Ügyszám: NAIH-2894-3/2021

Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban

Ügyintéző:

H A T Á R O Z A T

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) a **Budapest Főváros Kormányhivatala XI. kerületi Hivatalát** (cím: 1113 Budapest, Bocskai út 39-41.) (a továbbiakban: Ügyfél) érintő adatvédelmi incidenssel kapcsolatban 2020. április 21. napján megindított hatósági ellenőrzés során feltárt körülmények miatt 2020. július 6. napján hivatalból megindított **adatvédelmi hatósági eljárásban**

1) **megállapítja**, **hogy**

   a) Ügyfél megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdés a)-b) pontjait és (2) bekezdését, amikor nem alkalmazott az egészségügyi adatok továbbításának kockázataival arányos adatbiztonsági intézkedéseket: Ügyfél a Covid-19 gyorsteszthez kapcsolódóan kezelt, rendkívül részletes és pontos egészségügyi adatokat és elérhetőségeket is tartalmazó adatbázist egy Excel-fájlban, körzetenkénti leválogatás nélkül, továbbá azok bizalmasságát garantáló hozzáférésvédelem vagy titkosítás alkalmazása nélkül egyszerű e-mailben továbbította a címzett körzeti orvosoknak. Ügyfél ezen adattovábbítással így közvetlenül lehetővé tette a magas kockázatú adatvédelmi incidens bekövetkezését.

   b) Ügyfél megsértette az általános adatvédelmi rendelet 33. cikk (1) bekezdését, amikor a bekövetkezett magas kockázatú adatvédelmi incidensnek a Hatóság felé történő bejelentését nem tartotta szükségesnek, mivel nem megfelelően végezte el a kockázatelemzést.

   c) Ügyfél megsértette az általános adatvédelmi rendelet 34. cikk (1) bekezdését, amikor a bekövetkezett magas kockázatú adatvédelmi incidensről nem kívánta tájékoztatni az érintetteket.

2) **utasítja Ügyfelet, hogy a jelen határozat véglegessé válásától számított 15 napon belül tájékoztassa az érintetteket** a bekövetkezett incidens tényéről és körülményeiről, az érintett személyes adatok köréről és az elhárítás érdekében megtett intézkedésekről

3) a fenti jogsértés miatt Ügyfelet a **jelen határozat véglegessé válásától számított 30 napon belül**

   10.000.000 Ft, azaz tízmillió forint

   adatvédelmi bírság megfizetésére kötelezi;

4) **elrendeli a végleges határozatnak** Ügyfél 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-2894/2021 BÍRS. számra kell hivatkozni.

Amennyiben Ügyfél 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 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 keresetlevéllel közigazgatási perben megtámadható. A szigorított védekezés a keresetindítási határidőt nem érinti. A keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak. A szigorított védekezés ideje alatt a bíróság tárgyaláson kívül jár el, ideértve a perorvoslati eljárásokat is. A tárgyalás tartása iránti kérelmet a keresetlevélben jelezni kell.A teljes személyes illetékmentességben nem részesülők számára a közigazgatási per illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

I N D O K O L Á S

I. Előzmények és a tényállás tisztázása

1) A Hatósághoz egy magánszemély e-mail címéről közérdekű bejelentés érkezett, amelyhez a bejelentő egy neki továbbított e-mail üzenetet és annak mellékleteként egy Excel táblázatot csatolt. A közérdekű bejelentéshez csatolt eredeti e-mailt és táblázatot 2020. április 14-én Budapest Főváros Kormányhivatala, XI. Kerületi Hivatala, Hatósági Főosztály, Népegészségügyi Osztálya küldte meg Budapest XI., XII. és XXII. kerülete valamennyi felnőtt háziorvosa és házi gyermekorvosa részére. Az e-mail aláírója Ügyfél […] volt. A közérdekű bejelentő egyébként nem volt az eredeti üzenet címzettje, azt neki is csak közvetetten továbbították magán e-mail címére egy szintén másik magán e-mail címről. Az e-mail üzenethez mellékelt Excel táblázat 1153 sorban tartalmazza betegek személyes adatait, panaszaikat, vizsgálati eredményüket.

Az e-mail szövege alapján Budapest Főváros Kormányhivatala Népegészségügyi Főosztálya által a Covid-19 járványhoz kapcsolódó megbetegedésekkel kapcsolatosan az Országos Mentőszolgálat által 2020. március 20. és 2020. április 12. közötti időszakban levett minták adatait tartalmazza a fenti budapesti kerületek lakossága kapcsán az Excel táblázat. Az e-mail szerint továbbá a megküldött adatok mennyiségére az egészségügyi szolgáltatók egyéni tájékoztatása nem biztosítható, ezért a feladó felhívja az eredetileg címzett háziorvosok figyelmét az adatok bizalmas kezelésére. Az Excel fájl hozzáférésvédelemmel (pl. jelszó) nem volt ellátva.

A közérdekű bejelentés tartalmazta az eredeti e-mailhez mellékelt, egészségügyi adatokat tartalmazó Excel táblázatot. A táblázatban összesen 1153 érintett alábbi személyes adatai szerepeltek olvasható módon, titkosítás nélkül, bárki által megtekinthető formában:

- beteg teljes neve,

- lakcím (város, kerület, utca, házszám, emelet, ajtó pontossággal, néhol a kapucsengő száma és azon szereplő név is feltüntetésre került),
- beteg mobil és/vagy vezetékes telefonszáma,
- születési dátum,
- foglalkozás, néhol munkahely és végzettség megjelöléssel,
- körzeti orvos neve és címe, pecsétjének száma,
- Covid-19 gyorsteszt eredménye (pozitív/negatív),
- tünetek részletes leírása (pl. lázas, köhög x napja, hőemelkedés, hányás, hasmenés, légszomj, szag és ízérzékelés elveszítése, testhőmérséklet, fájdalmak leírása stb.),
- tesztelés dátuma napra pontosan,
- egyéb megjegyzés (pl. „3 hete Ausztriában járt munkaügyben", „tengerjáró hajón dolgozott: USA, Dél-Amerika több országa", „Izraelből jött haza", „édesapja Covid-19-ben exitált a hétvégén" stb.).

A Hatóság a közérdekű bejelentésre és a mellékelt táblázatban található különleges személyes adatokra tekintettel hatósági ellenőrzést indított 2020. április 21-én, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy az Ügyfél maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak.

A Hatóság a hatósági ellenőrzés során összesen két alkalommal végzéseivel nyilatkozattételre és iratszolgáltatásra szólította fel az Ügyfelet.

2) A Hatóság NAIH/2020/3454/2. számú végzésére Ügyfél által adott nyilatkozat alapján megállapítható, hogy Ügyfél a fertőző betegségek jelentésének rendjéről szóló 1/2014. (I. 16.) EMMI rendelet, a fertőző betegségek és a járványok megelőzése érdekében szükséges járványügyi intézkedésekről szóló 18/1998. (VI. 3.) NM rendelet és a Nemzeti Népegészségügyi Központ által kiadott eljárásrendek alapján végzi az új koronavírus okozta megbetegedéssel kapcsolatos feladatait.

Az Országos Mentőszolgálat 2020. március 19. napját követően kezdte alkalmazni a gyakorlatban az új koronavírus okozta megbetegedések kimutatására a gyorsteszteket. A gyorsteszteket által kimutatott eredmények továbbításáról 2020. április 8. napja előtt egységes álláspont nem született. Ügyfél elmondása szerint a helyzetét az is nehezítette, hogy az érintettek a tesztelés helyszínén azt az információt kapták, hogy az eredménnyel kapcsolatban háziorvosuknál érdeklődhetnek. A háziorvosok viszont Ügyfél Népegészségügyi Osztályánál (a továbbiakban: Osztály) érdeklődtek az eredmények iránt. A háziorvosok érdeklődésére történt meg az egyszeri e-mailes adattovábbítás […] által, amelynek mellékletét képezte az érintettek és háziorvosaik adatait tartalmazó Excel táblázat. Ügyfél […] az e-mailben felhívta a címzett háziorvosok figyelmét az egészségügyi adatok bizalmas kezelésére. Az e-mail-es adattovábbításban érintett adatok kezelésének jogalapjaként Ügyfél az általános adatvédelmi rendelet 9. cikk (1) bekezdés i) pontját jelölte meg.

Ügyfél a Hatóság végzésének kézhézvétele előtt nem minősítette az e-mail fenti módon való elküldését adatvédelmi incidensnek, az adattovábbítás adatvédelmi aggályairól külön jelzés alapján sem értesült. A Hatóság végzésének kézhezvétele után Ügyfél kikérte Budapest Főváros Kormányhivatala adatvédelmi tisztviselőjének véleményét, amely szerint viszont az egészségügyi adatoknak olyan módon történő megküldése a háziorvosok részére Ügyfél Osztálya által, hogy nem történt meg azok körzetenkénti leválogatása az általános adatvédelmi rendelet 4. cikk 12. pontja szerint minősülő adatvédelmi incidenst eredményezett. Az adatvédelmi tisztviselő

véleménye szerint a táblázat elküldése előtt az abban szereplő adatokat körzetenként le kellett volna válogatni és külön-külön megküldeni a háziorvosoknak. Az adatvédelmi tisztviselő szerint az Ügyfél nem mentesülhet a háziorvosok mihamarabbi értesítésének elsőbbségére hivatkozva az alól, hogy a célhoz kötöttség és adattakarékosság általános adatvédelmi rendeletben foglalt alapelveinek megfelelően a személyes adatokat csak az azok megismerésére jogosult címzett ismerhesse meg. Jelen ügyben az adott háziorvos csak a vele orvos-páciens viszonyban lévő érintettek adatait ismerhette volna meg, más betegek adatait nem.

Az adatvédelmi tisztviselő szerint az adatok válogatás nélkül való továbbításával kapcsolatban – függetlenül attól, hogy viszonylag sürgős intézkedések megtétele volt indokolt – megállapítható az adatvédelmi incidens bekövetkezése.

Az adatvédelmi tisztviselő a fentiek mellett azonban azt is kiemelte, hogy véleménye szerint az adatvédelmi incidens nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, így annak az általános adatvédelmi rendelet 33. cikk (1) bekezdése szerinti bejelentése a Hatóság irányába Ügyfél által nem indokolt. Ennek indokaként előadta, hogy a táblázat csak háziorvosok részére került megküldésre. Az Ügyfélnek ezért az incidenst csupán belső adatvédelmi incidens-nyilvántartásában kell rögzítenie az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján. Erről az adatvédelmi tisztviselő intézkedett.

Az Ügyfél álláspontja szerint sem érhette jogsérelem az érintetteket, mivel a járványügyi helyzetben – az arányosság elvére tekintettel – a potenciális fertőzöttek figyelmeztetése, ezáltal a lakosság megóvása nagyobb előnnyel járt, mint az adatok visszatartása a háziorvosoktól. Az Ügyfél ettől függetlenül felhívta a táblázatot megkapó háziorvosokat, hogy a nem a körzetükbe tartozó betegek adatait töröljék. Ezen felül az Ügyfél felülvizsgálja adattovábbítási gyakorlatát a jövőbeli hasonló incidensek elkerülése érdekében.

3) A Hatóság NAIH/2020/3454/7. számú végzésére Ügyfél által adott nyilatkozat alapján megállapítható, hogy adatok közlése kapcsán az Ügyfél közvetlen panaszt, bejelentést nem kapott sem az érintettektől, sem az orvosoktól. Ügyfél tudomása szerint a címzett háziorvosok, a veszélyhelyzet által teremtett körülményeket figyelembe véve, a megküldött adatokat a felhívásnak megfelelően bizalmasan kezelték. A rendelkezésre álló információk alapján a közvetlen betegellátás során senki nem élt vissza az adatokkal.

Ügyfél 2020. május 11-én felhívta az érintett háziorvosokat, hogy a nem a körzetükbe tartozó betegek adatait törölni szíveskedjenek.

Az ügyben az általános adatvédelmi rendelet 32-34. cikkeiben foglalt kötelezettségek Ügyfél általi feltételezhető megsértésének további szükséges vizsgálata miatt az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 60. § (1) bekezdésére tekintettel, a Hatóság a rendelkező részben foglaltak szerint adatvédelmi hatósági eljárás megindításáról döntött. Erről a Hatóság NAIH/2020/3454/9. számú, 2020. július 6-án kelt értesítésével értesített Ügyfelet, amelyet az a visszaérkezett tértivevény szerint 2020. július 9-én vett át.

A hatósági eljárás során a Hatóság nyilatkoztatta Ügyfelet arról NAIH-2894-1/2021. számú végzésével, hogy a hatósági ellenőrzés során tett nyilatkozatait fenntartja-e, továbbá az e-mail címzetti köre valóban csak Ügyfél illetékességi területén működő háziorvosokra terjedt-e ki, a táblázat nem lett-e megosztva esetleg másokkal is Ügyfél által.

Ügyfél válasza alapján fenntartja a hatósági ellenőrzés során tett nyilatkozatait. Ügyfél továbbá azt nyilatkozta, hogy az elektronikus levelet és annak mellékletét kizárólag az egészségügyi alapellátásban közreműködő háziorvosok részére továbbította. Ügyfél szerint az adattovábbítás fontos közérdeket és az érintettek létfontosságú érdekeit („az új koronavírus okozta megbetegedéssel kapcsolatos járványhelyzet terjedésének nyomon követését") szolgálta. Ügyfél ismét hangsúlyozta, hogy felhívta a címzettek figyelmét az adatok bizalmas kezelésére. Ügyfél szerint továbbá az adatközlés körzetenkénti leválogatás nélkül is alkalmas volt arra, hogy a kívánt hatást (a fertőzött személyek beazonosítása) elérje. Ügyfél véleménye szerint a háziorvosok mihamarabbi értesítése elsőbbséget élvezett a körzetenkénti pontos leválogatással kapcsolatos intézkedésekkel szemben.

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 az adatvédelmi 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 4. cikk 15. pontja szerint „egészségügyi adat": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

Az általános adatvédelmi rendelet 32. cikk (1) bekezdése értelmében az adatkezelő és az adatfeldolgozó a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. A rendelet ide érti többek között a 32. cikk (1) bekezdés a) pontja alapján a személyes adatok álnevesítését és titkosítását.

Az általános adatvédelmi rendelet 32. cikk (2) bekezdése értelmében 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.

Az általános adatvédelmi rendelet 33. cikk (1) 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 általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

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 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.

A közigazgatási bírság kiszabására vonatkozó feltételeket az általános adatvédelmi rendelet 83. cikke tartalmazza. A 83. cikk (7) bekezdése alapján 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) bekezdése 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 Infotv. 61. § (2) bekezdése szerint a Hatóság elrendelheti határozatának – az adatkezelő, illetve az adatfeldolgozó azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt közfeladatot ellátó szerv tevékenységével összefüggésben hozta.

A határozatra egyebekben az Ákr. 80. és 81. §-át kell alkalmazni.

III. Döntés

A Hatóság jelen ügyben kizárólag az Ügyfél általi e-mailes adattovábbítás adatvédelmi incidens jellegét, kockázatait, kezelését és alkalmazott adatbiztonsági intézkedéseit értékelte. Az egészségügyi adatok címzettek általi továbbkezelését jelen ügy keretei között nem vizsgálta.

1. Az eset adatvédelmi incidens jellege

Ügyfél elmondása szerint a 2020. április 14-én küldött e-mail-hez az egészségügyi adatok leválogatás nélküli csatolása az e-mailt küldő […] egyszeri döntésére vezethető vissza. Az adatokat továbbító személy részéről az ilyen jellegű egyszeri, eseti adattovábbításra a címzett háziorvosok felé azért került sor, mivel azok többször is érdeklődtek Ügyfél Osztályánál az Országos Mentőszolgálat által korábban levett Covid-19 gyorstesztek eredményei után a pácienseik viszonyában. A teszteredményekkel kapcsolatos kommunikációról nem volt egységes álláspont, továbbá a betegeket is úgy tájékoztatták a mintavételkor, hogy annak eredménye kapcsán háziorvosukat keressék. Az eredmények körzetenkénti leválogatására a háziorvosok folyamatos sürgetése, a járványhelyzet miatti fokozott nyomás és időhiány miatt nem került sor.

Ügyfél az esetet csupán akkor minősítette – a megkérdezett adatvédelmi tisztviselő véleményére is figyelemmel – adatvédelmi incidensnek, amikor a szóban forgó adatok továbbítása kapcsán indított hatósági ellenőrzésről a Hatóság első tényállás tisztázó végzéséből először értesült (a visszaérkezett tértivevény szerint) 2020. április 23-án. Az adatvédelmi incidensről való tudomásszerzésnek így Ügyfél részéről ez az időpont tekinthető.

Az általános adatvédelmi rendelet 4. cikk 12. pontja alapján adatvédelmi incidensnek minősül a biztonság sérülése, amely a kezelt személyes adatokhoz való jogosulatlan hozzáférést eredményezi. A fogalom szempontjából így a biztonsági eseménnyel való kapcsolat kulcselemnek tekinthető. Az adott ügyben a biztonsági sérülés abból adódott, hogy Ügyfél nem alkalmazott megfelelő technikai és szervezési intézkedéseket az egészségügyi adatok bizalmasságának megőrzése érdekében az adattovábbítás során. Az érintettek személyes adatait azok elküldése előtt (legalább) körzetenként le kellett volna válogatnia a küldőnek, így biztosítva azt, hogy minden háziorvos csak a saját körzetébe tartozó betegek adataihoz férhessen hozzá. Ezek alapján tehát a betegadatokhoz való jogosulatlan harmadik fél általi hozzáférés megakadályozására ezt az intézkedést kellett volna többek között alkalmaznia az Ügyfél képviseletében eljárónak.

A Hatóság egyetért Ügyfél adatvédelmi tisztviselőjének azon véleményével, hogy a betegadatokat tartalmazó táblázat oly módon történő továbbítása a háziorvosok részére, hogy abban körzetenkénti válogatás nélkül szerepelnek az érintettek adatai adatvédelmi incidenst eredményezett. Ennek oka, hogy a megfelelő és a kockázatokkal arányos biztonsági intézkedések hiánya miatt a nagyszámú érintett egészségügyi adatait tartalmazó adatbázisban szereplő valamennyi adat olyan címzettek számára is megismerhetővé vált, akik egyébként az adatok töredékének (így csak akivel ténylegesen orvos-páciens viszonyban vannak) megismerésére lennének jogosultak. Az intézkedések hiánya egyébként később azt is lehetővé tette, hogy a nagyszámú egészségügyi adatot olyanok is megismerjék, akik egyáltalán nem tartoznak a címzetti körbe (pl. a közérdekű bejelentő magánszemély, vagy a Hatóság). A megfelelő biztonsági intézkedések hiánya és az adatokhoz való jogosulatlan hozzáférések között így közvetlen ok-okozati összefüggés áll fenn.

Azt maga az Ügyfél is elismerte, hogy az érintettek adatainak egy táblázatban való, leválogatás nélküli továbbítása az ügyintéző részéről a járványhelyzet miatti nyomás és az ügymenet

gyorsítása miatt történt. Ezért is hívta fel az e-mailt küldő a háziorvosok figyelmét a körülmények méltányolhatósága okán az adatok bizalmas kezelésére. A Hatóság álláspontja szerint azonban önmagában a figyelemfelhívás nem elégséges intézkedés a bizalmasság és az adatok biztonságos kezelésének garantálása érdekében.

Az Ügyfél általi e-mailes adattovábbítás a nem megfelelő biztonsági intézkedések hiányában így az általános adatvédelmi rendelet 4. cikk 12. pontja szerinti adatvédelmi incidenst eredményezett.

2. A bekövetkezett adatvédelmi incidens kockázati besorolása

Az általános adatvédelmi rendelet 33. cikk (1) bekezdése szerint az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, köteles bejelenteni a felügyeleti hatóságnak. Az incidens bejelentése csak akkor mellőzhető, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az incidenssel járó kockázatok felmérése az adatkezelő feladata.

Az Ügyfél az incidens kapcsán utólagosan elvégzett kockázatértékelése szerint az incidens nem járt kockázattal a természetes személyek jogaira és szabadságaira nézve, így annak bejelentését a Hatóság felé szükségtelennek tartotta. Ennek indokaként azt jelölte meg, hogy a táblázat kizárólag háziorvosok részére került megküldésre, így az érintetteket komoly jogsérelem nem érhette. Ettől függetlenül az Ügyfél utólag felhívta a címzetti kört, hogy a nem körzetükbe tartozó betegek adatait töröljék.

A Hatóság a bekövetkezett adatvédelmi incidens Ügyfél által elvégzett kockázatértékelése kapcsán elsősorban arra hívja fel a figyelmet, hogy az általános adatvédelmi rendelet (75) preambulumbekezdése az olyan adatkezelést, amely során nagy számban egészségügyi adatokat kezelnek alapvetően kockázatosnak tekinti. Az olyan adatok kezelését, amelyekből személyiség-lopás, vagy személyazonossággal való visszaélés (ilyenek jelen ügyben az olyan azonosító adatok, mint pl. név, lakcím, telefonszám, születési dátum) fakadhat, szintén kockázatosnak tekintik a rendelet ezen előírásai.

A Hatóság megítélése szerint a nagyszámú, összesen 1153 érintett egészségügyi adatainak kezelése magas kockázatúnak tekinthető az általános adatvédelmi rendelet fenti előírásai alapján. A táblázatban szereplő adatkör rendkívül széles, gyakorlatilag teljesen egyedileg azonosíthatóvá tesz egy-egy pácienst, az adatok alapján sokszor konkrét diagnózis állítható fel a kezelt személlyel kapcsolatban. Az ilyen adatok megfelelő biztonsági intézkedések nélküli megosztása harmadik felekkel rendkívül magas kockázatokkal jár az érintettek magánszférájára nézve.

Az ilyen szenzitív és rendkívül pontos egészségügyi adatkört magában foglaló adatkezelés során, a biztonsági intézkedések hiánya miatt bekövetkező adatvédelmi incidens magas kockázatúnak minősül. A kockázatokat nem zárja ki teljes mértékben, ha magukat az egészségügyi adatokat csak szakmai titoktartásra kötelezett címzetti kör (orvosok) ismerik meg. Ennek oka, hogy az érzékeny egészségügyi adatok jogosulatlan harmadik személynek történő elküldése után az adatkezelő ráhatása azok sorsára kikerül az ellenőrzése alól. Az adatok kezelésének további bizalmas jellegét nem lehetséges teljes mértékben a továbbiakban garantálni. Az, hogy az adatokat csak szakmai titoktartásra kötelezett személyek kapták eredetileg meg, az incidens kockázatait ugyan kis mértékben csökkenti, de teljes mértékben már egyáltalán nem zárja ki.

Ügyfél az adatok kezelése alóli kikerülése miatt, azok további sorsára vonatkozó, a kockázatokat teljesen elimináló intézkedéseket nem tud tenni, az adatok címzettek általi – adott esetben jogellenes – továbbkezelésével járó kockázatokat már nem tudja teljesen csökkenteni. A címzettek utólagos felhívása az adatok törlésére sem zárja ki teljes mértékben a kockázatokat, csupán valamelyest csökkenti azokat. A fenti érvelést alátámasztja, hogy az egészségügyi adatokat tartalmazó táblázatot az eredetileg a címzettek között nem szereplő közérdekű bejelentő, majd a Hatóság is megkapta, az adatok (jogellenes) nyilvánosságra kerülésével járó kockázat így rendkívül magas.

A Hatóság továbbá az adatvédelmi incidens által jelentett kockázatokat tovább növelő tényezőnek tekinti, hogy az érintettek egészségügyi adatait tartalmazó Excel táblázat semmilyen hozzáférésvédelemmel, titkosítással nem volt ellátva. A megfelelő adatbiztonsági intézkedések alkalmazása csökkentette volna annak a kockázatát, hogy az egészségügyi adatokat az azokat megkapó harmadik személyek (pl. a közérdekű bejelentő) jogosulatlanul ne ismerhessék meg.

A nagyszámú, rendkívül részletes egészségügyi adatok együttes kezelése összevetve az incidens körülményeivel a Hatóság megítélése szerint magas kockázatú adatvédelmi incidenst eredményezett.

A fentiek alapján a Hatóság megítélése szerint az adatvédelmi incidens magas kockázatúnak tekinthető, ezért amennyiben egy ilyen esetről az adatkezelő tudomást szerez, úgy azt be kell jelentenie az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján a felügyeleti hatóságnak. A Hatóság a fentiekre tekintettel megállapítja, hogy az adatkezelő megsértette az általános adatvédelmi 33. cikk (1) bekezdését, mivel az incidens kockázatait nem megfelelően értékelte, így bejelentési kötelezettségének sem tudott volna eleget tenni.

A Hatóság az Ügyfél utólagos incidensbejelentésre való felhívásától eltekint, mivel arról már a közérdekű bejelentésből értesült, annak körülményeit a hatósági eljárás során feltárta.

3. Az érintettek tájékoztatásával kapcsolatos megállapítások

Az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az általános adatvédelmi rendelet (86) preambulumbekezdése szerint a tájékoztatás célja, hogy annak alapján az érintettek is meg tudják tenni azokat a további szükséges óvintézkedéseket a személyes adataikkal kapcsolatban, amelyekre az adatkezelő már nem rendelkezik ráhatással.

Ügyfél tudomása szerint a címzett háziorvosok, a veszélyhelyzet által teremtett körülményeket figyelembe véve, a megküldött adatokat a felhívásnak megfelelően bizalmasan kezelték. Ennek ellentmond, hogy a közérdekű bejelentő a háziorvosoknak küldött e-mailt és mellékelt táblázatot megkapta, holott nem szerepelt az eredeti címzettek között, azt neki is egy másik magán e-mail címről továbbították.

Ügyfél ugyan érintetti panaszt, bejelentést az incidenssel kapcsolatban nem kapott, azonban a nagyszámú, rendkívül pontos és részletes egészségügyi adat különösebb biztonsági intézkedés nélküli továbbküldésével megvalósuló adatvédelmi incidens ettől függetlenül is magas kockázatúnak tekinthető a Hatóság előző pontban kifejtett álláspontja alapján.

Az Ügyfél a titkosítás, vagy más hozzáféréskontroll nélkül e-mailben elküldött nagyszámú egészségügyi adat címzettek általi – adott esetben jogellenes – továbbkezelésével járó kockázatokat csak úgy tudja még tovább csökkenteni, ha arról az érintetteket is tájékoztatja. Az érintettek így meg tudják tenni azokat a további szükséges óvintézkedéseket a személyes adataikkal kapcsolatban, amelyekre az adatkezelő már nem rendelkezik ráhatással. A tájékoztatás elősegíti azt, hogy ezen rendkívül érzékeny személyes adataik kezelésével elkövetett esetleges további visszaélésekre az érintettek is kellő időben fel tudjanak készülni, azok ne érjék őket váratlanul.

Az incidensről való tájékoztatás miatt például az érintettet nem fogja teljesen váratlanul érni, ha a korábban a Covid-19 teszt miatt megadott és Ügyfél kezelésében lévő egészségügyi adataival valamely olyan másik (jogellenes) adatkezelőnél találkozik, amelynek azokat korábban sohasem adta meg (pl. egészségügyi szolgáltatás ajánlása direkt marketing módszerekkel).

A Hatóság a fentiekre tekintettel megállapítja, hogy Ügyfél megsértette az általános adatvédelmi rendelet 34. cikk (1) bekezdését és egyben felszólította Ügyfelet arra, hogy az érintetteket is tájékoztassa a bekövetkezett adatvédelmi incidensről.

4. Az adatkezelés biztonságával kapcsolatos megállapítások

Az általános adatvédelmi rendelet 32. cikk (1) bekezdése értelmében az adatkezelő a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. A rendelet ide érti többek között a 32. cikk (1) bekezdés a)-b) pontjai alapján a személyes adatok álnevesítését és titkosítását, valamint a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását.

Az általános adatvédelmi rendelet 32. cikk (2) bekezdése értelmében a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított személyes adatok jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

A Hatóság megítélése szerint az incidenssel érintett adatkezelés, így a Covid-19 gyorsteszten átesett 1153 érintett egészségügyi és más kapcsolódó adatainak (pl. elérhetőségek) kezelése magas kockázatúnak minősül az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak és a határozat III./2-3. pontjaiban is kifejtettek alapján.

Az adatkezelő, így jelen esetben Ügyfél feladata az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdései alapján, hogy az adatkezelés jellege, körülményei, céljai és kockázatai alapján, a tudomány és technológia állása szerint is megfelelő szintű adatbiztonsági intézkedéseket hajtson végre. Ezeknek az adatbiztonsági intézkedéseknek többek között azt kell garantálniuk, hogy a kezelt személyes adatok lehetőleg ne kerüljenek jogosulatlanul nyilvánosságra, vagy azokhoz ne lehessen jogosulatlanul hozzáférni.

A Hatóság megítélése alapján a nagyszámú érintett egészségügyi adatainak leválogatás nélküli továbbítása e-mailben egy egyszerű Excel táblázatban, bármilyen hozzáférésvédelem, vagy titkosítás alkalmazása nélkül nem felel meg jelen esetben a magas kockázatú adatkezeléssel jelentett kockázatokkal arányos adatbiztonság szintjének. Az egészségügyi adatok orvosoknak

való, leválogatás nélküli e-mailes továbbítása bármilyen további védelmi intézkedés alkalmazása nélkül komoly kockázatokkal jár az érintettek magánszférájára nézve. A megfelelő védelem alkalmazása nélkül ugyanis nem lehet azt a tudomány és technológia állása szempontjából is elégséges szinten garantálni, hogy a kezelt személyes adatok ne kerüljenek jogosulatlanul nyilvánosságra, vagy azokhoz ne lehessen jogosulatlanul hozzáférni. Az intézkedések hiányának komoly következményeire példa a jelen ügyben vizsgált adatvédelmi incidens bekövetkezése is.

A Hatóság megítélése szerint amennyiben az Ügyfél az adatok körzetek szerinti leválogatását és legalább jelszavas védelmet, továbbá a jelszó külön csatornán való megküldését alkalmazta volna a fájllal kapcsolatban, úgy az ügyben az adatbiztonság sérelme és emiatti adatvédelmi incidens sem következett volna be. A természetes személyek alapvető jogainak, így személyes adataik védelme szempontjából a Covid-19 járvány miatti veszélyhelyzet nem adhat teljes felmentést a megfelelő adatbiztonsági előírások betartása alól.

A Hatóság ugyanakkor ki kívánja ehelyütt azt is emelni, hogy az egészségügyi adatok továbbításával kapcsolatban egyáltalán nem tartja jó gyakorlatnak azok egyszerű Excel táblázatban, titkosítás nélkül, e-mailben történő elküldését. Erre sokkal biztonságosabb megoldást kínál egy erre a célra létrehozott, biztonságos platform (pl. az Egészségügyi Elektronikus Szolgáltatási Tér) használata.

A fentiek alapján a Hatóság megállapítja, hogy Ügyfél az adatbiztonsági intézkedések hiányában eszközölt adattovábbítással megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdését és annak a)-b) pontjait, továbbá ezen cikk (2) bekezdését.

5. Az alkalmazott szankció és indoklása

A Hatóság a tényállás tisztázása során megállapította, hogy Ügyfél az adatkezelése során megsértette az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseit, a 33. cikk (1) bekezdését és a 34. cikk (1) bekezdését.

A Hatóság megvizsgálta, hogy indokolt-e az Ügyféllel szemben adatvédelmi bírság kiszabása. E körben a Hatóság a GDPR 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az ügy összes körülményét.

Erre tekintettel a Hatóság az Infotv. 61. § (1) bekezdés a) pontja alapján a rendelkező részben foglaltak szerint döntött, és jelen határozatban Ügyfelet adatvédelmi bírság megfizetésére kötelezte.

A Hatóság a bírság kiszabása során az alábbi tényezőket vette figyelembe:

A Hatóság súlyosító körülményként vette figyelembe a következőket:

- A Hatóság az adatvédelmi incidensről közérdekű bejelentés alapján szerzett tudomást, Ügyfél által az adatvédelmi incidens saját tevékenységi körben történő észlelésére nem került sor.

- Ügyfélnél az egészségügyi adatok nagy számban történő kezelése alaptevékenységéhez tartozik és ezzel kapcsolatban közfeladatot ellátó szervnek minősül. Fokozottan elvárható így tőle ezen adatok körültekintő és adatvédelmi szempontból is megfelelő kezelése, az adatkezeléshez kapcsolódó kockázatok felmérésének képessége.

- Az adattovábbításból származó adatvédelmi incidens az érintettek jogaira és szabadságaira nézve magas kockázatokat hordozott, az érintettek tájékoztatását Ügyfél mégsem tervezte az elégtelenül elvégzett kockázatértékelés miatt.

- Az Ügyfél alaptevékenységéhez tartozó egészségügyi adatok nagyszámú kezelése miatt fokozottan elvárható tőle a megfelelő szintű adatbiztonság garantálása.

- A természetes személyek alapvető jogainak, így személyes adataik védelme szempontjából a Covid-19 járvány miatti veszélyhelyzet nem adhat felmentést a megfelelő adatbiztonsági előírások betartása alól.

A Hatóság enyhítő körülményként vette figyelembe a következőket:

- A Hatóság az incidenst kiváltó adatbiztonsági hiányosságot nem tekintette rendszerszintű problémának, mivel az csupán egy egyszeri adattovábbításhoz kapcsolódott és egyszeri kapkodásra, hanyagságra vezethető vissza.

- Az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán bármilyen konkrét hátrány vagy kár érte volna.

- A Hatóság figyelembe vette, hogy az Ügyféllel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést.

Egyéb, figyelembe vett körülmények:

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

A fentiekre tekintettel a Hatóság szükségesnek tartja a bírság kiszabását, csupán az Infotv. 75/A. §-a szerinti figyelmeztetés alkalmazását nem tartotta megfelelőnek, figyelemmel a jogsértés súlyára és a kezelt adatok körére.

Az adatvédelmi bírság összegét a Hatóság jogszabályon alapuló mérlegelési jogkörében eljárva határozta meg.

Ügyfél által elkövetett jogsértések az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja szerint az alacsonyabb összegű bírságkategóriába tartozó jogsértésnek minősülnek.

A bírság kiszabása során a Hatóság végül figyelembe vette, hogy az Infotv. 61. § (4) bekezdése b) pontja alapján a bírság mértéke százezertől húszmillió forintig terjedhet, ha az adatvédelmi hatósági eljárásban hozott határozatban kiszabott bírság megfizetésére kötelezett költségvetési szerv.

A Hatóság az Infotv. 61. § (2) bekezdés a) és b) pontjai alapján a határozatnak Ügyfél azonosító adataival történő nyilvánosságra hozatalát is elrendelte, mivel a jogsértés személyek széles körét érinti és azt közfeladatot ellátó szerv tevékenységével összefüggésben hozta.

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. § (1) bekezdése alapján a Hatóság döntésével szembeni közigazgatási per törvényszéki hatáskörbe tartozik, a perre a Kp. 13. § (3) bekezdés a) pont aa) alpontja alapján a Fővárosi Törvényszék kizárólagosan illetékes. A Kp. 27. § (1) bekezdés b) pontja alapján a törvényszék hatáskörébe tartozó perben a jogi képviselet kötelező. A Kp. 39. § (6) bekezdése szerint 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 veszélyhelyzet során érvényesülő egyes eljárásjogi intézkedések újbóli bevezetéséről szóló 112/2021. (III. 6.) Korm. rendelet (a továbbiakban: Veir.) 31. §-a szerint ha e rendelet eltérően nem rendelkezik, a szigorított védekezés a határidők folyását nem érinti. A Veir. 36. § (1)-(3) bekezdése szerint a szigorított védekezés ideje alatt a bíróság tárgyaláson kívül jár el, ideértve a perorvoslati eljárásokat is. Ha tárgyalás tartásának lenne helye, vagy azt bármelyik fél kérte, vagy a tárgyalást már kitűzték, az eljáró bíróság soron kívül értesíti a feleket a tárgyaláson kívüli elbírálás tényéről, és lehetőséget biztosít arra, hogy a felek nyilatkozataikat írásban előterjeszthessék. Ha a perben a szigorított védekezés idején kívül tárgyalást kellene tartani, a felperes akkor kérheti, hogy a bíróság tárgyaláson kívüli elbírálás helyett a tárgyalást a szigorított védekezés megszűnését követő időpontra halassza el, ha

a) a bíróság a közigazgatási cselekmény halasztó hatályát legalább részben nem rendelte el,

b) a keresetindításnak halasztó hatálya van, és a bíróság halasztó hatály feloldását nem rendelte el,

c) ideiglenes intézkedést nem rendeltek el.

A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Itv.) 45/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. 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, 2021. március 24.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár