Ügyszám: NAIH/2020/952/
NAIH/2019/5606

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 **Hungária Med-M Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság** (cím: 1132 Budapest, Csanády u. 6. B. ép. V. em. 2.) (a továbbiakban: Ügyfél) adatkezelését érintő adatvédelmi incidenssel kapcsolatban 2019. július 18. napján megindított hatósági ellenőrzés során feltárt körülmények miatt 2019. október 14. napján hivatalból megindított **adatvédelmi hatósági eljárásban**

**1) megállapítja, hogy**

a) az Ügyfél 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) 32. cikk (1) bekezdés b) pontjában foglalt kötelezettségének,

b) az Ügyfél nem tett eleget az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján fennálló incidensbejelentési kötelezettségének,

c) az Ügyfél nem tett eleget az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján fennálló tájékoztatási kötelezettségének a bekövetkezett adatvédelmi incidenssel kapcsolatban,

**2) utasítja az 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 az Ügyfelet a **jelen határozat véglegessé válásától számított 30 napon belül**

**7.500.000 Ft, azaz hétmillió-ötszázezer forint**

**adatvédelmi bírság megfizetésére kötelezi;**

**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/2020/952 BÍRS. számra kell hivatkozni.

A 2) pontban előírt intézkedések megtételét az Ügyfélnek az intézkedés megtételétől számított 15 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 2) pont szerinti kötelezés nem teljesítése, illetve 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 veszélyhelyzet a keresetindítási határidőt nem érinti. A keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak. A tárgyalás tartása iránti kérelmet a keresetlevélben jelezni kell. A veszélyhelyzet ideje alatt a bíróság tárgyaláson kívül jár el. 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.

## INDOKOLÁS

### I. Tényállás, előzmények

A Hatósághoz 2019. július 9-én közérdekű bejelentés érkezett, amely az Ügyfél online rendszerében fennálló, személyes-, köztük különleges adatokat érintő sérülékenységre hívta fel a figyelmet: az Ügyfél által üzemeltetett weboldal, a https://www.hungariamed.hu időpontfoglaló rendszerében – https://bejelentkezes.hungariamed.hu – kezelt orvosi leletek és beutalók nyilvánosan hozzáférhetők, illetve letölthetők jogosultsággal nem rendelkező felhasználók részére. A bejelentés mellékletét képezte egy képernyőfotó, melyet a bejelentő az általa elért, az időpontfoglaló rendszerben tárolt dokumentumok listáját megjelenítő felületről készített. A bejelentő elmondása szerint a problémát már jelezte az Ügyfélnél is közvetlenül, azonban visszajelzést nem kapott és a hiba sem került kijavításra.

A Hatóság a közérdekű bejelentés alapján 2019. július 18-án hatósági ellenőrzés megindításáról döntött annak ellenőrzése érdekében, hogy az Ügyfél maradéktalanul eleget tett-e az általános adatvédelmi rendelet 33-34. cikkében foglalt kötelezettségeinek. A közérdekű bejelentésben szereplő információk pontosítása, kiegészítése céljából a Hatóság NAIH/2019/5606/3, majd később NAIH/2019/5606/5 számú végzéseiben nyilatkozattételre hívta fel az Ügyfelet, amelyre az mindkét alkalommal határidőben válaszolt. Az ellenőrzés során tapasztaltak alapján az ügyben az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerinti különleges adatok (egészségügyi adatok) érintettsége miatti valószínűsíthető magas kockázat, illetve a rendelet 33. cikk (1) bekezdésének megfelelő bejelentési kötelezettség elmulasztása miatt – az Infotv. 60. § (1) bekezdésére tekintettel –, a Hatóság 2019. október 14-én az általános adatvédelmi rendelet 32-34. cikkei feltételezhető megsértése miatt adatvédelmi hatósági eljárást indított, amelyről az Ügyfelet NAIH/2019/5606/7 számú végzésével értesítette, valamint a tényállás további tisztázása érdekében újabb nyilatkozattételre hívta fel, melyre az Ügyfél az előírt határidőben válaszolt.

A közérdekű bejelentés nyomán megismert adatok, valamint a hatósági ellenőrzés és később a hatósági eljárás során, az Ügyfél nyilatkozatai és adatszolgáltatásai alapján a Hatóság az alábbiakat tárta fel.

A sérülékenység a https://bejelentkezes.hungariamed.hu/doc/, illetve a https://fogleu.hungariamed.hu/doc/ URL-eket érintette, ahol a betegek leleteit tartalmazó .pdf kiterjesztésű dokumentumokat tárolták. A webszerver a fenti speciális, /doc/ végződésű URL-ek meghívásával a kért időpontfoglaló felület megjelenítése helyett, a webszerveren található összes tartalmat kilistázta a képernyőre. Ez lehetővé tette, hogy a fenti linkek ismeretében bárki, bejelentkezés, vagyis az oldalon történő regisztráció nélkül hozzáférjen az online felületen tárolt személyes adatokat tartalmazó dokumentumokhoz.

A Hatóság IT biztonsági munkatársa megállapította, hogy az adatvédelmi incidenssel érintett rendszerben fennálló sérülékenység abból adódóan valósulhatott meg, hogy az Ügyfél a szerverén nem megfelelő konfigurációs beállításokat alkalmazott. Megfelelő beállítások esetén egy /doc/ végződésű URL beírásakor a szerver egy hibaüzenetet jelenít meg, mely szerint az URL a szerveren nem található. Az említett konfigurációs hiba következtében azonban az érintett URL-ek meghívásával a szerver megjelenítette a weboldalon található könyvtárszerkezetet, így az ott tárolt személyes adatokat tartalmazó dokumentumokhoz hozzá lehetett férni. (lásd: az ügyben készült NAIH/2019/5606/2. ügyiratszámú információbiztonsági szakértői vélemény).

Az adatvédelmi incidenssel érintett rendszerben az Ügyfél körülbelül 15 000 személyes adatot kezel: az Ügyféllel szerződéses jogviszonyban álló partnerek munkavállalóinak neve, születési helye- és ideje, anyja neve, TAJ száma, e-mail címe, telefonszáma, lakcíme, munkaköre, és egészségügyi adatai. Az érintettek személyes adatait az időpontfoglaló rendszerben először nyilvántartásba veszik, majd a vizsgálatokat követően leleteik is feltöltésre kerülnek, melyek a laborvizsgálati-, szakorvosi-, illetve foglalkozás-egészségügyi vizsgálataik eredményeit – ezen belül családi anamnézis adataikat is – tartalmazzák.

Az Ügyfél a Hatóságnak adott válaszában úgy nyilatkozott, hogy a weboldalán fennálló sérülékenységről csak a Hatóság 2019. július 19. napján kézhez vett végzéséből értesült. Az Ügyfél elmondása szerint korábban csak egy marketing jellegű, szolgáltatásértékesítő célú, riogató hangvételű levelet kapott, amelynek konkrét adatvédelmi incidensre utaló tartalma nem volt. Az Ügyfél ez alapján az általa használt informatikai rendszerek tekintetében miniauditot folytatott le, ez azonban informatikai kockázatot nem állapított meg. A Hatóság végzésében megjelölt sérülékenység feltárása érdekében ezt követően haladéktalanul belső IT biztonsági auditot indított, mely 2019. július 19-én egyetlen sérülékenységi pontot tárt fel informatikai rendszerében. Az Ügyfél megállapította, hogy az online felület leletlekérdező URL-jében az azonosítót át lehet írni, és ily módon esetleg dokumentumokat is le lehet kérni a rendszerből.

Az Ügyfél által folytatott vizsgálat során az informatikai rendszer naplófájljai is elemzésre kerültek. Ezek rendelkezésre álló állományai nem tartalmaztak olyan adatlekérdezést, amely a vizsgált tartományban ténylegesen jogosulatlan hozzáférésre utalt volna, és az Ügyfél egyéb módon sem szerzett tudomást az adatokhoz való jogosulatlan hozzáférésről.

A fennálló sérülékenységre tekintettel megállapításra került az adatvédelmi incidens bekövetkezése. Az adatvédelmi incidenssel kapcsolatban elvégzett kockázatelemzés során az Ügyfél az állapította meg, hogy az valószínűsíthetően nem jár kockázattal az érintettek jogaira és

szabadságaira nézve, tekintettel arra, hogy az adatokhoz való jogosulatlan hozzáférés nem állapítható meg, illetve a hiba az észlelést követően azonnal kijavításra került, így az incidens Hatóságnak történő bejelentését és az érintettek tájékoztatását az Ügyfél nem tartotta indokoltnak.

Az Ügyfél a Hatóság kérésére bemutatta hatályos Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) naplózásra vonatkozó előírásait. Eszerint „az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert (biztonsági napló) kell kialakítani, mellyel utólag nyomon követhetők a tárgyidőszakot megelőző 14 napon belül az informatikai rendszerben bekövetkezett fontosabb események – különös tekintettel azokra, amelyek a rendszer biztonságát érintik – és ezáltal lehetséges a hozzáférések jogosultságának ellenőrzése, illetéktelen hozzáférés megtörténtének, és amennyiben lehetséges a hozzáférő személyének megállapítása."

Az IBSZ a naplózásra vonatkozó előírások között felsorolja a minimálisan regisztrálandó események listáját, melyben többek között a be- és kijelentkezések is szerepelnek. A Hatóság ezzel kapcsolatban megállapította, hogy a feltárt sérülékenységből fakadó esetleges jogosulatlan hozzáférések nem sorolhatók a be- és kijelentkezések naplózási körébe, mivel az érintett személyes adatok az oldalra mutató link ismeretében regisztráció nélkül is bárki számára hozzáférhetők voltak. Az Ügyfél a közérdekű bejelentő által, valamint a Hatóság IT biztonsági munkatársa által, a hatósági ellenőrzés során végrehajtott adatlekérdezést sem észlelte, annak ellenére, hogy arra az IBSZ-ben foglalt naplózási időintervallumon belül került sor. A naplófájlok ebből adódóan nem voltak alkalmasak annak megállapítására, hogy történt-e jogosulatlan hozzáférés a rendszerhez.

Az Ügyfél nem tudta pontosan meghatározni, hogy maga a sérülékenység mióta állt fent a rendszerében. Az incidensről való tudomásszerzést követően az észlelt hiányosság viszont általa azonnal elhárításra került. A webszerveren nem csak az azonosító, hanem a bejelentkezett felhasználó is ellenőrzésre kerül, így az azonosító átírásával már kizárólag az adott felhasználó dokumentumainak lekérdezésére van lehetőség.

Az Ügyfél tájékoztatta arról a Hatóságot, hogy az incidenst milyen tartalommal vette az általános adatvédelmi rendelet 33. cikk (5) bekezdése szerinti nyilvántartásba. Eszerint az Ügyfél által működtetett időpontfoglaló rendszerben tárolt adatok az Ügyfél által nem ismert biztonsági rés eredményeként, a rendszer megkerülésével, jogosultsággal nem rendelkező személyek számára is hozzáférhetővé váltak, tényleges adathozzáférés ugyanakkor nem állapítható meg. Az Ügyfél megítélése szerint erre tekintettel az incidens valószínűsíthetően nem jár kockázattal az érintettek alapvető jogaira és szabadságaira nézve, ezért a Hatóságnak részére történő bejelentési kötelezettsége nem áll fenn, és az érintettek incidensről való tájékoztatása sem indokolt.

A Hatóság az eljárás során többször megpróbálta felhívni a közérdekű bejelentőt arra, hogy juttassa el a Hatóságnak azokat a megkereséseket, amelyekben a sérülékenységet jelezte az Ügyfél felé. Ezekre a bejelentő a hatósági eljárás lezárásáig nem reagált.

A Hatóság 2020. március 6-án, NAIH/2020/952/2 számú végzésével értesítette az Ügyfelet, hogy az ügyben bizonyítási eljárást folytatott le, és tájékoztatta, hogy a bizonyítási eljárás során keletkezett információbiztonsági szakértői véleményt – az iratokba való betekintés szabályai figyelembevételével – megismerheti, és további bizonyításra irányuló indítványt terjeszthet elő; valamint felhívta, hogy nyilatkozzon 2019. évi bevételéről. A végzésre az Ügyfél az előírt határidőben válaszolt és iratbetekintési kérelmet terjesztett elő, melynek a Hatóság 2020. március

12-én, NAIH/2020/952/6 számú végzésével helyt adott és az Ügyfél kérésére az információbiztonsági szakértői véleményről készült másolatot elküldte részére.

Az Ügyfél 2020. március 16-án kelt válaszlevelében tett nyilatkozata szerint a 2019. év zárásának és mérlegének elkészítése 2020. május hónapban, a könyvvizsgálatot követően történik meg, így erről nem áll rendelkezésre egyértelmű bevételi adat. A jelenlegi becsült bevétel a 2019. év tekintetében 800 000 000 HUF, melyet az Ügyfél vezetői becslés alapján állapított meg. Az Ügyfél továbbá tájékoztatta a Hatóságot, hogy az időközben lefolytatott informatikai vizsgálat eredménye alapján megállapította, hogy az adatvédelmi incidens feltehetően körülbelül 9000 fő személyes adatait érinthette. Ennek megfelelően az Ügyfél módosította incidensnyilvántartását és ismételten megküldte azt a Hatóság részére.

Az Ügyfél az információbiztonsági szakértői vélemény megismerését követően, 2020. április 3-án nyilatkozatot terjesztett elő, melyben a következőkről tájékoztatta a Hatóságot. Az Ügyfél a jogosulatlan hozzáférési lehetőségről a Hatóság végzéséből értesült, melyet azonnal és teljes mértékben elhárított. A felmerült adatbiztonsági kockázatok azonnali megszüntetése, és azok jövőbeli teljes kiküszöbölése érdekében az alábbi technikai és szervezési intézkedéseket foganatosította. A webszerveren található /doc/ könyvtárhoz kapcsolódóan azonnal gondoskodott a letiltásról, ezt követően már nem lehetett az említett mappa tartalmához illetéktelen személyek által hozzáférni. Külső IT biztonsági auditot folytatott le, melynek keretében ellenőriztette az általa használt rendszerek adatlekérdezésre alkalmas funkcióit, az esetleges adatszivárgási kockázatok elhárítása érdekében. A vizsgálat során megállapításra került, hogy az iratbetekintés keretében megismert „Információbiztonsági szakértői vélemény a NAIH/2019/5656 ügyhöz kapcsolódóan” című szakértői véleményben megállapított biztonsági résen kívül nem volt megállapítható más sérülékenységre, jogosulatlan hozzáférésre, lekérdezésre, információszivárgásra vonatkozó információ.

Az időpontfoglaló rendszer php alapú kódjai az Ügyfél által újratervezésre kerültek, a korábbi procedurális megközelítés objektumorientáltra került átdolgozásra, ami még nagyobb biztonságot nyújt az adatok tárolására. Az Ügyfél a könyvtárak titkosítását, a jogosultsági szintek és a felhasználói hozzáférések szigorítását is eszközölte, ezzel kiküszöbölte az esetleges rendszerhibától független adatvisszaéléseket. Emellett felülvizsgálta fejlesztési elveit és politikáit, valamint a fejlesztéssel foglalkozó kollégák infomációbiztonsági továbbképzését rendelte el annak érdekében, hogy bármilyen saját rendszerfejlesztés csak az információbiztonsági követelmények maradéktalan érvényesülésével valósuljon meg.

## 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 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 9. cikk (1) bekezdése alapján az egészségügyi adat a személyes adatok különleges kategóriájába tartozó, s mint ilyen, magasabb szintű védelmet igénylő személyes adat (különleges személyes adat), figyelemmel a rendelet (53) preambulumbekezdésére is figyelemmel.

Az általános adatvédelmi rendelet 32. cikk (1) bekezdése értelmében az adatkezelő 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, ideértve, többek között, (a b) pont szerint) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét.

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 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. 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 általános adatvédelmi rendelet 32–34. cikkének megsértése esetén a kiszabható bíróság felső határa az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja alapján a 10 000 000 eurónak (EUR) megfelelő összeg.

Az Infotv. 61. § (2) bekezdése szerint a Hatóság elrendelheti határozatának – az adatkezelő, illetve az adatfeldolgozó azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha a határozat személyek széles körét érinti, azt közfeladatot ellátó szerv tevékenységével összefüggésben hozta, vagy a bekövetkezett jogsérelem súlya a nyilvánosságra hozatalt indokolja.

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

## III. **Döntés**

1. az adatvédelmi incidens kezelésével kapcsolatos intézkedések

Az adatvédelmi incidensről az Ügyfél saját elmondása szerint először a Hatóság NAIH/2019/5606/3. ügyiratszámú tényállástisztázó végzése alapján lefolytatott belső vizsgálat során, 2019. július 19-én szerzett tudomást. A közérdekű bejelentő ezzel szemben azt állította, hogy a sérülékenységet már korábban is jelezte az Ügyfélnél.

A Hatóság az eljárás során többször megpróbálta felhívni a közérdekű bejelentőt arra, hogy küldje meg a sérülékenységet jelző, Ügyfélnek írt megkereséseit, azonban ezekre a bejelentő a hatósági eljárás lezárásáig nem reagált. Ennek ellenére a jogsértés ténye az alábbiakban kifejtettek miatt a rendelkezésre álló adatok alapján is megállapítható.

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 adatvédelmi incidens bejelentésére sem korábban, sem annak ellenére nem került sor, hogy a Hatóság megindította hatósági ellenőrzését, majd a jelen hatósági eljárást az Ügyféllel szemben. A bejelentés mellőzését az Ügyfél azzal indokolta, hogy az általa elvégzett kockázatelemzés alapján

az adatvédelmi incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira nézve.

A Hatóság megítélése szerint az incidens Ügyfél általi kockázatértékelése nem elfogadható. Az, hogy az Ügyfélnek nem áll rendelkezésére arra vonatkozó bizonyíték, hogy az informatikai rendszerében fennálló sérülékenységet arra jogosulatlan személyek ténylegesen kihasználták volna, nem elegendő annak a megállapításához, hogy személyes adatokhoz való jogosulatlan hozzáférés nem történt. A Hatóság az eljárás során megállapította, hogy az Ügyfél naplózási rendszere nem volt alkalmas a külső hozzáférések kimutatására, mivel az Ügyfél által vizsgált időszakban a Hatóság IT biztonsági munkatársa, valamint korábban a közérdekű bejelentő is hozzáfért a kezelt adatokhoz, anélkül, hogy ezt az Ügyfél észlelte volna.

A Hatóság nem tudja elfogadni az Ügyfél azon érvelését sem, miszerint az incidens azért nem járt kockázattal, mert a feltárt sérülékenységet annak észlelését követően azonnal kijavította. Azt ugyanis, hogy ez a sérülékenység pontosan mióta állt fent informatikai rendszerében, az Ügyfél szintén nem tudta megállapítani, így annak megállapítására sem volt képes, hogy az IBSZ-ben foglalt naplózási időintervallumon kívül történt-e jogosulatlan hozzáférés.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből személyazonosság-lopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül. Az érintettek neve, születési adatai, anyjuk neve és különösképpen TAJ száma olyan adatok, amelyekkel elkövethető személyazonosság-lopás, személyazonossággal visszaélés.

Az érintettek jogaira jelentett magas kockázati besorolást továbbá önmagában is megalapozza az, hogy az Ügyfél az incidenssel érintett rendszerben tárolt nagyszámú (körülbelül 15 000 darab) személyes adat között egészségügyi adatokat is kezel, melyek az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerint a személyes adatok különleges kategóriájába tartoznak. Ezen adatok kiemelését a személyes adatok általános fogalma alól az indokolja, hogy az ilyen információk az érintett életének érzékenyebb aspektusaira vonatkoznak, ezért azok illetéktelen általi megismerésének, vagy nyilvánosságra kerülésének lehetősége is különösen sérelmes lehet az érintett számára. Ezen adatok jogellenes kezelése negatívan befolyásolhatja az egyén jó hírnevét, magán- és családi életét, hátrányos megkülönböztetés oka vagy indoka lehet az érintettel szemben. A már említett (75) preamubulumbekezdés az egészségügyi adatok kezelését önmagában is olyan adatkezelésnek minősíti, amely az érintett személyek jogaira és szabadságaira nézve alapvetően kockázatos.

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 a Hatóságnak.

A Hatóság továbbá úgy ítéli meg, hogy az incidens olyan magas kockázatúnak minősül, amely indokolja, hogy az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján arról az érintetteket is tájékoztassák.

Az incidensről való tájékoztatásra a Hatóság megítélése szerint kifejezetten azért is van szükség, mivel az érintett magánszférájára jelentett kockázat a személyazonosításra alkalmas adatok (név, születési idő, születési hely, anyja neve, TAJ szám, lakcím, e-mail cím, telefonszám)

nyilvánosságra kerülése esetén olyan jellegű (ezen adatok birtokában elkövethető személyazonossággal visszaélés), amelynek kockázatai – az általános adatvédelmi rendelet (85)-(86) preambulumbekezdéseiben foglaltaknak megfelelően – csak úgy mérsékelhetők eredményesen, ha az érintettek erről tudomással bírnak, és megtehetik az általuk szükségesnek tartott további intézkedéseket. Ezen felül az egészségügyi adatok érintettsége is magas kockázatú adatvédelmi incidenst eredményez, mivel ezek ismerete alapot szolgáltathat hátrányos megkülönböztetésre, de akár az érintett magán- és családi életét is befolyásolhatja, ami miatt szintén indokolt az érintettek tájékoztatása.

A Hatóság felhívja arra a figyelmet, hogy az általános adatvédelmi rendelet 34. cikk (3) bekezdés c) pontja alapján, ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé, úgy az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

2. Az adatbiztonsági intézkedésekkel kapcsolatos megállapítások

Az incidens által jelentett kockázat megítélése céljából a Hatóság megvizsgálta azt is, hogy az Ügyfél mennyiben tett eleget az incidens bekövetkezésével közvetlenül összefüggő adatbiztonsági követelményeknek.

Az általános adatvédelmi rendelet 32. cikk (1) bekezdésében foglaltak alapján az adatkezelőnek a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében a tudomány és technológia állásának megfelelő technikai és szervezési intézkedéseket kell végrehajtania, ide értve a rendelet a 32. cikk (1) bekezdés b) pontja alapján a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét.

A fentieken túl az általános adatvédelmi rendelet 24. cikk (1) bekezdése is kimondja a megfelelő technikai és szervezési intézkedések végrehajtásának kötelezettségét az adatkezeléssel kapcsolatban. E cikk az adott adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével kívánja meg az ilyen intézkedések alkalmazását.

A kezelt adatokhoz való hozzáférések tekintetében az Ügyfél nem tudta kimutatni, hogy azokhoz vajon kívülről hányan férhettek hozzá jogosulatlanul. Nyilatkozata szerint naplózási rendszere nem mutatott ki ilyen hozzáféréseket, valamint az általa alkalmazott egyéb eszközök (hardveres és szoftveres tűzfalak, hálózatbiztonsági program) sem jeleztek. Az Ügyfél az eljárás során úgy nyilatkozott, hogy ugyan minden pdf letöltést naplóznak (regisztrációhoz kötöttet és regisztráció nélkülit is), de mégsem tudnak a releváns időszakban külső hozzáférést kimutatni. Ehhez képest a kezelt adatokhoz mind a Hatóság IT biztonsági munkatársa, mind a közérdekű bejelentő hozzáfért kívülről az adott időszakban. Az Ügyfél a bizonyítási eljárás során készült információbiztonsági szakértői vélemény megismerését követően sem tudott olyan újabb információt a Hatóság rendelkezésére bocsátani, mely ezt az ellentmondást feloldotta volna. Az Ügyfél továbbá azt sem tudta megállapítani, hogy a sérülékenység mióta áll fent informatikai rendszerében.

A csupán egy egyszerű internetes link birtokában a kezelt egészségügyi adatokhoz való illetéktelen hozzáférések megakadályozásán túl, a konkrét hozzáférések (tkp. ebben az ügyben külső dokumentumletöltések), akár külső rosszindulatú támadások naplózására való képesség, továbbá az illetéktelen hozzáférő személyét kimutatni tudó hálózatbiztonsági eszközök megfelelő

beállítások melletti, naprakész alkalmazása az Ügyfél IBSZ-ében is meghatározása került, mint belső szabály. A Hatóság megjegyzi, hogy véleménye szerint ezek a belső szabályok egyébként – az általános adatvédelmi rendelet 32. cikkében foglaltaknak megfelelően – a tudomány és technológia jelen állása szerint is elvárható biztonsági intézkedések nagyszámú egészségügyi adat kezelése kapcsán. Ez főleg igaz az olyan piaci szereplőkre, amelyek anyagi hasznot is realizálnak az ilyen adatok kezelésével összefüggő főtevékenységükkel. Az Ügyfél az illetéktelen hozzáférések kimutatásának elégtelenségével ezért nem csupán saját belső szabályzatának, hanem a kockázatokkal arányos, általánosan elvárható védelmi szintnek sem felelt meg.

A külső hozzáférések, letöltések kimutatására való képtelensége miatt az Ügyfél megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját.

Az egészségügyi adatok – mint az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerinti különleges adatok –, kezelése az előző pontokban kifejtetteknek megfelelően önmagában is magas kockázatú adatkezelést eredményez. Az ilyen adatok kezelése során ezért az adatkezelők részéről fokozottan elvárható, hogy a magas kockázattal arányos technikai és szervezési intézkedéseket tegyenek az adatbiztonság garantálása érdekében.

Ezt az általános adatvédelmi rendelet 32. cikk (2) bekezdése is megerősíti, amikor kimondja, hogy 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.

Tekintettel arra, hogy az adatvédelmi incidenssel érintett rendszerben fennálló sérülékenység abból adódóan valósulhatott meg, hogy az Ügyfél a személyes adatok kezelése során nem megfelelő biztonsági beállításokat alkalmazott az érintett rendszerében, – amely lehetővé tette, hogy az oldalra mutató link ismeretében bárki, az oldalon történő regisztráció nélkül hozzáférjen az online felületen tárolt személyes adatokat tartalmazó dokumentumokhoz, – az Ügyfél szintén megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját.

3. Alkalmazott szankció és indoklása

A Hatóság a tényállás tisztázása során megállapította, hogy az Ügyfél megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját, a 33. cikk (1) bekezdését, valamint a 34. cikk (1) bekezdését. Erre tekintettel a rendelkező részben foglaltak szerint a Hatóság utasította az Ügyfelet, hogy tegye meg a szükséges intézkedéseket annak érdekében, hogy az érintettek adatvédelmi incidensről való tájékoztatása az általános adatvédelmi rendelet 34. cikkében foglaltak szerint megvalósuljon.

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 az Ügyfelet adatvédelmi bírság megfizetésére is kötelezte.

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

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

A Hatóság súlyosbító körülményként vette figyelembe a következőket:

- Az incidenssel érintett személyes adatok kezelése az adatok jellegéből fakadóan magasabb kockázattal jár, ezért az adatkezelőknek fokozott elővigyázatossággal kell eljárniuk a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében, az Ügyfél ennek ellenére nagyszámú (körülbelül 15 000 darab) személyes adat, – köztük egészségügyi adatok – kezelésére használt rendszere folyamatos bizalmas jellegének biztosítása érdekében nem hozott megfelelő intézkedéseket. Az Ügyfél továbbá az incidensről való tudomásszerzést követően, – annak ellenére, hogy az érintett adatok különleges személyes adat jellege nyilvánvaló, – nem tette meg a Hatóság részére a bejelentéssel, valamint az érintettek tájékoztatásával kapcsolatos intézkedéseket, így magatartása kifejezetten magas fokon felróható. [GDPR 83. cikk (2) bekezdés a) pont].

- A Hatóság megállapította, hogy egy alapvetően magas kockázatú, különleges adatokat is érintő adatkezelés tekintetében az Ügyfél a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott, amikor az egészségügyi és további személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt az Ügyfél észlelte volna. Az ilyen adatok kezelésére való biztonsági felkészültség, az egészségügyi tevékenységet fő tevékenységként kifejtő, profit alapú vállalkozásoktól fokozottan elvárható. [GDPR 83. cikk (2) bekezdés d) pont].

- A jogsértés személyes adatok különleges kategóriáit is érinti. Az ilyen adatokra vonatkozó jogsértés esetén súlyosabb szankcionálás lehet indokolt, mivel jogosulatlan megismerésük jelentős következménnyel járhat az érintettek számára. [GDPR 83. cikk (2) bekezdés g) pont].

- A Hatóság az adatvédelmi incidensről közérdekű bejelentés alapján szerzett tudomást, az Ügyfél által az adatvédelmi incidens bejelentésére nem került sor, annak ellenére, hogy a Hatóság megindította hatósági ellenőrzését, majd a jelen hatósági eljárást az Ügyféllel szemben. [GDPR 83. cikk (2) bekezdés h) pont].

A Hatóság enyhítő körülményként vette figyelembe a következőket:

- Az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán kár érte volna [GDPR 83. cikk (2) bekezdés a) pont].

- A feltárt tényállásból arra lehet következtetni, hogy a jogsértés nem volt szándékos, azt az Ügyfél gondatlansága okozta. Erre utal az is, hogy az Ügyfél az incidensről való tudomásszerzést követően azonnal intézkedéseket tett a feltárt sérülékenység megszüntetése érdekében [GDPR 83. cikk (2) bekezdés b) pont].

A Hatóság a jogkövetkezményekről való döntés meghozatala során az általános adatvédelmi rendelet 83. cikk (2) bekezdésének c) e) f) i) j) és k) pontjait nem tartotta relevánsnak.

A fentiekre tekintettel a Hatóság szükségesnek tartja a bírság kiszabását, csupán az Infotv. 75/A. §-a szerinti figyelmeztetés alkalmazását nem tartotta megfelelőnek.

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

A bírság kiszabása során a Hatóság végül figyelembe vette, hogy az Ügyfélnek 2018. évi beszámolója szerint 631 480 000 HUF bevétele volt. Az Ügyfél nyilatkozata szerint a 2019. év zárásának és mérlegének elkészítése 2020. május hónapban történik meg, így erről nem áll rendelkezésre egyértelmű bevételi adat, vezetői becslés alapján az Ügyfél 2019. évi bevétele 800 000 000 HUF volt. A jogsértés súlyára és az Ügyfél gazdálkodási adataira tekintettel a kiszabott bírság mértéke ezért a Hatóság megítélése szerint arányosnak tekinthető.

## 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 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.

A veszélyhelyzet ideje alatt érvényesülő egyes eljárásjogi intézkedésekről szóló 74/2020. (III. 31.) Korm. rendelet (a továbbiakban: Korm. rendelet) 35. §-a szerint ha e rendelet eltérően nem rendelkezik, a veszélyhelyzet a határidők folyását nem érinti.

A Korm. rendelet 41. § (1) bekezdése szerint a veszélyhelyzet ideje alatt a bíróság tárgyaláson kívül jár el. Ha a perben a veszélyhelyzet idején kívül tárgyalást kellene tartani, a felperes akkor kérheti, hogy a bíróság tárgyaláson kívüli elbírálás helyett a tárgyalást a veszélyhelyzet megszűnését követő időpontra halassza el, ha

*a)* a bíróság a közigazgatás 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.

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, 2020. április 27.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár