

Dr. Szabó Endre Győző A SWIFT adatkezeléséről

2006 júniusának végén Európában és az Egyesült Államokban először a sajtó vetette fel annak kérdését, hogy a belgiumi székhelyű SWIFT (Society for Worldwide Interbank Financial Telecommunication) jogszerűen továbbított-e banki adatokat az amerikai hatóságnak (Office of Foreign Assets Control of the United States Department of the Treasury, a továbbiakban: UST). A SWIFT világszerte bankok közötti tranzakciókhoz kapcsolódó üzeneteket továbbít. A UST a terrorizmus elleni harc keretében a SWIFT-hez címzett adatigényléseket követően hozzáférést kapott olyan adatokhoz, amely adatok alanyai az adattovábbításról semmilyen információt nem kaptak, sőt, valójában az adatok Egyesült Államokba való továbbításának lehetőségét sem ismerték. Amint azt lentebb látni fogjuk, a SWIFT adatkezelésének talán legnagyobb hibája az átláthatóság hiánya, illetve alapvető tények elhallgatása volt. Ez vezetett az európai adatvédelem utóbbi időszakának talán legnagyobb botrányához. A transzparencia hiányát és az adatkezelés jogszerűségének egyéb hiányosságait a SWIFT az utóbbi időszakban megfeszített munkával igyekszik orvosolni. Ennek tárgyalása előtt azonban vegyük sorra a vitatott adatkezelés menetét és az adatvédelmi hatóságok lépéseit.

A SWIFT szervezeti felépítése és az általa kezelt adatok köre

Azt követően, hogy a sajtó nyilvánosságra hozta, hogy a SWIFT közelebről nehezen körülhatárolható körű és mennyiségű adatot továbbított a UST-nek, különböző adatvédelmi hatóságok vizsgálatot indítottak. Ezek között elsőként a belga adatvédelmi hatóságot¹ kell említeni, amely azért illetékes, mert a SWIFT székhelye Belgiumban, Brüsszel közelében, Hulpe-ben van. Külön ki kell említeni a 29-es Munkacsoportot, amely nem hatóság ugyan, de az Európai Unió adatvédelmi hatóságait összefogva fontos szerepet játszott a tények és azok jogi megítélésének felderítésében.

A SWIFT korlátolt felelősségű egyesülés² formájában működik, mintegy 7800 tagot számlál. Tagjai - ahogyan ügyfelei is - pénzügyi intézmények, amelyek a bankközi átutalásokhoz kapcsolódó üzenetszolgáltatást, az úgynevezett SWIFTNet Fin szolgáltatást igénybe vehetik. Az ügy nyilvánosságra kerülését követő első időszakban a SWIFT visszautasította annak lehetőségét, hogy adatkezelőként járna el, arra hivatkozva, hogy ő mindössze a bankoktól kapott megbízások alapján továbbít üzeneteket a bankok által meghatározott tartalommal, pontosan megjelölt címzettnek. Ennek megfelelően önmagát csupán adatfeldolgozóként határozta meg, és kizárta az adatkezelői felelősséget. A 29-es Munkacsoport, egyetértésben a belga hatósággal, úgy ítélte meg, hogy a SWIFT a szokásos adatfeldolgozó szerepen túlmutató lépéseket tett, amelynek jó példája az, hogy a UST adatigénylése kapcsán tagjaival való egyetértés nélkül bocsátkozott tárgyalásokba a továbbítandó adatok köréről, valamint az adattovábbítás módjáról. Ebből következően a SWIFT adatvédelmi jogi szempontból adatkezelőnek minősül és nem vonhatja ki magát az ezzel járó felelősség alól. Ugyanígy a SWIFT tagjai, a bankok is adatkezelőnek tekintendők. A felelősség mértékét nehéz lenne meghatározni, az elkészült jelentések, vélemények a „közös felelősséget” emelik ki.

A SWIFT felépítése kapcsán meg kell még említenünk, hogy működését az ún. G-tízek csoportja felügyeli, amely tíz ország³ központi bankjainak képviselőiből áll. A felügyelet elsősorban a kockázatok kezelésére, a pénzügyi infrastruktúra helyes működésére összpontosít, valamint érinti az átláthatóság, a működési kockázatok, köztük a jogi kockázatok kérdéseit is. Eszközeiben a G-tízek csoportjának felügyelete meglehetősen gyenge, a SWIFT vezető testületének döntéseit nem bírálhatja felül. Gyakorlatilag tárgyalásos úton, mindössze a „meggyőzés eszközeivel” élhet, ha a működést nem találja megfelelőnek. Adatvédelmi kérdésekben a G-tízek csoportja azonban nem foglal állást, mivel álláspontja szerint erre nem terjed ki a megbízatása.

A SWIFT által kezelt adatok körének meghatározásakor fontos tisztázni, hogy a SWIFT nem bankok közötti elszámolásokat végez, hanem pusztán az átutalásokhoz kapcsolódó üzeneteket továbbít. Ennek megfelelően a bankok számára továbbított üzenetek tartalmazzák az utalt összeg mennyiségét, a pénznemet, az értéknapot, az átutaló nevét és bankját, valamint a kedvezményezettet és annak bankját. Ezek az adatok lehetővé teszik az átutalás lebonyolítását, amelyben a SWIFT már nem vesz részt.

A bankközi tranzakciókhoz kötődő üzenetek magukban foglalják az egy országon belüli, valamint a nemzetközi, beleértve a kontinensek közötti átutalásokat is. Az üzenetek tartalmát a SWIFT 124 napig tárolja központi adatbázisában. A kockázatok csökkentése érdekében a SWIFT európai adatbázisának

tökéletes tükörképét jelentő adatbázist működtet az Egyesült Államok területén, amely valamennyi adattovábbítást azonnal rögzít, megőrizve garanciális szerepét bármilyen rendellenesség esetére. Ez tehát az a pont, ahol európai banki adatok kerülnek az Egyesült Államokba, gyakorlatilag pusztán biztonsági megfontolásból. Ez a pont meghatározónak bizonyult az ügy további alakulására nézve.

Az amerikai hatóság adatigénylése

A UST értesülést szerezve az amerikai földön elérhető SWIFT adatállományról, adatokat igényelt. Az adatigénylés célja az volt, hogy a terrorizmus elleni küzdelem során használható információkhoz jussanak.

A UST által igényelt adatok körét pontosan nem ismerjük. Azt tudjuk azonban, hogy a UST kérésének megfelelő adatokat nem egyesével tette elérhetővé a SWIFT, hanem egy úgynevezett „fekete dobozban” adta át a keresési szempontoknak megfelelő adatkört (például két ország között az adott időszakban lebonyolított tranzakciókhoz kötődő adatok), amelyben aztán az amerikai hatóság további kereséseket hajthatott végre.

A SWIFT az erre irányuló kritikákat elhárítva mindvégig vitatta, hogy az adatigényléseket sikeresen megtámadhatta volna, hangsúlyozva, hogy a kapott kéréseknek köteles volt eleget tenni. Sikerként könyveli el ugyanakkor, hogy a UST-vel való egyeztetések során az igényelt adatok körét bizonyos mértékben szűkíteni tudták, elérték, hogy az amerikai hatóságok az igényelt adatok védelmét és szigorúan a célnak megfelelő felhasználását ígérték. További garanciaként értékelték, hogy a jogszerűséget biztosítandó, az adattovábbításokat egy kívülálló fél, egy tanácsadó cég kísérte figyelemmel⁴. Ennek ellenére a „fekete doboz” az ismétlődő adatigényléseknek megfelelően 2001 végétől kezdődően újra meg újra feltöltötték, és a UST mind a mai napig hozzáférhet a kívánt adatokhoz.

Talán érdemes egy pillantást vetni arra, hogy milyen méretű adatáramlásról van is itt szó. A SWIFT 2005-ös éves jelentése szerint napi átlagban 12 millió üzenetet továbbított, ami évente két és fél milliárd továbbítást, ebből 1,6 milliárd európai tranzakciókhoz kötődő üzenet-továbbítást jelentett. E mögött a szám mögött természetes és jogi személyek milliói vannak, akik - és ezt hangsúlyozni kell - semmilyen információval nem rendelkeztek arra nézve, hogy adataikat az Egyesült Államok bármely hatósága az eredeti gazdasági céltól eltérő célra felhasználhatja majd.

Adatvédelmi vizsgálatok eredményei

A 2006 júniusában megjelent sajtóhírek nyomán viszonylag gyorsan elkezdődtek a vizsgálatok. Az Európai Parlament már július elején a helyzet tisztázását kérte a hatáskörrel rendelkező nemzeti és európai szervektől, az európai adatvédelmi biztostól azt kérte, hogy vizsgálja meg az Európai Központi Bank szerepét és felelősségét. A belga adatvédelmi hatóság véleményét szeptember végén hozta nyilvánosságra. Az ügy jelentőségét kiemelve a jelentést⁵ maga a miniszterelnök mutatta be a sajtónak. Az Európai Parlament illetékes bizottsága (Állampolgári Jogi, Bel- és Igazságügyi Bizottság) október elején nyilvános ülést tartott a SWIFT adatkezeléséhez kapcsolódóan, ahol a SWIFT felső vezetői közül, az EKB, az Európai Bizottság, valamint a belga nemzeti bank és szenátus képviselői is részt vettek. Ezen az ülésen mind a 29-es Munkacsoport, mind az európai adatvédelmi biztos nyilvánosságra hozta készülő jelentésének egyes elemeit, többek között felvetve az Európai Központi Bank felelősségét azért, hogy értesüléseiről nem tájékoztatta egyik adatvédelmi hatóságot sem.

Minden megszületett vélemény és vizsgálati eredmény mindenekelőtt azt kellett, hogy megvizsgálja: milyen jogszabályok alapján ítélandó meg a SWIFT adatkezelésének jogszerűsége. A belga adatvédelmi hatóság megállapította, hogy a belga jog és a belga adatvédelmi jog alkalmazandó, amely megállapítással a SWIFT is egyetértett. A 29-es Munkacsoport az adatvédelmi irányelv követelmény-rendszerét vette alapul vizsgálatához⁶. Mind a belga adatvédelmi hatóság, mind a 29-es Munkacsoport egybehangzóan azt állapította meg, hogy a UST az európai adatvédelmi normák megsértésével került a SWIFT által kezelt adatok birtokába. Azt is megállapították, hogy a SWIFT, valamint a tagságot képező bankok közös felelősséget viselnek a jogszerűtlen adattovábbításért.

A hatóságok kifogásolták, hogy az adatokat úgy továbbították az Egyesült Államok területére, hogy az adatvédelmi irányelv⁷ erre vonatkozó előírásai nem teljesültek. Az Egyesült Államok nem nyújt megfelelő szintű védelmet a személyes adatok védelme tekintetében, az erre az esetre előírt garanciákat pedig a SWIFT elmulasztotta teljesíteni. Kifogásként fogalmazták meg, hogy az adatalanyok nem kaptak megfelelő tájékoztatást az adatkezelés körülményeiről. A SWIFT ebben a

vonatkozásban többször is arra emlékeztetett, hogy ügyfélkörükbe nem tartoznak természetes személyek, csupán jogi személyek, így a kezelt személyes adatok nem ügyfél adatok, csupán az „ügyfelek ügyfeleinek” adatai. Erre hivatkozva a SWIFT úgy foglalt állást, hogy a tagság (pénzügyi intézmények), és nem a SWIFT feladata az adatalanyok tájékoztatása.

Ezen túl felróták a SWIFT vezetésének, hogy az adatbázis tervezésének és létrehozásának időszakában nem kerestek meg egyetlen adatvédelmi hatóságot sem. A konzultációk, vagy egy esetleges előzetes ellenőrzés alkalmat adhattak volna arra, hogy az adatkezeléshez kapcsolódó adatvédelmi jogi kockázatokat azonosítani lehessen.

Az adatvédelmi vizsgálatok kiemelt figyelmet szenteltek a célhoz kötöttség elve érvényesülésének. Ebben a tekintetben mindenek előtt azt emelték ki, hogy a SWIFT adattovábbításai gazdasági célokat szolgálnak, a SWIFT feladata a bankok közötti átutalások megkönnyítése, felgyorsítása, illetve adott esetben a tranzakció körülményeinek visszakereshetőségét biztosítja. Az Egyesült Államokban létrehozott második adatbázis az eredeti céllal megegyezően az előbb említett feladatok zökkenőmentes végrehajtását szolgálta. A SWIFT által kezelt adatokat a UST az eredetitől eltérő célra, a terrorizmus elleni küzdelemre használta fel. A 29-es Munkacsoport ismételten hangsúlyozta a bűnözés és kiemelten is a terrorizmus elleni harc iránti elkötelezettségét, ugyanakkor leszögezte, hogy ez nem történhet az alapvető adatvédelmi elvek figyelmen kívül hagyásával.

Az előbb felsoroltakon túl azt követően, hogy a belga adatvédelmi hatóság megállapította a SWIFT adatkezelői minőségét, valamint a belga adatvédelmi jog alkalmazhatóságát, emlékeztetett arra, hogy a SWIFT adatkezelésébe kellett volna jelenteni a belga adatvédelmi nyilvántartásba.

A SWIFT álláspontja és a jogszerű működéshez szükséges lépések

Amint azt fentebb láttuk, az adatvédelmi vizsgálatok számos tekintetben megállapították a SWIFT adatkezelésének jogszerűtlen, illetve az európai adatvédelmi követelményeknek meg nem felelő voltát. A lista tartalmazza az adatalanyok számára átláthatatlan működést, az adatok útjának követhetlenségét, az adatalanyok tájékoztatásának hiányát, jogszabályoknak meg nem felelő adattovábbítást harmadik országba, az adatok hozzáférhetővé tételét az eredetivel össze nem egyeztethető célra, adatvédelmi hatóságokkal való konzultáció, valamint az adatkezelés bejelentésének elmulasztását. Ehhez a felsoroláshoz hozzá kell még tennünk azt is, hogy a SWIFT szervezetén belül nem működött hatékony felügyeleti rendszer, amely az adatvédelmi jogszabályoknak való megfelelést biztosíthatta volna.

Az ügy kipattanása után a SWIFT, ahogyan az várható volt, rövid ideig vonakodott elismerni a történetekért való felelősséget. Arra hivatkozott, hogy jogszerűen kívánt eljárni, ezért adta át a UST adatigénylésének megfelelő adatokat. Éppen ez az egyébként, amit Európában a vizsgálatok jogszerűtlennek találtak. A SWIFT ebben a helyzetben jogbiztonságot követel: kész együttműködni a hatóságokkal mindkét kontinensen, ugyanakkor azt kéri, hogy jelöljék ki számára világosan, mi az, amit köteles megtenni, és mi az, amit köteles elkerülni. A SWIFT annak a helyzetnek a tarthatatlanságára hívja fel a figyelmet, hogy ami az egyik földrészen kötelezettsége, az a másikon jogszerűtlen, illetve fordítva. Ezt a panaszt az európai adatvédelmi szervek megértették, álláspontjukat azonban nem változtatták meg, és konkrét lépéseket követeltek a SWIFT-től annak érdekében, hogy a jogellenes állapotot megszüntesse.

A SWIFT a kezdeti bizonytalanság után úgy döntött, hogy az európai adatvédelmi vizsgálatok eredményeit nem vitatva az európai normáknak való teljes megfelelést tűzi ki célul⁸. Az Egyesült Államokba való adattovábbítást illetően ezt a Safe Harbour⁹ státusz elérésén keresztül kívánja megvalósítani. Ezen túl a SWIFT egy ún. adatvédelmi munkacsoportot állított fel¹⁰, amelynek az a feladata, hogy a SWIFT szerződéseinek rendszerét áttekintve az átláthatóbb működés elérésére tegyen javaslatokat. A SWIFT végül kész információs rendszere felépítésének felülvizsgálatára is annak érdekében, hogy szolgáltatásai ne csak a kereskedelmi elvárásoknak, hanem az adatvédelmi normáknak is jobban megfeleljen. Meg kell jegyeznünk, hogy az európai hatóságokat leginkább feltehetően az a megoldás nyugtatná meg, ha az európai banki tranzakciók adatait nem továbbítanák más kontinensre. Mindazonáltal egyelőre homály fedi, hogy egy ilyen léptékű struktúra-váltásra, amely minden bizonnyal több évet venne igénybe, a SWIFT hajlandó lesz-e.

A jogszerű működés helyreállítása kapcsán érdemes megemlíteni, hogy ez az ügy jó fokmérője az európai adatvédelmi szervek azon képességének, hogy mennyire tudják kikényszeríteni egy gazdasági szereplőtől az adatvédelmi elvárásoknak való megfelelést. Tény, hogy ez a nyomás nem csak a SWIFT vezető testületére, hanem a tagságot képező bankok mindegyikére és a felügyeletben részt vevő

központi bankokra is nehezedik. A SWIFT ügy kapcsán egyébként az adatvédelmi hatóságok szövetségeseiként különböző gazdasági szereplők tűntek fel, amelyek a gazdasági kémkedés lehetőségét vetették fel és kritikát fogalmaztak meg a SWIFT-tel szemben. Elfogadhatatlannak tartják ugyanis azt, hogy a banki átutalásokhoz kötődő adatok ellenőrizhetetlen úton és módon vándorolhatnak olyan hatóságok kezébe, amelyek az európai adatvédelmi normákat nem teljes körűen érvényesítik. Ezek a gazdasági szereplők az európai adatvédelmi szervekkel együtt követelik és sürgetik a jogszerű működés helyreállítását.

Kétségtelen tény, hogy az ügy napvilágra kerülése presztízavesztést okozott a SWIFT-nek. A bankoknál is bekövetkezhetett hasonló veszteség, de a mértéke feltehetően lényegesen kisebb. A 29-es Munkacsoport fentebb már említett véleményében apellált erre a felelősségre, és erre is hivatkozott annak érdekében, hogy mielőbbi cselekvésre készítse a bankokat. Mindenesetre tény, hogy jelenleg a SWIFT-re várnak a legsürgetőbb feladatok, függetlenül attól, hogy a tagság a szervezeten belül miképpen tudja befolyásolni a döntéshozatalt. Márpedig a SWIFT láthatóan a lehető legkisebb veszteséggel szeretné lezárni az ügyet. Erre annál is inkább szüksége van, hiszen éppen jelenleg áll fejlesztés alatt a SEPA (Single Euro Payment Area - Egységes eurófizetési térség), amelynek működése 2010-től várható. A SWIFT üzleti tekintélyének megtépázása értelemszerűen rontaná annak esélyeit, hogy a SWIFT a SEPA-ban terveinek megfelelő pozíciókat tudjon megszerezni. Amikor az adatvédelmi normáknak való megfelelésről, és a SWIFT lépéseiről beszélünk, ezt a szempontot sem hagyhatjuk figyelmen kívül, annak ellenére, hogy ez utóbbi adatvédelmi szempontból nem tűnik relevánsnak.

Egyéb szervek szerepe

Amint azt fentebb láttuk, az Európai Központi Bankkal együtt tizenkét központi bank vesz részt a SWIFT felügyeletében, az ún. G-tízek csoportjában. Ma már tudjuk, hogy az Európai Központi Bank már 2002-ben értesülést szerzett a USB adatigényléseiről, ennek ellenére nem értesítette az adatvédelmi hatóságok egyikét sem. Az európai adatvédelmi biztos az Európai Központi Bank SWIFT ügyben betöltött szerepéről szóló véleményében¹¹ rámutatott: nem fogadható el az EKB azon érvelése, mely szerint a szakmai titoktartás állt az értesítés útjában, hiszen ez az európai adatvédelmi jog egyik alapelve, melyhez az adatvédelmi hatóságok is kötve vannak. Ez garantálja, hogy a hatóság birtokába kerülő adatokat valóban csak az ellenőrzés céljaira használják fel.

Új, és bizonyos értelemben meglepő fejleményekkel szolgáltak azok a nyilatkozatok, amelyek egy tizenkét fős, európai parlamenti képviselőkből álló delegáció tagjaitól származnak. Ez a delegáció április közepén Washingtonba látogatott, ahol az amerikai adminisztráció illetékeseivel emberi jogi kérdéseket tekintettek át¹². A „feszült pillanatoktól sem mentes” tárgyalás-sorozat folyamán a delegáció megtudta, hogy az EU pénzügyminiszterei a UST korábban már tájékoztatta a SWIFT adatbázisát érintő adatigénylésekről. Közelebbről nem határozta meg ennek a tájékoztatásnak az időpontját, de feltehetjük, hogy ez 2006 nyara elé esett. A delegáció egyik holland tagja elmondta azt is: azért alkalmazták a UST adatigénylései kapcsán a „fekete dobozt”, mert a SWIFT nem tudja kiszűrni a hatóság szempontjából szükséges adatokat, ezért leválogatott adatok helyett inkább egy tágabb keresési szempontnak megfelelő adatállományt helyeznek el a „fekete dobozban”, amelyben aztán a hatóság tovább kutathat.

Záró gondolatok

Ahogy arra fentebb már utaltam, a SWIFT adatkezelésének legnagyobb hiányossága a nem megfelelő átláthatóság, valamint az adatalanyok elégtelen tájékoztatása volt. A SWIFT adatvédelmi jogi felelőssége úgy fogalmazható meg, hogy az Egyesült Államokba irányuló jogszerűtlen adattovábbítás révén olyan helyzetet teremtett, amelyben jogszerűen már nem tudta megakadályozni, hogy az érintettek adatai olyan környezetbe kerüljenek, ahol az európai adatvédelmi normák nem érvényesülnek maradéktalanul. Ennek következménye az, hogy míg a SWIFT, mint a bankközi tranzakciókhoz kötődő adatok kezelője az átutalásokat nyomon követhetővé tudja tenni, az általa kezelt adatok tekintetében ezt a követelményt már nem tudja teljesíteni. A SWIFT ügy kapcsán elvégzett adatvédelmi vizsgálatok üzenete világos ebben a tekintetben, és azonos szintű követelményt vár el az átutalt összegek és a kezelt személyes adatok útját illetően is. Ahogy egy szervezet megfelelő működése során elvárható, hogy minden pénzmozgással el tudjon számolni, ugyanúgy a személyes adatok útját is nyilvánvalóan nyomon követhetővé kell tennie, akár az adatalany érdeklődése, akár hatósági vizsgálat céljából. Ezt az elvet egyébként a hazai adatvédelmi hatóság is alkalmazza, és ha ilyen formában nem is fogalmazza meg, az az ügyintézés következetes gyakorlataból kiolvasható.

Az ügy tanulsága, hogy a személyes adatok útjának nyomon követhetőségének követelménye mindaddig nem fog kielégítően érvényesülni, amíg az érintett szereplők megfelelően együtt nem működnek egymással. A SWIFT ügy, amely még közel sincsen a megnyugtató lezáráshoz, jó alkalmat teremt arra, hogy az adatvédelmi hatóságoktól kezdve az egyéb kormányzati szerveken át a gazdasági szereplők tisztázzák, ki mit vár a másiktól ezen a téren.

¹ Commission de la protection de la vie privée; honlapcím : www.privacycommission.be

² Cooperative limited-liability company

³ Ezek az országok: Belgium, Kanada, Németország, Franciaország, Olaszország, Japán, Hollandia, Svédország, Svájc, Egyesült Királyság és az Egyesült Államok. A G-tízek csoport tagjaként az Európai Központi Bank is részt vesz a SWIFT felügyeletében.

⁴ <http://193.191.208.6/juris/jurfv.htm> (7. oldal)

⁵ <http://193.191.208.6/juris/jurfv.htm>

⁶ A 29-es Munkacsoport véleménye magyar nyelven elérhető:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_hu.pdf

⁷ Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

⁸ Meg kell jegyeznünk, hogy a SWIFT világszerte 207 országra kiterjedő ügyfélköréből adódóan gyakorlatilag valamennyi európai állam joghatósága alá tartozó személlyel kapcsolatban áll. Ez áttekinthetetlen jogi sokszínűséget jelent, még ha az Európai Unió tagállamainak adatvédelmi joga harmonizált is. A bemutatott tények alapján számos adatvédelmi hatóság indított „saját” vizsgálatot, amely az adott ország bankjainak, központi bankjainak adatkezelését a SWIFT tevékenységével összefüggésben vizsgálta. El kell ismernünk, hogy ebben a helyzetben a SWIFT joggal igényli, hogy a hatékony együttműködés érdekében korlátozott számú hatósággal tudjon, illetve legyen köteles egyeztetni.

⁹ A Safe Harbour jogi keretét az Európai Unió és az Egyesült Államok közötti tárgyalások eredményeként alakították ki. Ennek lényege, hogy a Safe Harbour-höz csatlakozó európai vállalatok úgy kezelhetnek adatokat az Egyesült Államok területén, hogy azt az EU az európai adatvédelmi normákkal összhangban lévőnek ismeri el. Ennek háttérében az áll, hogy az Egyesült Államok a személyes adatok védelme terén az EU álláspontja szerint nem biztosít megfelelő szintű védelmet.

¹⁰ Az adatvédelmi munkacsoport (Data Protection Working Group) a SWIFT ügyfeleinek 11 európai, illetve Európán kívüli szakértőjéből áll. A munkacsoport tevékenységéről a SWIFT vezető testületének számol be.

¹¹ EDPS opinion on the role of the European Central Bank in the SWIFT case,

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/07-02-01_Opinion_ECB_role_SWIFT_EN.pdf

¹² <http://www.library.ep.ec/PressAg/EisNet/2007/DERE070423.htm#ret77799>