Ügyiratszám: NAIH/2018/429/2/V

[...]
adatvédelmi felelős részére

[...]

Budapest
[...]

Tisztelt Adatvédelmi Felelős Úr!

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) NAIH/2017/3107/4/V ügyiratszámú levelében tájékoztatta a [...]-t (a továbbiakban: Társaság) az adatkezelési tevékenységével összefüggésben bejelentés alapján indított vizsgálatról, illetve tájékoztatást kért több, a vizsgálat lefolytatásához szükséges kérdésben.

Tekintettel arra, hogy a 2017. augusztus 23. napján kelt válaszában (a továbbiakban: első válasz) a Társaság képviselője nem válaszolt a Hatóság által feltett valamennyi kérdésre, továbbá arra, hogy a Társaság által megküldött fenti válasz további kérdéseket vetett fel, valamint arra, hogy a Társaság nem küldött meg minden, a Hatóság által kért dokumentumot, a Hatóság szükségesnek látta a Társaság ismételt megkeresését.[1]

1. A Társaság által az ügyben adott tájékoztatás összefoglalása

1.1. A Hatóság kérésére küldött tájékoztatás szerint a [...] (lakcím: [...], telefonszám: [...], a továbbiakban: Bejelentő) panaszával érintett incidens eseti jellegű ügyintézői hiba miatt történt, mivel a Társaság ügyfélkiszolgálást végző boltjaiban (a továbbiakban: [...]) már 2015. óta nincs hibajavítás, így a Társaság munkatársának nem lett volna szabad 2016. novemberében szerviz tevékenységet ellátnia, az ilyen ügyféligényeket minden esetben belső utasításaik szerint a gyártóhoz kell továbbítani. A Társaság képviselője előadta, hogy a fentiekből kifolyólag egyetlen, további [...]-ban sem végeznek készülék-profilmentést, iTunes szinkronizálást.

1.2. A Társaság álláspontja szerint adatvédelmi incidens az ügyben nem történt, hiszen a Bejelentő személyes adatait a Társaság nem hozta nyilvánosságra, azokat nem hozta harmadik személy tudomására, illetve nem adta át harmadik személy részére. A Társaság a Hatóság ismételt megkeresésére küldött, 2017. szeptember 20. napján kelt tájékoztatásában (a továbbiakban: második válasz) az adatvédelmi incidenssel összefüggésben részletesen előadta, hogy a Társaságnál vezetett adatvédelmi nyilvántartásba miért nem rögzítettek a Bejelentő panaszával összefüggésben adatvédelmi incidenst.
Ennek oka egyrészt az volt, hogy a Társaság adatvédelmi felelőse a Hatóság első megkereséséig nem értesült az adatvédelmi incidensről, azt neki, mint az adatvédelmi incidens nyilvántartását vezető személynek nem jelezték az incidenssel érintett munkavállalók.

[1] NAIH/2017/3107/6/V

Emellett a Társaság adatvédelmi felelőse előadta, hogy álláspontja szerint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 15. § (1a) bekezdése alapján a nyilvántartás vezetésének kettős célja van, egyrészt az incidenssel kapcsolatos intézkedések nyilvántartása, másrészt az érintett tájékoztatása. Előadta továbbá, hogy *„amikor az érintett [...]-ban dolgozó kolléga szembesült az „ismeretlen" profil feltöltésével a bevitt készülékre, azonnal és sikeresen kezdeményezte a kapcsolatfelvételt [...] úrral, és közösen, ott és akkor megoldották a problémát, [...] úr segítő közreműködése mellett. Az ügy adatvédelmi oldalról „megoldódott", szerencsére [...] úr adataihoz senki nem fért hozzá, azokat harmadik személyek nem ismerhették meg, és az adatokat még aznap törölték. Jóval később került hozzám az ügy a T. Hatóság megkeresésekor, melyet követően már indokolatlannak tartottam egy új incidens felvételét a nyilvántartásunkba. Természetesen, amennyiben a T. Hatóság ezt indokoltnak tartja, a kérésének készséggel eleget teszek."*

1.3. A Társaság képviselője második válaszához csatolta a Társaság biztonsági területe által végzett belső vizsgálatról készült, 2017. június 19. napján kelt jegyzőkönyvet, továbbá tájékoztatta a Hatóságot arról, hogy jelen ügyhöz hasonló ügy sem a Társaság adatvédelmi felelőse, sem a biztonsági terület, sem pedig a bolthálózatért felelős terület előtt nem ismert.

1.4. A Társaság csatolta továbbá a Társaság adatvédelmi felelőse által az üggyel összefüggésben küldött belső tájékoztatását, melynek célja a hasonló esetek elkerülése volt. A Társaság adatvédelmi felelőse előadta továbbá, hogy annak oka, hogy a fenti tájékoztatást csak a Hatóság megkeresését követően küldte ki, az ügyek feltorlódása volt, nem volt célja a Hatóság megtévesztése.

2. Az adatvédelmi incidensről

2.1. A Hatóság első megkeresésének 8. pontjában részletesen kifejtette álláspontját az adatvédelmi incidens jogi természetével és hatályos törvényi szabályozásával kapcsolatosan. Arra tekintettel azonban, hogy a Társaság második válaszában az adatvédelmi tisztviselő – a Hatóság álláspontja szerint – továbbra is az Infotv. szabályaival ellentétesen értelmezte az adatvédelmi incidens fogalmát, valamint az adatvédelmi incidensek nyilvántartására vonatkozó *kötelezettségét*, így a Hatóság szükségesnek látja a korábbi tájékoztatás megismétlését és kiegészítését.

2.2. Az Infotv. 3. § 26. alapján adatvédelmi incidensnek minősül *személyes adat jogellenes kezelése vagy feldolgozása*, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

A fentiek alapján tehát annak a körülménynek, hogy a Társaság nem hozta a Bejelentő személyes adatait harmadik személy tudomására, illetve nyilvánosságra, valamint annak, hogy az ügy *„adatvédelmi oldalról „megoldódott", [...] az adatokat még aznap törölték"* – az incidens nyilvántartása szempontjából – nincs jelentősége, *az adatvédelmi incidens már a Bejelentő személyes adatainak jogellenes kezelésével – jelen ügyben a biztonsági másolat elkészítésével és jelentős időn át történő tárolásával – megvalósult.*

2.3. A Társaság adatvédelmi felelősének álláspontja szerint az Infotv. 15. § (1a) bekezdése alapján a nyilvántartás vezetésének kettős célja van, egyrészt az incidenssel kapcsolatos intézkedések nyilvántartása, másrészt az érintett tájékoztatása.

Az Infotv. 15. § (1a) bekezdése alapján az adatvédelmi incidensekről vezetett nyilvántartás célja az adatvédelmi incidenssel kapcsolatos intézkedések *ellenőrzése*, valamint az érintett tájékoztatása. Amennyiben az adatkezelő arra hivatkozással nem rögzít egy adatvédelmi incidenst

az incidens-nyilvántartásba, hogy az érintett tájékoztatása már megtörtént, úgy az adatkezelő megsérti az Infotv. fenti rendelkezését, mivel *megnehezíti azt, hogy a Hatóság ellenőrizze az adatvédelmi incidenssel kapcsolatban a Társaság által megtett intézkedéseket.*

2.4. A fentiekre tekintettel a Hatóság felhívja a Társaság figyelmét arra, hogy az Európai Parlament és a Tanács (EU) 2016/679 rendelete (a továbbiakban: Rendelet)[2] alapján – melyet 2018. május 25. napjától kell alkalmazni – az adatkezelőket és az adatfeldolgozókat is egy általános adatvédelmi incidens bejelentési kötelezettség terheli, mely alapján az adatkezelőknek az incidenseket be kell jelenteniük a felügyeleti hatóságnak, illetve, bizonyos esetekben tájékoztatniuk kell az incidensekről az érintetteket is.

A fentieken túl a Rendelet az incidenseket egyértelműen a biztonság sérülésén keresztül határozza meg.[3] Az adatvédelmi incidensekre vonatkozó rendelkezések elhelyezése is ezt támasztja alá, mivel a Rendelet az incidensekkel kapcsolatos kötelezettségeket az adatkezelőre és adatfeldolgozóra vonatkozó szabályok keretében, az adatbiztonsággal kapcsolatos rendelkezések között, az adatbiztonság cím alatt részletezi. Ezt támasztja alá a Rendelet 32. cikk (2) bekezdésének megfogalmazása is, mely szerint a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek. Mint látható, a Rendelet 32. cikk (2) bekezdésének megfogalmazása gyakorlatilag egybeesik az adatvédelmi incidens fogalmával, azaz már a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, melyek adatvédelmi incidensekből származhatnak.

Az elszámoltathatóság elvével[4] összhangban az adatkezelőknek és feldolgozóknak belső adatvédelmi incidens jelző eljárásokat kell kidolgozniuk, valamint fel kell készülniük az incidensek kezelésére és elhárítására, illetve az ilyen eljárásaikat rendszeresen felül kell vizsgálniuk és tesztelniük kell.

Fontos kiemelni, hogy a Rendelet 83. cikk (4) bekezdése alapján az adatvédelmi incidensekre vonatkozó rendelkezések megsértése miatt maximum 10.000.000. EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összegű bírsággal sújtható az adatkezelő és az adatfeldolgozó. A Rendelet 83. cikk (5) bekezdése alapján az adatkezelés elveinek[5] megsértése miatt pedig legfeljebb 20.000.000. EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összegű bírsággal sújtható az adatkezelő és az adatfeldolgozó.

A fentiek alapján a Hatóság megállapította, hogy a Társaság *az adatvédelmi incidens kezelése során megsértette az Infotv. rendelkezéseit, mivel nem tett eleget az Infotv. 15. § (1a) bekezdése alapján fennálló kötelezettségének* akkor, mikor nem rögzítette az adatvédelmi incidensek nyilvántartásába az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és

[2] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

[3] Rendelet 4. cikk 12. „adatvédelmi incidens": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

[4] Rendelet 5. cikk (2)

[5] Rendelet 5. cikk

számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket sem.

3. Az adatbiztonság követelményéről

3.1. Az adatbiztonság elve[6] alapján az adatkezelési műveleteket úgy kell megtervezni és végrehajtani, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, továbbá – a technika mindenkori fejlettségére tekintettel – *meg kell tennie azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek.* Az adatokat 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.

Az Infotv. fenti rendelkezései tehát előírják az adatkezelők számára, hogy az érintettek magánszférájának védelme érdekében adatbiztonsági intézkedéseket kell hozniuk. Ezen belül is hangsúlyos az Infotv. 7. § (3) bekezdése, amely példálódzva felsorolja azokat a kockázatokat, veszélyeket, amelyek elkerülése érdekében az adatkezelőknek megfelelő intézkedéseket kell tenniük.

3.2. Az Infotv. alapvető rendelkezései között találjuk a célhoz kötött és a tisztességes adatkezelés elvét. A fenti elvek alapján személyes adat kizárólag meghatározott célból kezelhető, mely cél csak jog gyakorlása vagy kötelezettség teljesítése lehet.[7] Az adatminimalizálás elvéből következően pedig csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas.[8] Ezen alapelv figyelembevétele szavatolja, hogy az adatkezelés céljára tekintettel csupán a legszűkebb, indokolt adatkör kezelésére kerül sor.

3.3. A Társaság képviselőjének tájékoztatása alapján megállapítható, hogy a Társaság adatkezelőként jogellenesen, megfelelő jogalap és cél nélkül kezelte a Bejelentő – telefonkészülékén tárolt, a Társaság *[...]*-ban található számítógépre lementett – személyes adatait, így a fenti adatkezelés során a Társaság megsértette az Infotv. 4. § (1) – (2) bekezdéseinek rendelkezéseit.

Emellett megállapítható, hogy a *[...]* alkalmazottjának lehetősége volt egyrészt arra, hogy az ott található számítógépre biztonsági mentést készítsen a Bejelentő személyes adatait tartalmazó készülékről, másrészt arra, hogy a fenti adatokat a Társaság több hónapig kezelje, és végül arra is, hogy az adatokat figyelmetlenségből kimásolja egy harmadik személy tulajdonában álló készülékre is, így a Társaság megsértette az Infotv. 7. § (2) – (3) bekezdéseinek rendelkezéseit is.

4. A belső adatvédelmi felelős feladatairól

4.1. Az Infotv. alapján a Társaság szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó belső adatvédelmi felelőst kell kinevezni vagy megbízni.[9] Az Infotv. szerint a belső adatvédelmi felelős egyik feladata, hogy ellenőrizze az Infotv. és az adatkezelésre

[6] Infotv. 7. §
[7] Infotv. 4. § (1)
[8] Infotv. 4. § (2)
[9] Infotv. 24. § (1) c)

vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását.[10]

4.2. A Hatóság álláspontja szerint a Társaság belső adatvédelmi felelőse – ezen ügy kapcsán – nem teljesítette az Infotv. által számára előírt kötelezettségeit, mivel nem rögzítette az Infotv. 15. § (1a) bekezdése szerinti nyilvántartásban az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket sem.

4.3. A Társaság belső adatvédelmi felelőse válaszához csatolta az üggyel összefüggésben küldött belső tájékoztatását, melynek célja a hasonló esetek elkerülése volt. A Társaság belső adatvédelmi felelőse az adatvédelmi incidenshez kapcsolódó intézkedésként felszólította a Társaság munkatársait[11], hogy tegyék meg „a szükséges intézkedéseket, hogy hasonló eset ne fordulhasson elő a jövőben". A Hatóság megállapította, hogy a Társaság belső adatvédelmi felelőse nem tett megfelelő intézkedéseket, mivel túl általános felszólítást küldött ki, illetve a Társaság más munkatársaira hárította egy bizonytalan, túl általános megfogalmazású intézkedés megtételét. A kiküldött belső tájékoztatás mindösszesen egy figyelemfelhívásnak tekinthető, nem pedig intézkedésnek, melyet az a körülmény is alátámaszt, hogy abban tájékoztatást is kért a Társaság munkatársai által megtett intézkedésekről.

A Hatóság álláspontja szerint – a rendelkezésre álló információk alapján – a Társaság belső adatvédelmi felelőse fenti intézkedésével – a belső tájékoztatás kiküldésével – megsértette az Infotv. 21. § (2) a) pontját, mely szerint köteles közreműködni, illetve segítséget nyújtani az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában.[12]

A Hatóság álláspontja szerint megfelelő intézkedésnek minősülhet *például* a Társaság adatvédelmi és adatbiztonsági szabályzatának olyan módosítása, melyben rögzítik, hogy az ügyfélszolgálati eszközökre telepített segédprogramokban ki kell kapcsolni a biztonsági mentés funkciót. Emellett megfelelő intézkedésnek tekinthető *például* az is, ha a Társaság olyan új folyamatokat, ellenőrzési módszereket dolgoz ki, illetve olyan eljárások vezet be, olyan oktatási anyagokat készít a munkatársai számára, melyek elősegíthetik azt, hogy a Társaság adatvédelmi felelőse mielőbb tudomást szerezzen az esetleges adatvédelmi incidensekről.

5. A fentiekre tekintettel a Hatóság az Infotv. 56. § (1) és (2) bekezdései alapján

f e l s z ó l í t j a

a Társaságot, hogy tegye meg az alábbi intézkedéseket:

1. Tegyen eleget az Infotv. 15. § (1a) bekezdésében előírt kötelezettségének, és rögzítse az ügyben vizsgált adatvédelmi incidenst a Társaság incidens-nyilvántartásába!
   A fentiek igazolásaképpen küldje meg – elektronikus formában – a Hatóság részére az Infotv. 15. § (1a) bekezdés szerinti, adatvédelmi incidenseket tartalmazó nyilvántartásból ügyben vizsgált adatvédelmi incidensre vonatkozó teljes bejegyzést!

2. Tegyen lépéseket annak érdekében, hogy a jövőben hasonló adatbiztonsági incidens a Társaságnál ne fordulhasson elő, így tegye meg azokat a technikai és szervezési

[10] Infotv. 24. § (2) b)
[11] Sem a második válaszból, sem annak 5. számú mellékletét képező tájékoztatásból nem derült ki a Hatóság számára az a körülmény, hogy pontosan ki, a Társaság mely munkatársai voltak a tájékoztatás címzettjei.
[12] Infotv. 24. § (2) a), d), f)

intézkedéseket – például az automatikus biztonsági mentés funkció kikapcsolása valamennyi *[...]*-ban elhelyezett számítógépen – és alakítsa ki azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek! A megtett intézkedésekről küldjön részletes – dokumentumokkal alátámasztott – tájékoztatást a Hatóságnak!

3. Tegyen lépéseket annak érdekében, hogy a Társaság munkatársai a jövőben az adatvédelmi incidenseket felismerjék és megfelelően kezeljék, ide értve különösen, de nem kizárólagosan azt, hogy az adatvédelmi incidensekről a Társaság belső adatvédelmi felelősét megfelelő időben értesítsék!

4. A Társaság a fentiek igazolásaképpen küldje meg továbbá az új és a módosított szabályzatokat, belső utasításokat, képzési anyagokat és a munkatársak részére készített tájékoztatókat a Hatóság részére!

Kérem, hogy a felszólítás nyomán megtett intézkedéseiről, illetve – egyet nem értése esetén – álláspontjáról a felszólítás kézhezvételétől számított *harminc (30) napon belül* írásban tájékoztassa a Hatóságot.[13]

Tájékoztatom, hogy a fentiek alapján elkészített, illetve módosított szabályzatokat és belső utasításokat, valamint valamennyi egyéb, a válaszához mellékelni kívánt dokumentumot megküldheti elektronikus formában is a Hatóság részére.

Felhívom figyelmét, hogy amennyiben a fenti felszólítás alapján a jogsérelem, illetve a jogsérelem közvetlen veszélyének megszüntetése érdekében a Társaság nem hozza meg a szükséges lépéseket *úgy a Hatóság adatvédelmi hatósági eljárást indíthat, melynek eredményeképpen a Hatóság – százezertől húszmillió forintig terjedő – bírságot szabhat ki.*[14]

Budapest, 2018. január „ ”

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

[13] Infotv. 56. § (2)
[14] Infotv. 58. § (1) – (2) a); 61. § (1) g); 61. § (3)