Ügyszám: NAIH/2019/2471/6

Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban

H A T Á R O Z A T

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) a **Budapesti Rendőr-főkapitányság** (cím: 1139 Budapest, Teve u. 4-6.) (a továbbiakban: Ügyfél) által 2019. február 25-én postai úton bejelentett adatvédelmi incidenssel (a továbbiakban adatvédelmi incidens) kapcsolatban 2019. március 11. napján megindított hatósági ellenőrzést a mai napon lezárja, egyben az ellenőrzés során feltárt körülmények miatt hivatalból megindított **adatvédelmi hatósági eljárásban**

1. **megállapítja**, hogy az Ügyfél a személyes adatokat tartalmazó pendrive elvesztésével okozott adatvédelmi incidenssel összefüggésben nem tett eleget 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 szóló (EU) 2016/679 rendelet (a továbbiakban: általános adatvédelmi rendelet) 33. cikk (1) bekezdése szerinti, indokolatlan késedelem nélküli, a tudomásszerzéstől számított 72 órán belüli incidensbejelentési kötelezettségének;

2. a fenti jogsértés miatt az Ügyfelet a **jelen határozat véglegessé válásától számított 30 napon belül**

5.000.000 Ft, azaz ötmillió forint

adatvédelmi bírság megfizetésére kötelezi;

3. **utasítja az Ügyfelet**, hogy a jelen határozat véglegessé válásától számított 30 napon belül tegye meg a szükséges intézkedéseket annak érdekében, hogy egy esetleges jövőbeni adatvédelmi incidensek bejelentése az általános adatvédelmi rendelet 33. cikk (1) bekezdésében előírt határidőben valósuljon meg; és

4. **elrendeli** a végleges határozatnak az adatkezelő azonosító adatainak közzétételével történő **nyilvánosságra hozatalát.**

A bírságot a Hatóság központosított bevételek beszedési célelszámolási forintszámlája (10032000-01040425-00000000 Központosított beszedési számla IBAN: HU83 1003 2000 0104 0425 0000 0000) javára kell átutalással megfizetni. Az összeg átutalásakor a NAIH/2019/2471 BÍRS. számra kell hivatkozni.

A 3. pontban előírt intézkedések megtételét az Ügyfélnek az intézkedés megtételétől számított 10 napon belül kell írásban – az azt alátámasztó bizonyítékok előterjesztésével együtt – igazolnia a Hatóság felé.

Amennyiben a Kötelezett a bírságfizetési kötelezettségének határidőben nem tesz eleget, késedelmi pótlékot köteles fizetni. A késedelmi pótlék mértéke a törvényes kamat, amely a késedelemmel érintett naptári félév első napján érvényes jegybanki alapkamattal egyezik meg. A késedelmi pótlékot a Hatóság központosított bevételek beszedési célelszámolási forintszámlája (10032000-01040425-00000000 Központosított beszedési számla) javára kell megfizetni.

A 3. pont szerinti kötelezés nem teljesítése, illetve a 2. pont szerinti bírság és a késedelmi pótlék meg nem fizetése esetén a Hatóság elrendeli a határozat, a bírság és a késedelmi pótlék végrehajtását.

Jelen határozattal szemben közigazgatási úton jogorvoslatnak nincs helye, de az a közléstől számított 30 napon belül a Fővárosi Törvényszékhez címzett keresettel közigazgatási perben megtámadható. A keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak. A tárgyalás tartása iránti kérelmet a keresetben jelezni kell. A teljes személyes illetékmentességben nem részesülők számára a bírósági felülvizsgálati eljárás illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

INDOKOLÁS

I. Tényállás, előzmények

A Hatóság az Ügyfél által postai úton 2019. február 25-én bejelentett adatvédelmi incidenssel kapcsolatban – az általános adatvédelmi rendelet 33-34. cikkében foglalt kötelezettségek teljesítése tárgyában – 2019. március 11. napján NAIH/2019/2471 ügyszámon hatósági ellenőrzés megindításáról döntött, egyben a bejelentésben szereplő információk pontosítása, kiegészítése céljából tényállástisztázó végzéseket küldött az Ügyfél részére. Az első NAIH/2019/2471/2. számú tényállás tisztázó végzésre adott, 2019. március 20. napján kelt válasz 2019. március 26-án érkezett meg a Hatóság részére. A második NAIH/2019/2471/4. számú tényállás tisztázó végzésre adott, 2019. június 4-én kelt válasz 2019. június 11-én érkezett meg a Hatóság részére.

Az incidensbejelentésből, valamint a Hatóság által kiküldött tényállás tisztázó végzésekre adott válaszokból az adatvédelmi incidensre az alábbiakban részletezettek szerint került sor.

A 2019. február 25-i incidensbejelentés szerint 2019. január 11. napon […] a Budapesti Rendőr-főkapitányság […] szolgálati feladatai ellátása során, az általa adattárolásra használt egyik 4 GB tárhellyel rendelkező pendrive-ot elveszítette. Az adathordozón megtalálható volt a BRFK teljes nevesített személyzeti állománytáblája, továbbá a rendvédelmi szolgálati jogviszonyváltásra vonatkozó teljes személyügyi anyag elektronikus másolatban. Az incidenssel érintett személyek számát az Ügyfél 1733 főben jelölte meg, amely a rendvédelmi alkalmazotti jogviszonnyal érintett teljes állományt takarja. Az adathordozó, valamint az azon található állományok semmilyen hozzáférésvédelemmel (pl. jelszó, titkosítás) nem voltak ellátva. Az adathordozón nem szerepelt egyébként olyan anyag, amely más forrásból ne lenne helyreállítható.

A Hatóság NAIH/2019/2471/2. számú tényállástisztázó végzésére Ügyfél által adott válaszok szerint a pendrive elveszítésére úgy került sor, hogy […] 2019. január 10-11. között […] kihelyezett vezetői értekezleten vett részt, amely során használta az adathordozót. A 2019. január 10-i értekezlet után […] az adathordozót a gépjárműve indítókulcsán helyezte el, a kulcsot pedig a szállodai szobába vitte. Az értekezlet második napján, 2019. január 11-én a szállodából

kijelentkezett, majd a helyszínt elhagyta és – egy gyorséttermi kitérőt követően – visszatért a szolgálati helyére Budapesten. A visszaérkezést követően észlelte, hogy az adathordozó nem található meg a kulcskarikán. Az adathordozó elveszítésének tényét és az érintett adatok körét még aznap telefonon jelentette a közvetlen szolgálati elöljárójának.

Az adathordozó feltalálására […] azonnali intézkedéseket foganatosított, így felvette a kapcsolatot a vele a szállodai szobát együtt használó […] (aki ekkor még a szállodában tartózkodott), a szálloda recepciójával, valamint […] a gyorsétterem parkolójának ellenőrzése céljából is. A keresési intézkedések sajnos azonban nem vezettek eredményre. Később […] visszatérő ellenőrzéseket is folytatott, és többször is felvette a szállodával a kapcsolatot az adathordozó esetleges megkerülésével kapcsolatban, de továbbra sem sikerült az eszköz hollétére vonatkozó információkat szerezni.

A pendrive-on tárolt adatokkal kapcsolatban az Ügyfél előadta, hogy a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény módosítása miatt a rendvédelmi ágazatban foglalkoztatott közalkalmazottak 2019. február 1-jei hatállyal rendvédelmi igazgatási szolgálati jogviszonyban történő tovább foglalkoztatására került sor. A vezetői értekezletre az adathordozón szereplő állománytáblában feltüntetett személyek adatai azért kerültek átmásolásra, mert az értekezleten részt vevő munkáltatói jogkört gyakorló vezetők részére bemutatásra kerültek az állományukba tartozó munkavállalók egyénre szabott rendvédelmi igazgatási szolgálati jogviszonyban történő jogviszonyváltásának tervezete. Az adathordozóra átmásolt személyes adatok általános jellegűek, az egyének beazonosítását elősegítő adatok voltak. Az dokumentumokban a következő személyes adatok szerepeltek a mintegy 1733 érintett személlyel kapcsolatban: születési név, születési idő, anyja neve, TAJ szám, beosztás, munkakör.

Az Ügyfél arról is tájékoztatta a Hatóságot, hogy […] a személyes adatokat tartalmazó dokumentumokat nem a szolgálati, hanem magáncélra használt adathordozóra másolta át, és nem alkalmazott semmilyen biztonsági intézkedést a tárolt adatokkal kapcsolatban, ezzel pedig megszegte az Ügyfél Informatikai Biztonsági Szabályzatáról szóló 18/2018. (V. 31.) ORFK utasításában foglaltakat, így különösen a 109., 116. és 118. pontjait.[1] Erre tekintettel Budapest Rendőrfőkapitánya – azóta jogerősen lezárult – fegyelmi eljárást rendelt el nevezettel szemben.

Az adatokhoz való jogosulatlan hozzáférés tényére utaló információ, körülmény nem jutott az Ügyfél tudomására. Bejelentés a pendrive megtalálásával, illetve az adatokkal való visszaéléssel kapcsolatban nem érkezett az Ügyfélhez azóta sem. Az Ügyfél valószínűsíti, hogy az adathordozó az elveszítésének időpontjában fennálló időjárási körülmények miatt (hó, fagy, sáros környezet) megsemmisült. A nem megfelelően védett, átmásolt adatok elveszítésén túl így további biztonsági esemény (pl. jogosulatlan hozzáférés, nyilvánosságra hozatal) az adatokkal kapcsolatban nagy valószínűséggel nem történt.

[1] 18/2018. (V. 31.) ORFK utasítás:
109. pont: A Rendőrség által biztosított felhasználói eszközöket jelszavas védelemmel kell ellátni. Az eszköz zárolásra kerül 5 perc inaktivitást követően.
116. pont: Az adatot tartalmazó adathordozókat védelmi kell a jogosulatlan hozzáféréstől, visszaéléstől és megrongálódástól.
118. pont: A mobil eszközöket biztonságos módon kell kezelni, annak érdekében, hogy ne kerülhessenek illetéktelen felhasználásra, ezért amennyiben a technológia rendelkezésre áll, a rajta tárolt információkat központi management eszközzel titkosítva kell tárolni.

Az Ügyfél tájékoztatta arról a Hatóságot, hogy az incidenst milyen tartalommal vette az általános adatvédelmi rendelet 33. cikk (5) bekezdése szerinti nyilvántartásba.

Az Ügyfél a fentieken túl továbbította a Hatóságnak az incidenssel kapcsolatban elrendelt parancsnoki kivizsgálás eredményeit tartalmazó, 2019. február 8-án kelt jegyzőkönyvet, továbbá az Országos Rendőr-főkapitányság (a továbbiakban: ORFK) Ügyfélnek címzett, 2019. február 12-én kelt (ügyiratszám: 29000/4423-1/2019. ált.) válaszát, amely az adatvédelmi incidens kockázatértékelésével kapcsolatban tartalmaz általános megállapításokat és szakirányítást.

A jövőbeli hasonló incidensek elkerülése és a kockázatok mérséklése érdekében az Ügyfél belső ellenőrzést folytatott le, hogy az adatok tárolására szolgáló külső adathordozók nyilvántartása, kezelése, átadás-átvételének dokumentálása, megsemmisítése az ideiglenes adatvédelmi szabályzatról szóló 15/2018. (V. 25.) számú ORFK utasításban foglaltaknak megfelelően történjen. Ezen felül – az ORFK által javasoltakat is figyelembe véve – felhívta az állomány figyelmét az adatvédelemmel kapcsolatos szabályok mindenkori maradéktalan betartására.

A Hatóság a fentieken túl NAIH/2019/2471/4. számon újabb tényállástisztázó végzést küldött az Ügyfél részére. Az Ügyfél által a végzésre adott válaszok szerint […] 2019. január 11-én (péntek), az incidens észlelése után jelentette a pendrive elveszítését közvetlen szolgálati elöljárójának. Az incidensről szóló jelentést […] 2019. január 14-én (hétfő) 07:30-kor készítette el, amelyet ezután leadott Budapest rendőrfőkapitányának. A szolgálati elöljáró így legkorábban már 2019. január 11-én tudomást szerzett az incidenst bekövetkezéséről, amelynek hivatalos írásbeli megerősítésére az incidenst okozó személy által 2019. január 14-én került sor.

Ezt követően került sor az incidens körülményeinek tisztázása érdekében parancsnoki kivizsgálása elrendelésére. Az Ügyfél adatvédelmi tisztviselőjének az adathordozó elveszítésének körülményeit feltáró, […] által korábban készített rendőri jelentés 2019. január 28-án 07:30-kor került átadásra. Az adatvédelmi tisztviselő így legkorábban ebben az időpontban értesülhetett az incidensről. A parancsnoki kivizsgálás befejezésére 2019. február 8-án került sor.

Az Ügyfél adatvédelmi tisztviselője a parancsnoki kivizsgálás befejezését követően 2019. február 8-án 13:50-kor kereste meg az ORFK-t, melyben állásfoglalást kért arról, hogy az adatvédelmi incidens az érintettek jogait és szabadságait érintően milyen szintű kockázattal jár. Az ORFK már fentiekben is hivatkozott, 29000/4423-1/2019. ált. számú állásfoglalása 2019. február 12-én 15:45-kor került kézbesítésre az Ügyfél részére.

Az ORFK állásfoglalása szerint a bekövetkezett incidens alapvetően kockázatosnak tekinthető, mivel abban nem csak közérdekből nyilvános adatok (név, beosztás), hanem más, egyébként nem nyilvános adatok is (születési adatok, TAJ szám) érintettek. Az azokhoz való jogosulatlan hozzáférés, nyilvánosságra hozatal, vagy közlés azonban nem állapítható meg, továbbá az incidensben különleges adatok sem érintettek, amely a kockázatokat mérséklő körülmény. Az adatok elveszítésén túl azonban, a folyamatos bizalmassági sérülésnek való kitettség kockázata indokolja az ORFK megítélése szerint, hogy az incidenst be kell jelenteni az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján a Hatóságnak. Az ORFK arra is felhívta az Ügyfél figyelmét, hogy az ideiglenes adatvédelmi szabályzatról szóló 15/2018. (V. 25.) számú ORFK utasítás tartalmazza a rendőri szervekre irányadó incidenskezelési szabályzatot (91-101. pontok). Az incidenst elkövető személy az ORFK véleménye szerint nem az e szabályzatban lévő incidenskezelési eljárásrendnek megfelelően járt el, amikor nem jelentette haladéktalanul az adatvédelmi incidenst a szervezeti egység vezetőjének.

A fentiek után az Ügyfél 2019. február 25-én adta fel postai úton az incidesbejelentésre szolgáló, a Hatóság honlapján megtalálható, a szükséges adatokkal kitöltött formanyomtatványt. Az incidensbejelentést tartalmazó levélküldemény végül 2019. február 28-án érkezett meg a Hatósághoz és került iktatásra.

A Hatóság az ellenőrzést lezárta, és mivel a hatáskörébe tartozó jogsértést tapasztalt, megindította hatósági eljárását, amelyben a jelen határozatot hozta.

II. Alkalmazott jogszabályi rendelkezések

Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 99. §-a alapján a hatóság – a hatáskörének keretei között – ellenőrzi a jogszabályban foglalt rendelkezések betartását, valamint a végrehajtható döntésben foglaltak teljesítését.

Az általános adatvédelmi rendelet 2. cikk (1) bekezdése alapján a bejelentett incidenssel érintett adatkezelésre az általános adatvédelmi rendeletet kell alkalmazni.

Az általános adatvédelmi rendelet 4. cikk 12. pontja határozza meg, hogy mi minősül adatvédelmi incidensnek, ez alapján „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.

Az általános adatvédelmi rendelet 33. cikk (1) és (2) bekezdése szerint az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2. § (2) bekezdése szerint az általános adatvédelmi rendeletet az ott megjelölt rendelkezésekben foglalt kiegészítésekkel kell alkalmazni.

Az Ákr. 101. § (1) bekezdés a) pontja alapján, ha a hatóság a hatósági ellenőrzés során jogsértést tapasztal, megindítja a hatósági eljárását. Az Infotv. 38. § (3) bekezdése és 60. § (1) bekezdése alapján a Hatóság az Infotv. 38. § (2) és (2a) bekezdés szerinti feladatkörében a személyes adatok védelméhez való jog érvényesítése érdekében hivatalból adatvédelmi hatósági eljárást folytat.

Az Ákr. 103. § (1) bekezdése alapján az Ákr.-nek a kérelemre indult eljárásokra vonatkozó rendelkezéseit az Ákr. 103 és 104. §-ában foglalt eltérésekkel kell alkalmazni.

Az Infotv. 61. § (1) bekezdés a) pontja alapján a Hatóság a 2. § (2) és (4) bekezdésében meghatározott adatkezelési műveletekkel összefüggésben az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja.

Az általános adatvédelmi rendelet 83. cikk (7) bekezdése szerint, a felügyeleti hatóságok 58. cikk (2) bekezdése szerinti korrekciós hatáskörének sérelme nélkül, minden egyes tagállam megállapíthatja az arra vonatkozó szabályokat, hogy az adott tagállami székhelyű közhatalmi vagy egyéb, közfeladatot ellátó szervvel szemben kiszabható-e közigazgatási bírság, és ha igen, milyen mértékű. Az Infotv. 61. § (4) bekezdés b) pontja alapján, a bírság mértéke százezertől húszmillió forintig terjedhet, ha az adatvédelmi hatósági eljárásban hozott határozatban kiszabott bírság megfizetésére kötelezett költségvetési szerv, az általános adatvédelmi rendelet 83. cikke szerint kiszabott bírság esetén.

Az általános adatvédelmi rendelet 58. cikk (2) bekezdés b) és i) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva elmarasztalja az adatkezelőt vagy adatfeldolgozót, ha adatkezelési tevékenysége megsértette a rendelet rendelkezéseit, illetve a 83. cikknek megfelelően közigazgatási bírságot szab ki, az adott eset körülményeitől függően az e bekezdésben említett intézkedéseken túlmenően vagy azok helyett. Ugyanezen cikk (2) bekezdés d) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva utasítja az adatkezelőt vagy az adatfeldolgozót, hogy adatkezelési műveleteit – adott esetben meghatározott módon és meghatározott időn belül – hozza összhangba a rendelet rendelkezéseivel.

A közigazgatási bírság kiszabására vonatkozó feltételeket az általános adatvédelmi rendelet 83. cikke tartalmazza. Az Infotv. 75/A. § - a szerint a Hatóság az általános adatvédelmi rendelet 83. cikk (2)-(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi rendelet 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik.

Az Infotv. 61. § (2) bekezdés b) pontja alapján, a Hatóság elrendelheti határozatának – az adatkezelő, illetve az adatfeldolgozó azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt közfeladatot ellátó szerv tevékenységével összefüggésben hozta.

Az Ákr. 104. § (1) bekezdés a) pontja szerint a Hatóság az illetékességi területén hivatalból megindítja az eljárást, ha az eljárás megindítására okot adó körülmény jut a tudomására; ugyanezen bekezdés (3) bekezdése alapján a hivatalbóli eljárás az első eljárási cselekmény elvégzésének napján kezdődik, megindításáról az ismert ügyfél értesítése mellőzhető, ha az eljárás megindítása után a hatóság nyolc napon belül dönt.

III. Döntés

A Hatóság a feltárt tényállás alapján megállapította, hogy a bejelentett adatvédelmi incidenssel kapcsolatban az Ügyfél az ORFK véleményének felhasználásával elvégzett egy kockázatelemzést, amely során azt állapította meg, hogy az kockázattal jár az érintettek jogaira és szabadságaira nézve, így az incidenst bejelentette a Hatóságnak.

A Hatóság megítélése szerint az incidens kockázatértékelése elfogadható. A Hatóság e körben egyetért azzal, hogy az incidens kockázatos besorolását az adja, hogy a pendrive-on tárolt adatok között megtalálhatóak voltak nem nyilvánosan hozzáférhető, illetve nem közérdekből nyilvános adatok is, így az érintettek születési adatai, anyjuk neve és TAJ száma. Ezen, nem nyilvánosan hozzáférhető adatok folyamatos bizalmassági sérülésnek való kitettsége pedig olyan kockázati

tényező, amely indokolja az incidens bejelentését az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből – így jelen ügyben az adatok pendrive-on való tárolásából – személyazonosság-lopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül. Az érintettek születési adatai, anyjuk neve és különösképpen TAJ száma (a név és munkahely, beosztás ismerete mellett) olyan adatok, amelyekkel elkövethető személyazonosság-lopás, személyazonossággal visszaélés.

A Hatóság kiemeli, hogy az adatvédelmi incidens fogalmának elemei közül csak az adatok elveszítése valósult meg jelen esetben. A biztonsági sérülés tehát közvetlenül csak az elveszítést eredményezte, másfajta incidens megvalósulására (pl. jogosulatlan hozzáférés, nyilvánosságra hozatal) nem utal konkrét körülmény. A további bizalmassági sérülésnek való kitettség kockázata azonban fennáll az ügyben, mivel az adathordozó és azon tárolt adatok nem voltak semmilyen technikai intézkedéssel védve a jogosulatlan hozzáféréstől. Az ilyen adatok megfelelő védelem nélküli elveszítése ezért önmagában is kockázatos adatvédelmi incidenst eredményez, akkor is, ha egyébként az azokhoz való jogosulatlan hozzáférés, nyilvánosságra hozatal, vagy az adatokkal való egyéb visszaélés ténye nem is állapítható meg.

A kockázatos adatvédelmi incidens bejelentésére azonban nem került sor az általános adatvédelmi rendelet 33. cikk (1) bekezdése által meghatározott határidőben, vagyis indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens az adatkezelő tudomására jutott.

Az Ügyfél úgy nyilatkozott, hogy a pendrive elveszítésére valószínűleg 2019. január 11-én került sor és aznap erről […] rövid úton a szolgálati elöljáróját is tájékoztatta, ezért a Hatóság megítélése szerint az Ügyfél általi hivatalos tudomásszerzésnek ez az időpont minősül. A Hatóság megítélése szerint a tudomásszerzés idejének megítélése szempontjából elég, ha olyan érdemi ügyintéző / elöljáró tudomására jut az incidens bekövetkezésének ténye az adatkezelőnél, aki azt nem maga okozta, és akinek minden lehetősége és eszköze megvolt a releváns döntéshozók, tisztviselő értesítésére. Ezt az értelmezést alátámasztja a 29. cikk szerinti Adatvédelmi Munkacsoport iránymutatása is az adatvédelmi incidens bejelentéséről, amely alapján „tudomásszerzésnek az minősül, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.”[2]

Az Ügyfélnek a fentiek alapján 2019. január 11. napon, a szolgálati elöljáró tudomásszerzésétől számítva 72 óra állt rendelkezésére arra, hogy az incidens által jelentett kockázatokat mérlegelje és azzal kapcsolatban megtegye az esetleges bejelentést a Hatósághoz, amennyiben azt állapítja meg, hogy az incidens kockázattal jár az érintettek jogaira és szabadságaira nézve. Ehhez képest a Hatóságnak az incidensbejelentés megküldésére – a postai borítékon lévő, a küldemény feladása dátumát igazoló postai pecsét szerint – 2019. február 25-én került sor. Ezek alapján az incidensről való tudomásszerzés és a bejelentés között összesen 45 nap telt el, amely az általános adatvédelmi rendelet által főszabályként előírt bejelentési határidő tizenötszörös túllépését jelenti.

A Hatóság az incidensbejelentési kötelezettséggel kapcsolatban kihangsúlyozza, hogy ha a tudomásszerzéstől számított 72 órás határidőt az adatkezelő nem tudja tartani, úgy minden

[2] Lásd: 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, 10. oldal.

esetben igazolnia kell a késedelmes bejelentés indokait a Hatóság felé. A késedelmes bejelentés indokait az adatkezelő abban jelölte meg az incidensbejelentésében, hogy az ügy teljes körű parancsnoki kivizsgálása volt szükséges, valamint állásfoglalást kért az ORFK-tól arra vonatkozóan, hogy az incidens az érintettek jogai és szabadságai tekintetében milyen kockázatúként értékelhető. A parancsnoki kivizsgálás az ügyben 2019. február 8-án zárult le, az ORFK állásfoglalása pedig 2019. február 12-én 15:45-kor került kézbesítésre az Ügyfél részére.

A Hatóság nem tudja elfogadni az Ügyfél fenti indokait a bejelentési határidő többszörös túllépésére vonatkozóan. Ennek oka, hogy az incidens bekövetkezésének összes körülményéről, és az érintett személyes adatok köréről az Ügyfél már 2019. január 11-én, az erről szóló rövid utas értesítés megtételekor tudomást szerzett a pendrive-ot véletlenül elveszítő […]-tól. Az incidens kockázatértékeléséhez szükséges valamennyi tény és körülmény gyakorlatilag ettől az időponttól kezdve rendelkezésére állt az Ügyfélnek, illetve rövid úton tudott volna egyeztetni az incidensben érintett munkavállalójával annak további pontosítása érdekében. A Hatóság megjegyzi, hogy irreleváns a 72 órás bejelentési határidő számítása szempontjából, hogy az incidens pénteki napon történt és ezért az incidensbejelentési határidő hétvégi napokat is magába foglalt. Ez különösen azért is igaz, mivel az Ügyfél olyan kiemelt jelentőségű rendvédelmi feladatokat ellátó államigazgatási szervként működik, amelynek gyakorlatilag az év minden napján, napi 24 órában biztosítania kell, hogy el tudja látni a közfeladatait.

Az Ügyfél által hivatkozott parancsnoki kivizsgálás eredményének bevárása nem szolgáltathat önmagában indokot az incidens késedelmes bejelentésére, különösképpen azért, mert annak fő célja nem is az incidenst kockázatainak értékelése volt, hanem az abban érintett munkavállaló fegyelmi felelősségének megállapítása. Ezt támasztja alá, hogy a kivizsgálásról készült jegyzőkönyv végén is csupán a fegyelmi felelősség kérdésében van megállapítás az Ügyfél informatikai szabályzatának megsértése miatt.

A Hatóság továbbá az ORFK kockázatértékeléssel kapcsolatos válaszának bevárását sem tudja elfogadni, mint a 72 órás bejelentési határidő átlépésére vonatkozó indokot. A Hatóság ezzel kapcsolatban kiemeli, hogy Ügyfél bűnüldözési, bűnmegelőzési, rendvédelmi és igazgatásrendészeti feladatokat ellátó költségvetési szerv, és mint ilyen a személyes adatok kezelése szempontjából kiemelt jelentőségű államigazgatási intézmény. Működése során nagyszámban kezel rendkívül érzékeny, önmagában is magas kockázatot jelentő személyes adatokat. Az Ügyfél által végzett adatkezelésekben főként nem is az incidensben érintett, a foglalkoztatási jogviszonnyal összefüggő személyes adatok érintettek, hanem bűnüldözési célból[3] kezelt, rendkívül érzékeny adatok. A Hatóság megítélése szerint ezért Ügyfélnél elvárható, hogy az adatvédelmi tudatosság szintje rendkívül magas legyen. Elvárható ezért az Ügyféltől, hogy ha egy adatvédelmi incidens a tudomására jut, azzal kapcsolatban önállóan el tudja végezni a kockázatok értékelését és mérlegelni tudja, hogy az bejelentési kötelezettség alá esik-e vagy sem. Ez főként igaz a jelen ügy tárgyát képező esetre, ahol gyakorlatilag a tudomásszerzés időpontjában valamennyi releváns adat rendelkezésre állt.

[3] Lásd: Infotv. 3. § 10a. pont: *bűnüldözési célú adatkezelés:* a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából - ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is - (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése.

Ezzel összefüggésben hangsúlyozandó, hogy a Hatóságnak való bejelentés főszabály szerint kötelező, és csak akkor mellőzhető, ha valószínűsíthető, hogy az incidensnek semmilyen kockázata nincs az érintettekre nézve. Márpedig ha az incidens kockázatának megítélése a jelen ügyben nehézséget jelentett, az már önmagában arra mutat, hogy a bejelentés mellőzésének nem álltak fenn a feltételei.

Szükséges azt is megjegyezni, hogy ha a Hatóság a bejelentésre vonatkozó 72 órás határidő átlépésével kapcsolatban elfogadná az Ügyfél azon indokát, hogy szükséges volt az ORFK válaszának bevárása, úgy a válasz 2019. február 12-én 15:45-kor történő megérkezése és az incidens tényleges bejelentése (2019. február 25.) között még mindig további 13 nap telne el, amely szintén többszörösen indokolatlanul túllépi a rendelet szerinti 72 órás határidőt.

A Hatóság a fentiek alapján megállapította, hogy az Ügyfél tudomásszerzése (2019. január 11.) és az adatvédelmi incidens bejelentése (2019. február 25.) között 45 nap telt el. Az Ügyfél nyilatkozatában megjelölt időpont (2019. február 12. nap 15:45 perc) figyelembe vétele esetén is 13 nap telt el az incidensről való tudomásszerzés és az incidens Hatóságnak történő bejelentése között.

A Hatóság a késedelem Ügyfél általi igazolását a fentiek alapján nem fogadta el, mivel az általános adatvédelmi rendelet 33. cikkében előírt bejelentési kötelezettség teljesítése érdekében az adatkezelő köteles intézkedni az első figyelmeztető jelzés alapján, és megállapítani, hogy valóban történt-e incidens, és lehetőleg 72 órán belül vizsgálatot folytatni, valamint bizonyítékokat és más lényeges részleteket gyűjteni.

Az incidens időben történő bejelentése előtt az sem lehet akadály, ha nem állnak rendelkezésre pontos információk, mivel az általános adatvédelmi rendelet 33. cikk (4) bekezdése lehetővé teszi, hogy a bejelentésre részletekben, szakaszosan kerüljön sor. A Hatóság hangsúlyozza azt is, hogy incidens észlelése esetén haladéktalanul értesíteni kell a megfelelő vezetési szinten lévő felettest, hogy az incidenst kezelni és szükség szerint jelenteni lehessen a 33. és – adott esetben – a 34. cikknek megfelelően.[4] Az incidens megfelelő kezelése szempontjából a bejelentés szakaszos megtétele elfogadható megoldás az adatkezelő részéről akkor, ha egyébként nem teljesen biztos a kockázatok értékelését illetően, illetve ennek lefolytatására még nem áll rendelkezésére valamennyi információt, azt azonban már nagy valószínűséggel meg tudja állapítani, hogy adatvédelmi incidens történt.

Jelen esetben az incidens technikai szempontból viszonylag egyszerű megítélésű és azzal kapcsolatban a legtöbb adat (lényegében a bejelentés megtételéhez szükséges összes releváns adat) már a tudomásszerzés időpontjában rendelkezésre állt, így a 72 órán belüli – akár szakaszos – bejelentéstétel feltételei mindenképpen adottak voltak. Nincs annak akadálya, hogy az adatkezelő kiegészítse az incicensbejelentését a 72 órás határidőt követően tudomására jutott tényekkel (pl. jelen ügyben a parancsnoki kivizsgálás eredményével, illetve az ORFK-tól kért állásfoglalással).

[4] Vö. A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv 29. cikke szerint létrehozott Adatvédelmi Munkacsoport WP 250rev.01 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, melyet az Európai Adatvédelmi Testület is álláspontjaként ismert el.

A Hatóság kiemeli továbbá, hogy ha az adatkezelő rendelkezik adatvédelmi tisztviselővel, úgy őt az incidens bekövetkezéséről a tudomásszerzés után haladéktalanul értesíteni kell, hogy a szükséges intézkedéseket megtehesse. Jelen ügyben az adatvédelmi tisztviselő értesítésére is bőven a tudomásszerzéstől számított 72 órán túl, 2019. január 28-án 07:30-kor került sor, amely a Hatóság megítélése szerint szintén elfogadhatatlan gyakorlat az Ügyfél részéről.

A Hatóság végül figyelembe vette azt, hogy az Ügyfél rendelkezik az adatvédelmi incidensek kezelésére vonatkozó belső eljárásrenddel, amelyet a már többször hivatkozott, az ideiglenes adatvédelmi szabályzatról szóló 15/2018. (V. 25.) számú ORFK utasítás (a továbbiakban: Utasítás) tartalmaz. Az Ügyfél az ügy tárgyát képező adatvédelmi incidens kezelésével kapcsolatban nem csak az általános adatvédelmi rendeletben foglaltakat, hanem saját belső eljárásrendjét sem tartotta be az alábbiak miatt.

Az Utasítás 93. pontja alapján az adatvédelmi incidens észlelését követően azt azonnal jelenteni kell a szervezeti egység vezetőjének. A jelen ügyben ez megtörtént, hiszen az incidenst okozó személy a rendelkezésre álló adatok alapján azt még a pendrive elveszítésének napján rövid úton jelentette szolgálati elöljárójának, továbbá erről (még mindig 72 órán belül) rendőri jelentésben tájékoztatta a szervezeti egység vezetőjét, így Budapest rendőrfőkapitányát. A Hatóság véleménye szerint ezért az adatvédelmi incidens kezelése szempontjából, az azt okozó […] megfelelően kezelte a kialakult helyzetet, mind az általános adatvédelmi rendelet által támasztott elvárások, mind az Utasításban foglaltak alapján. Az incidenskezelés szempontjából részére ezért csupán az Ügyfél informatikai biztonsági előírásainak be nem tartása róható fel (ennek felrovására pedig fegyelmi eljárásban is sor került).

Az Utasítás 94. pontja alapján a szervezeti egység vezetője vagy az általa kijelölt személy a jelzést követően azonnal tájékozódik az eset lényeges körülményeiről és a kárenyhítési intézkedések megtétele mellett értékeli annak az érintettek jogaira nézve gyakorolt hatásának súlyosságát. Az Utasítás 95. pontja alapján a hatások felmérése után a szervezeti egység vezetője vagy az általa kijelölt személy felméri az incidenssel jelentett kockázatokat. Amennyiben úgy ítéli meg, hogy az incidens kockázatos besorolású, úgy soron kívül és a szolgálati út kihagyásával közvetlenül értesíti a szerv adatvédelmi tisztviselőjét.

A jelen ügyben az Utasítás fenti, 94-95. pontjai szerinti előírások betartására már nem került sor. Az Ügyfél a tudomásszerzést követően nem tájékozódott azonnal és nem mérte fel saját maga a kockázatokat, valamint nem értesítette soron kívül a szerv adatvédelmi tisztviselőjét. A kockázatok értékelését az Ügyfél az incidens viszonylag egyszerű megítélése és a releváns adatok rendelkezésre állása ellenére nem végezte el saját hatáskörben, hanem azzal kapcsolatban bevárta az ORFK válaszát, amely 2019. február 12-én érkezett meg. Az adatvédelmi tisztviselő értesítésére is csak jóval később, a tudomásszerzéstől számított 72 órán túl, 2019. január 28-án került sor.

Az Utasítás 98. pontja szerint az adatvédelmi tisztviselő indokolatlan késedelem nélkül, de legkésőbb az észleléstől számított 72 órán belül a rendelkezésre álló adatokat bejelenti a Hatóságoz az e célból rendszeresített felületen keresztül […]. Az Utasítás 99. pontja kiemeli, hogy ha a bejelentés nem tehető meg 72 órán belül, akkor meg kell jelölni a késedelem okait, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet. Az Ügyfél az incidenskezeléssel kapcsolatban ezen előírásokat sem tartotta be, hiszen nem történt meg az incidens – akár szakaszos – bejelentése a Hatóság felé az előírt határidőben, annak ellenére, hogy az eset értékelésével kapcsolatban valamennyi releváns információ rendelkezésre

állt. Megjegyzendő, hogy az eset indokolatlan késedelem nélküli bejelentésére még akkor sem került sor, amikor az Ügyfél már megkapta az ORFK-tól a kért állásfoglalást 2019. február 12-én, hiszen a tényleges bejelentés megtételével még innen számítva is további 13 napot várt, egészen 2019. február 25-ig.

A fentiek alapján a Hatóság megállapította, hogy az Ügyfél megsértette az általános adatvédelmi rendelet 33. cikk (1) bekezdésében foglalt kötelezettségét, mivel az alapvetően kockázatos adatvédelmi incidenst nem jelentette be a tudomásszerzést követően indokolatlan késedelem nélkül. Tette ezt annak ellenére, hogy az incidenskezeléssel kapcsolatban belső eljárásrenddel is rendelkezik, amely előírásainak szintén nem feleltethető meg az incidens kezelése.

A Hatóság emellett utasította az Ügyfelet arra, hogy tegye meg a szükséges intézkedéseket annak érdekében, hogy egy esetleges jövőbeni adatvédelmi incidens bejelentése az általános adatvédelmi rendelet 33. cikk (1) bekezdésében előírt határidőben megvalósuljon.

A Hatóság az alkalmazott bírsággal kapcsolatos döntés során a rendelet 83. cikk (2) bekezdése alapján mérlegelte az ügy összes körülményét. Annak eldöntésekor, hogy szükség van-e közigazgatási bírság kiszabására, illetve a közigazgatási bírság összegének megállapítása során, az alábbiakat vette figyelembe.

Ügyfél költségvetési szerv, melynek esetében az Infotv. 61. § (4) bekezdés b) pontja alapján a bírság mértéke százezertől húszmillió forintig (HUF) terjedhet. Az Ügyfelet ezt megelőzően a személyes adatok védelmére vonatkozó jogszabályi rendelkezések megsértése miatt a Hatóság még nem marasztalta.

A Hatóság az alkalmazott szankció megállapításakor figyelembe vette, hogy az incidenssel érintett személyes adatok kezelése az adatok jellegéből, illetve az érintettek köréből fakadóan magasabb kockázattal jár, mivel azoknak a jogosulatlan megismerése jelentős következménnyel járhat az érintettek számára. A kezelt személyes adatok köre, jellege, valamint az érintettek köre (munkavállalók, szolgálati jogviszonnyal érintettek) is azt támasztják alá, hogy az ilyen adatok kezelésekor az adatkezelőknek fokozott elővigyázatossággal kell eljárniuk, és az ilyen kategóriájú személyes adatokra vonatkozó jogsértés esetén súlyosabb szankcionálás lehet indokolt.

A Hatóság továbbá figyelembe vette, hogy az Ügyfél nem csupán az adatvédelmi incidens Hatóság részére történő bejelentésének nem tett eleget indokolatlan késedelem nélkül, hanem azzal kapcsolatos intézkedések megtételéről – így különösen a kockázatelemzésről – is csak az incidensről való tudomásszerzést követő 27. napon, 2019. február 8-án intézkedett, ráadásul ezt nem is saját hatáskörben végezte el, hanem azt gyakorlatilag a felettes szervével (ORFK) végeztette el. Az Ügyfél incidenskezelése továbbá nem csak az általános adatvédelmi rendelet, hanem saját belső incidenskezelési eljárásrendjének sem feleltethető meg.

Enyhítő körülményként vette figyelembe a Hatóság, hogy a feltárt tényállás alapján az incidens bekövetkezése nem vezethető vissza az Ügyfélnél fennálló komolyabb adatbiztonsági problémára, mivel az adatok elvesztése – a belső informatikai biztonsági szabályzat megsértésével elkövetett – munkavállalói gondatlanság eredménye. A Hatóság emellett azt is figyelembe vette, hogy az Ügyfél, bár nem indokolatlan késedelem nélkül, de bejelentette a Hatóság számára az adatvédelmi incidenst, és az egyéb, az adatvédelmi incidenst követően hozott intézkedései is elfogadhatóak a kockázatok csökkentése érdekében.

A Hatóság figyelemmel volt arra is, hogy az Ügyfél együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – kifejezetten enyhítő körülményként nem értékelte.

A fentiek alapján a Hatóság szükségesnek tartja bírság kiszabását, az Infotv. 75/A. § szerinti figyelmeztetés alkalmazása jelen esetben nem lenne megfelelő jogkövetkezmény. A szankció kapcsán a Hatóság az incidenskezelésben tapasztalható, a szabályozás ellenére fennálló súlyos gyakorlati hiányosságokat rendszerszintű problémának tekintette, ami indokolja a súlyosabb szankció, így a bírság kiszabását. Megjegyzi továbbá a Hatóság, hogy bírság összege meghatározásakor figyelemmel volt arra is, hogy az Ügyfél az ország egyik legnagyobb rendőr-főkapitánysága, amelynek egyrészt minden lehetősége adott, hogy adatkezelési folyamatait megfelelően megszervezze (ez tevékenysége jellegénél fogva sem okozhat semmilyen nehézséget számára), másrészt méretéből adódóan jelentős költségvetési erőforrásokkal rendelkezik, így a bírság szankció is csak akkor érheti el célját, ha legalábbis érzékelhető nagyságú a megbírságolt adatkezelő számára.

Az Ügyfél közfeladatot ellátó, költségvetési szerv, és a jogsértő adatkezelésre e közfeladata ellátásával összefüggésben került sor. A Hatóság ezért az Infotv. 61. § (2) bekezdés b) pontja alapján elrendelte a határozatnak az adatkezelő, vagyis az Ügyfél azonosító adatainak közzétételével történő nyilvánosságra hozatalát.

IV. Egyéb kérdések

A Hatóság hatáskörét az Infotv. 38. § (2) és (2a) bekezdése határozza meg, illetékessége az ország egész területére kiterjed.

Az Ákr. 112. §-a, és 116. § (1) bekezdése, illetve a 114. § (1) bekezdése alapján a határozattal szemben közigazgatási per útján van helye jogorvoslatnak.

A közigazgatási per szabályait a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) határozza meg. A Kp. 12. § (2) bekezdés a) pontja alapján a Hatóság döntésével szembeni közigazgatási per törvényszéki hatáskörbe tartozik, a perre a Kp. 13. § (11) bekezdése alapján a Fővárosi Törvényszék kizárólagosan illetékes. A polgári perrendtartásról szóló 2016. évi CXXX. törvénynek (a továbbiakban: Pp.) – a Kp. 26. § (1) bekezdése alapján alkalmazandó – 72. §-a alapján a törvényszék hatáskörébe tartozó perben a jogi képviselet kötelező. Kp. 39. § (6) bekezdése szerint – ha törvény eltérően nem rendelkezik – a keresetlevél benyújtásának a közigazgatási cselekmény hatályosulására halasztó hatálya nincs.

A Kp. 29. § (1) bekezdése és erre tekintettel a Pp. 604. § szerint alkalmazandó, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) 9. § (1) bekezdés b) pontja szerint az ügyfél jogi képviselője elektronikus kapcsolattartásra kötelezett.

A keresetlevél benyújtásának idejét és helyét a Kp. 39. § (1) bekezdése határozza meg. A tárgyalás tartása iránti kérelem lehetőségéről szóló tájékoztatás a Kp. 77. § (1)-(2) bekezdésén alapul. A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Itv.) 44/A. § (1) bekezdése határozza meg. Az illeték előzetes megfizetése alól az Itv. 59. § (1) bekezdése és 62. § (1) bekezdés h) pontja mentesíti az eljárást kezdeményező felet.

Az Ákr. 132. §-a szerint, ha a kötelezett a hatóság végleges döntésében foglalt kötelezésnek nem tett eleget, az végrehajtható. A Hatóság határozata az Ákr. 82. § (1) bekezdése szerint a közléssel véglegessé válik. Az Ákr. Az Ákr. 133. §-a értelmében a végrehajtást - ha törvény vagy kormányrendelet másként nem rendelkezik - a döntést hozó hatóság rendeli el. Az Ákr. 134. §-a értelmében a végrehajtást - ha törvény, kormányrendelet vagy önkormányzati hatósági ügyben helyi önkormányzat rendelete másként nem rendelkezik - az állami adóhatóság foganatosítja. Az Infotv. 60. § (7) bekezdése alapján a Hatóság határozatában foglalt, meghatározott cselekmény elvégzésére, meghatározott magatartásra, tűrésre vagy abbahagyásra irányuló kötelezés vonatkozásában a határozat végrehajtását a Hatóság foganatosítja.

Budapest, 2019. június 25.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár