európai Unión kívüli országba irányuló adatátvitel tekintetében. A minisztérium elismeri azonban, hogy az önszabályozási törekvések sikerességéhez elengedhetetlenül szükséges, hogy a „biztonságos kikötő" rendszerben kitűzött adatvédelmi elvek követésére kötelezettséget vállaló légitársaságok ezekhez ténylegesen tartsák is magukat. Ehhez az önszabályozásnak támogatásra van szüksége a jogérvényesítés oldaláról. A minisztérium ezért meglévő fogyasztóvédelmi hatósági jogkörét felhasználva biztosítani fogja, hogy a légitársaságok megfeleljenek a nyilvánosság felé tett adatvédelmi kötelezettségvállalásuknak, és keresetet indít minden vélelmezett nem megfelelés esetén, amelyet önszabályozó szervezetek és mások – az Európai Unió tagállamait is beleértve – eljuttatnak hozzánk.

A minisztérium illetékességét jogérvényesítő intézkedések megtételére e területen a 49 U. S. C. 41712. határozza meg, amely megtiltja a fuvarozó vállalkozásoknak, hogy légi fuvarozás értékesítésében „tisztességtelen vagy félrevezető gyakorlatot vagy tisztességtelen versenymódszert" alkalmazzanak, amely károsítja vagy károsíthatja a fogyasztót. A 41712. szakasz a Szövetségi Kereskedelmi Bizottságról szóló törvény (15 U. S. C. 45) 5. szakasza mintájára épül fel. A légi fuvarozó vállalkozások azonban mentesek a Szövetségi Kereskedelmi Bizottság 5. szakasz szerinti szabályozása alól a 15 U. S. C. 45(a)(2) pontja szerint.

Hivatalom vizsgálatot indít és eljár a 49 U. S. C. 41712 alá tartozó esetekben (Lásd pl.: a következő DOT végzéseket: 99–11–5, 1999. november 9.; 99–8–23, 1999. augusztus 26.; 99–6–1, 1999. június 1.; 98–6–24, 1998. június 22.; 98–6–21, 1998. június 19.; 98–5–31, 1998. május 22. és 97–12–23, 1997. december 18.). Ezeket az eljárásokat saját vizsgálataink alapján folytatjuk, illetve magánszemélyektől, utazási irodáktól, légitársaságoktól, valamint az Egyesült Államok és más országok kormányzati ügynökségeitől kapott hivatalos és nem hivatalos panaszok alapján.

Szeretném felhívni a figyelmet arra, hogy ha valamely fuvarozó vállalkozás nem őrzi meg az utasoktól kapott információ titkosságát, ez önmagában nem minősül a 41712. szakasz megsértésének. Amennyiben azonban a fuvarozó vállalkozás nyilvánosan és hivatalosan elkötelezi magát a megszerzett fogyasztói információ titkosságának védelmét biztosító „biztonságos kikötő" elvek mellett, a minisztérium jogosult arra, hogy éljen a 41712 szakaszban kapott hatósági jogkörével az elvek betartásának biztosítására. Amennyiben tehát egy utas információt közöl egy olyan fuvarozóval, amely vállalta a „biztonságos kikötő" elvek követését, akkor az elvek be nem tartása a fogyasztónak valószínűleg kárt okozna, és a 41712. szakasz megsértésének minősülne. Hivatalom nagy fontosságot tulajdonít minden ilyen állítólagos tevékenység kivizsgálásának és az ilyen tevékenységre való esetekben eljárás folytatásának. Ezen túlmenően tájékoztatjuk a Kereskedelmi Minisztériumot minden ilyen eset végeredményeiről.

A 41712. szakasz megsértése abbahagyásra kötelező közigazgatási határozat kiadását, a határozat megsértése pedig polgári jogi büntetés kiszabását vonhatja maga után. Bár nem áll hatáskörünkben az egyéni panaszosoknak kártérítést megítélni vagy pénzbeli jóvátételt nyújtani, jogosultak vagyunk a vizsgálatokból és a minisztérium által indított keresetekből következő egyezségek jóváhagyására, amelyek a fogyasztónak kárenyhítésként, vagy az egyéb esetben fizetendő pénzbüntetés kiegyenlítéseként pénzbeli előnyt jelentenek. A múltban így jártunk el, és amennyiben a körülmények szükségessé teszik, a „biztonságos kikötő" elvek összefüggésében ezt továbbra is így kezelhetjük, és így is fogjuk kezelni. Ha az Egyesült Államok valamely légitársasága 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. (Lásd az 1993. június 23-i 93–6–34 és az 1993. június 9-i 93–6–11 DOT végzést. Bár ez az eljárás nem a 41712. szakaszon

alapult, egy légitársaság működési engedélyének visszavonásához vezetett a Szövetségi Légügyi Törvény rendelkezéseinek, egy kétoldalú megállapodásnak, valamint a minisztérium szabályainak és rendeleteinek teljes figyelmen kívül hagyása miatt.)

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

Szívélyes üdvözlettel:

Samuel Podberesky

Légügyi végrehajtási és eljárási

főtanácsos-helyettes

VII. MELLÉKLET

Hivatkozva az 1. cikk (2) bekezdésének b) pontjára, az Egyesült Államok azon kormányzati szervei, amelyek hatáskörrel rendelkeznek a panaszok kivizsgálására és jóvátétel kieszközlésére tisztességtelen és félrevezető gyakorlat esetén, valamint magánszemélyek kárpótlására, függetlenül azok állandó lakóhely szerinti országától vagy állampolgárságától, a GYFK-val összhangban megvalósított elvek nem teljesítése esetén, a következők:

1. a Szövetségi Kereskedelmi Bizottság; és

2. az Egyesült Államok Közlekedési Minisztériuma

A Szövetségi Kereskedelmi Bizottság a Szövetségi Kereskedelmi Bizottságról szóló törvény 5. szakasza szerinti felhatalmazás alapján működik. A Szövetségi Kereskedelmi Bizottság hatásköre az 5. szakasz szerint bankok, takarék-, kölcsön- és hitelintézetek, távközlési vállalkozások, államközi közhasznú fuvarozó vállalkozások, légi fuvarozók, konzervgyárak és vágóhidak tekintetében kizárt. Bár a biztosítási üzletágat az 5. szakaszban a kivételek listája kifejezetten nem említi, a McCarran–Ferguson-törvény ([1]) a biztosítási üzletág szabályozását az egyes államok hatáskörébe utalta. Az FTC-törvény rendelkezései azonban annyiban vonatkoznak a biztosítási üzletágra, amennyiben ezt az üzletágat az állam törvényei nem szabályozzák. Az FTC továbbá fenntartja a hatáskört a biztosítóvállalkozások által folytatott tisztességtelen vagy félrevezető gyakorlat esetén, ha ezek a vállalkozások nem biztosítással foglalkoznak.

Az Egyesült Államok Közlekedési Minisztériuma az Egyesült Államok törvénykönyv 41712. szakaszának 49. címe szerinti felhatalmazás alapján működik. Az Egyesült Államok Közlekedési Minisztériuma az eljárásokat a saját vizsgálata alapján, illetve magánszemélyektől, utazási irodáktól, légitársaságoktól, valamint az Egyesült Államok és külföldi országok kormányzati hivatalaitól kapott hivatalos és nem hivatalos panaszok alapján folytatja.

([1]) 15 U. S. C. § 1011 et seq.