Ügyszám: […]
Ügyintéző: […]

[…]

Tisztelt […]!

Korábbi leveleimben tájékoztattam, hogy […] panasszal fordult a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban: Hatóság), amelyben előadta, hogy véleménye szerint adatvédelmi szempontból aggályos az, hogy a […] Zrt. (a továbbiakban: Bank) informatikai rendszere bizonyos online szolgáltatásokhoz (internetbank, online befektetési rendszer) kapcsolódóan az ügyfelek külső e-mail címeire nem titkosított csatornán keresztül küldi el az értesítéseket, amelyek sokszor érzékeny személyes adatokat is tartalmaznak (pl. átutalási adatok, bankkártya száma, befektetési tranzakciók adatai).

A panaszos továbbá tájékoztatta arról is a Hatóságot, hogy a problémával kapcsolatban többször is megkereste a Bank ügyfélszolgálatát, először […] az […] webes felületen keresztül. A Bank tájékoztatta a panaszost, hogy az ügyfelek külső e-mail címeire kiküldött értesítéseket továbbra sem fogja titkosítani, ellenben javasolta a panaszosnak, hogy az internetbankos felületen beállíthatja, hogy nem kér e-mailben értesítéseket. A panaszos arról is tájékoztatta a Hatóságot, hogy a Bank által javasolt ezen megoldás az Internetbank esetén valóban működő opció, de az Online Befektetési Rendszer esetén erre már nincs lehetőség, az onnan jövő értesítések kikapcsolását csak személyesen lehet kérni valamelyik bankfiókban.

A fentiek után a panaszos […] ismét megnézte az Internetbank e-mailes értesítések kikapcsolására vonatkozó felületét, ahol szerepelt egy újonnan írt figyelmeztetés arra vonatkozóan, hogy az ügyfél vállalja az azzal kapcsolatos felelősséget, hogy az Internetbanktól érkező e-mailek nem titkosított csatornán jutnak el hozzá.

A panaszos a fentieken túl azt is jelezte, hogy a Bank a marketing célú e-mailjei és hírlevelei kiküldéséhez az Internetbankkal és Online Befektetési Rendszerrel ellentétében használ titkosítást.

A fenti problémával kapcsolatban a Hatóság vizsgálati eljárást indított az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 52. § (1) bekezdése alapján, amely során az Infotv. 54. § (1) bekezdés a) és c) pontjaira hivatkozva megkereste a problémával kapcsolatban a Bankot.

A Bank részéről a belső adatvédelmi felelős azt a tájékoztatást adta, hogy az […] Internetbank segítségével igénybe vehető szolgáltatásokkal összefüggő üzeneteket az Internetbank védett rendszerén keresztül, a […] funkció segítségével küldi és fogadja. Ez az Internetbank üzenet közvetítő rendszere.

Mivel az ügyfelek részéről korábban igény merült fel arra, hogy a […] érkező üzenetek továbbíthatóak legyen külső e-mail fiókba is, ezért a Bank ezt lehetővé tette. A belső üzenetek külső e-mail fiókba történő átirányítását az ügyfél állíthatja be vagy kapcsolhatja ki az Internetbank fiókján keresztül. Mivel az üzenetek külső e-mail címre történő átirányítása

alacsonyabb biztonsági szintet jelent, a beállítás használata előtt a Bank az internetbankos felületen felhívja az érintettek figyelmét erre.

Az üzenetek külső e-mail címre történő továbbítása során az Internetbank nem használ titkosítást. A Bank részéről a belső adatvédelmi felelős által küldött válasz alapján technikailag lehetséges lenne TLS titkosítás bekapcsolására. Ez azonban véleménye alapján azért felesleges, mivel az egy „hamis biztonságérzetet" keltene az ügyfelek nagy részében. Ugyanis, ha a fogadó oldali szolgáltató (a külső e-mail fiók szolgáltatója) nem képes titkosított levél fogadására, akkor a levelek a beállítástól függetlenül titkosítás nélkül érnek célba, dacára az Internetbankban eszközölt beállításoknak. A TLS titkosítás bevezetését ezért nem tervezik, aminek oka nem a technikai megvalósítás hiánya, hanem a felelős ügyféldöntés hangsúlyozása.

Illetéktelen hozzáféréssel kapcsolatban eddig panaszt a Bank nem kapott. […]

A Bank részéről a fentieken túl a belső adatvédelmi felelős azt is közölte, hogy az nem alkalmaz titkosítást marketing vagy hírlevél célú üzenetei küldésénél. Megküldte továbbá a Bank adatkezelési szabályzatát, illetve az üggyel kapcsolatba hozható egyéb releváns dokumentációkat […].

A fentiekkel kapcsolatban a Hatóság az alábbi álláspontot alakította ki:

Az Infotv. 3. § 2. pontja értelmében az Internetbankon keresztül elérhető szolgáltatásokkal összefüggésben kezelt adatok, így a számlatulajdonos neve, elérhetőségei (pl. az e-mail címe is) és a számlával végzett egyes tranzakciók személyes adatoknak minősülnek, mivel azok alapján az érintett személye beazonosítható és különösen pénzügyi szokásaira nézve különböző következtetések is levonhatóak rá nézve.[1]

Az Infotv. 3. 10. pontja értelmében az adatkezelő által kezelt személyes adatoknak egy külső, harmadik személy által üzemeltetett szolgáltatás részére való továbbítása, így jelen esetben a banki ügyfelek személyes adatainak egy külső e-mail címre való kiküldése adatkezelésnek minősül.[2]

Az Infotv. 5 § (1) bekezdésének a) pontja alapján *„személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul."* Mivel az online banki szolgáltatások igénybevétele jellemzően a pénzintézetekkel megkötött, a számlavezetéshez kapcsolódó szerződéses jogviszonyon (jelen ügyben: az Internetbank igénybevételét tartalmazó, általános szerződési feltételek elfogadásával létrejövő szerződésen) alapul, az azzal kapcsolatban az ügyfél személyes adatainak kezelése (itt: továbbítása külső e-mail címre) az ő hozzájárulásához kötött. Más, az Infotv-ben nevesített adatkezelési jogalap alkalmazása az ügy kapcsán nem merült fel.

Az Infotv. a fentieken túl a 7. §-ban határozza meg az adatbiztonság követelményét, mely szerint az adatok kezelése, így például azok továbbítása során megfelelő technikai intézkedésekkel

---

[1] Infotv. 3. § 2. pont: *„személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés."*

[2] Infotv. 3. § 10. pont: *„adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése,* ***továbbítása****, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;"*

védeni kell azokat többek között a jogosulatlan hozzáférés, továbbítás, vagy nyilvánosságra hozatal ellen is.[3]

Az Infotv. adatbiztonságra vonatkozó előírásai alapján egyértelmű, hogy az adatkezelő kötelessége az, hogy megfelelő technikai intézkedésekkel is védje a személyes adatokat kezelésük, így jelen ügyben azok külső elektronikus levelezési címre történő továbbítása során a jogosulatlan hozzáférés ellen. A Hatóság álláspontja alapján az adatkezelőnek az adatbiztonság megtartása érdekében mindent meg kell tennie saját részéről a személyes adatok biztonságának garantálása érdekében a számára elérhető és tőle elvárhatóan alkalmazható technikai megoldások keretei között.

Amennyiben tehát az ügyfél a szolgáltatás igénybevételével és a vonatkozó feltételek elfogadásával előzetesen hozzájárul ahhoz, hogy a Bank az Internetbankon keresztüli üzeneteteket részére külső e-mail címére továbbítsa, még nem mentesíti az adatkezelő Bankot azon törvényi előírás alól, hogy a személyes adatok továbbítása során a maga részéről a rendelkezésére álló technikai megoldások keretei között mindent megtegyen az adatbiztonság követelményének minél teljesebb érvényesülése érdekében.

A Hatóság álláspontja szerint nem mentesülhet az adatkezelő a személyes adatok biztonságos továbbításának követelménye alól arra való hivatkozással, hogy ha a fogadó oldali e-mail szolgáltató nem képes titkosított levél fogadására, akkor az üzenetek titkosítatlanul érnek célba. Az adatkezelőnek a maga részéről meg kell tennie a szükséges intézkedéseket az adatok biztonságának garantálása érdekében és nem hivatkozhat általánosságban a másik adatkezelőknél esetlegesen fennálló technikai hiányosságra.

Az ügyfelekben történő „hamis biztonságérzet keltés" pedig kiküszöbölhető azáltal, ha a Bank a funkció igénybevétele előtt előzetesen felhívja az ügyfél figyelmét erre az esetleges, szolgáltatófüggő problémára.

Mindezek alapján az Infotv. 56. § (1) bekezdésére hivatkozva a Hatóság felszólította a Bankot, hogy az Infotv. 7. § (1)-(3) bekezdéseinek, valamint jelen állásfoglalásban kifejtetteknek megfelelően az Internetbankból a személyes adatok külső e-mail címre való továbbítása során tegyenek eleget az adatbiztonság követelményének és az e-mailek küldése során használják a megfelelő titkosítást.

[…]

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

---

[3] Infotv. 7. § (1)-(3) bekezdései: *„(1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.*

(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen."