Ügyszám: NAIH/2020/402/4 Tárgy: kérelemnek helyt adó döntés
Előzmény: NAIH/2019/6090

HATÁROZAT

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) a […] (a továbbiakban együtt: Kérelmezők) 2019. július 30-án kelt **kérelmére** a Szegedi Tudományegyetemmel (Szentgyörgyi Albert Klinikai Központ) (6720 Szeged, Dugonics tér 13.) (a továbbiakban: Adatkezelő vagy Kérelmezett) szemben indult **adatvédelmi hatósági eljárásban**

határozatában a Kérelmezők kérelmének helyt ad, és

1. **megállapítja**, hogy a Kérelmezett megnevezett szervezeti egysége által alkalmazott rendszerrel összefüggésben megvalósuló adatkezelés során, a Kérelmezők személyes adataival kapcsolatban bekövetkezett 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 vagy GDPR) 33.-34 cikkeiben foglalt kötelezettségeinek;
2. **kötelezi** a Kérelmezettet, hogy a vizsgált adatvédelmi incidenst rögzítse a GDPR 33. cikk (5) bekezdése szerinti nyilvántartásába**;**
3. **kötelezi** a Kérelmezettet, hogy a Kérelmezőket tájékoztassa az adatvédelmi incidensről a GDPR 34. cikk (2) bekezdésében előírt módon és tartalommal.
4. a fenti jogsértés miatt a Kérelmezettet a **jelen határozat véglegessé válásától számított 30 napon belül 500 000 Ft, azaz ötszázezer forint adatvédelmi bírság megfizetésére kötelezi.**

A Hatóság megállapította, hogy túllépte az ügyintézési határidőt, ezért akként rendelkezik, hogy 10 000 Ft-ot, azaz tízezer forintot a Kérelmezőknek – írásban megjelölendő választásuk szerint – bankszámlára utalással vagy postai utalvánnyal megfizet.

A 2. és 3. pontban előírt intézkedések megtételét a Kérelmezettnek a határozat kézhezvételétől számított 15 napon belül kell írásban – az azt alátámasztó bizonyítékok előterjesztésével együtt – igazolnia a Hatóság felé.

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/2020/402 BÍRS. számra kell hivatkozni.

Amennyiben a Kérelmezett 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, illetve a 2. és 3. pont szerinti kötelezettségek nem teljesítése 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 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 bírósági felülvizsgálati eljárás illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

Az eljárásban eljárási költség nem merült fel.

INDOKOLÁS

I. Tényállás, előzmények

A Kérelmezők 2019. július 30-án kérelmet nyújtottak be a Hatósághoz, mely a Hatósághoz 2019. augusztus 2-án érkezett meg. A kérelemben előadták, hogy a Kérelmezett egyik szervezeti egységének vezetője (a továbbiakban: Intézetvezető), visszaélve vezetői pozíciójával, jogosulatlanul ismerte meg a Kérelmezők egészségügyi személyes adatait számos alkalommal. A jogosulatlan megismerésre olyan módon került sor, hogy a Kérelmezett nevezett alkalmazottja a MedSolution és az eMedSolution információs rendszerekben, a Kérelmezőkre vonatkozó, egészségügyi állapotukra vonatkozó személyes adatokat lekérte, megnézte és a számítógépe vágólapjára helyezte. A kérelemhez is mellékelt, a Kérelmezők 2018. július 5-én kelt, hozzáférési kérelemre adott válasz mellékletét képező, az információs rendszerek naplófájljait tartalmazó táblázatokból megállapítható, hogy az említett vezető a Kérelmezők személyes adatait összesen 82 alkalommal lekérte, megtekintette, és a számítógépe vágólapjára helyezte. Az Intézetvezető nem volt egyik Kérelmezőnek sem kezelőorvosa, azonban […] munkahelyi felettese volt a lekérdezések időpontjában. A Kérelmezők előadták továbbá, hogy a jogosulatlanul megismert személyes adatokat az említett vezető a kollégák között terjesztette, harmadik személyekkel közölte.

Álláspontjuk szerint az eset adatvédelmi incidens(eke)t valósított meg, amely magas kockázatot jelent az érintettekre, vagyis a Kérelmezőkre nézve, különös tekintettel arra, hogy az az érintettek nagy mennyiségű, különleges, egészségügyi személyes adatát érintette. A Kérelmezők kifogásolták, hogy az Adatkezelő az esetet nem azonosította adatvédelmi incidensként, és azzal kapcsolatban nem hozott megfelelő intézkedéseket, így például nem jelentette be azt a Hatósághoz. Kérelmükben kérték, hogy a Hatóság állapítsa meg a jogellenes adatkezelés tényét, és marasztalja el az Adatkezelőt, illetve amennyiben indokolt, szabjon ki bírságot.

A kérelem alapján az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 60. § (1) bekezdése alapján, 2019. augusztus 2-án adatvédelmi hatósági eljárás indult. Mivel a kérelem nem tartalmazta a Kérelmezők azonosításához szükséges minden adatot, illetve a megjelölt jogsértés orvoslása iránti döntésre vonatkozó határozott kérelmet, a Hatóság a Kérelmezőket felhívta, hogy pótolják a kérelem hiányait. A Kérelmezők ezt a felhívást a Hatósághoz 2019. augusztus 16-án érkezett beadványukkal teljesítették.

A hatósági eljárás során a Hatóság három alkalommal, 2019. szeptember 5-én, 2019. november 7-én, illetve 2020. január 8-án nyilatkozattételre hívta fel az Adatkezelőt.

A végzésekre válaszul küldött nyilatkozatok, adatszolgáltatások, illetve a Kérelmezők által rendelkezésre bocsátott információk alapján a Hatóság az alábbiakat tárta fel:

Az Adatkezelő a betegellátási tevékenységének nyilvántartását integrált informatikai rendszer alkalmazásával, az erre szolgáló MedSolution/eMedSolution rendszer segítségével végzi. A rendszer tehát arra szolgál, hogy abban az Adatkezelő az ellátott betegek egészségügyi ellátásával kapcsolatos adatait, például leleteit rögzítse, tárolja, kezelje. Ez alapján tehát a rendszer alkalmazásával, használatával az Adatkezelő adatkezelést végez.

A rendszer használatával tehát adatkezelés valósul meg, amelyre vonatkozóan a Szegedi Tudományegyetem Szent-Györgyi Albert Klinikai Központ és Általános Orvostudományi Kar Adatvédelmi Szabályzatának 1. sz. kiegészítése az irányadó. Ez a szabályzat rendezi többek között azt, hogy a rendszerben tárolt adatokhoz kinek és milyen módon van jogosultsága hozzáférni. A szabályzat lefekteti a felhasználói jogosultság igénylésének menetét, illetve általában, az adatkezeléssel kapcsolatban is tartalmaz előírásokat. 9. § (1) bekezdése előírja például, hogy „Az Eüaktv. rendelkezései szerinti adatkezelési célokra csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósulásához elengedhetetlenül szükséges. Ennek szabályozása számítógépes programmal csak részben támogatható, alapvetően a betegellátó szakmai döntésén alapszik. Az adatkezelés törvényességének ellenőrzéséhez az elektronikus adatkezelési rendszer az adatkezelések naplózásával járul hozzá.” A szabályzat 11. § (1) és (2) bekezdése alapján „a diagnosztikai munkahelyeken a munkalistán megjelenő betegek adatait a leletező orvos, a vizsgálatokban részt vevő egyéb orvos, valamint az orvosok utasításai alapján az adminisztrátor kezelheti. A vizsgálat során a beteg korábbi eseteivel kapcsolatban a saját intézetben felvett valamennyi adat megtekinthető, a más betegellátási egységben felvett adatok esetében azok, amelyeket egyébként a beteg a kezébe kap. A későbbi adatbetekintés naplózásra kerül.”

Felhasználói jogosultságot csak az adott szervezeti egységnél az igénylésre kijelölt személy igényelhet az erre kialakított elektronikus felületen. Az igénylés során meg kell jelölni a leendő felhasználó munkakörét, és azt, hogy milyen körre terjedjen ki a felhasználói jogosultsága. Az igénylőlapot a felettes tanszékvezető írja alá. Ha az igényt befogadják, létrejön a felhasználónév és fiók, amely azt követően válik aktívvá, hogy a leendő felhasználó részt vesz egy, az üzemeltető által szervezett képzésen, ahol a rendszer használatához szükséges ismereteket sajátítja el, és amelyről számot is kell adnia. A hozzáférés sikeres képzés esetén aktiválódik, ezáltal a felhasználó hozzáférhet azokhoz az egységekhez, amelyek az igénylés során előre megjelölésre kerültek.

Azt, hogy a rendszerben tárolt személyes adatokhoz valóban csak az férjen hozzá, akinek arra jogosultsága van, jelenleg csak utólagosan ellenőrzik. A rendszer naplózza az adatkezelés teljes tartamát, tételesen visszakereshetők a rendszerben az elvégzett tevékenységek. Az Adatkezelő úgy nyilatkozott, hogy „bármelyik érintett számára rendelkezésre áll, a GDPR 15. cikkében rögzített, hozzáféréshez való joga alapján, az a lehetőség, hogy a személyes adatainak kezelése vonatkozásában kikérje a naplófile másolatot. Amennyiben, a naplófile kivonatokat áttekintve, visszaélés gyanúját észleli, panasszal élhet (…).” Jelenleg folyamatban van a rendszerben a célhoz kötött adatkezelést a gyakorlatban érvényesítő, és az elszámoltathatóságot biztosító programbővítés, technikai mechanizmus, amely folyamatossá tenné az adatkezelési tevékenységek ellenőrzését.

Az Adatkezelő a munkavállalók részére évente tart adatvédelmi tárgyú oktatást, melynek során megismerik az őket terhelő kötelezettségeket is, és melynek keretében a rendszer naplózási funkciójára és a hozzáférés jogára is felhívja a figyelmet.

Az Adatkezelő (ahogyan azt 2019. szeptember 23-án kelt válaszában kifejtette) a Kérelmezők által kifogásolt esetet nem minősítette adatvédelmi incidensnek, mivel megítélése szerint nem történt biztonsági sérülés. Az Intézetvezető az adatok megismerésekor „jogosult volt használni a MedSolution, illetve eMedSolution rendszereket, magatartása nem okozott biztonsági sérülést, hanem a célhoz kötött és jogszerű adatkezelés elveinek megsértését eredményezte." Az Adatkezelő emellett hivatkozott arra is, hogy az eljárásuk helyességét támasztotta alá a Hatósággal 2019. április 8-án folytatott konzultáció is, ahol „megerősítést kapott" a Hatóság részéről jelenlévőktől, hogy „az esemény nem adatvédelmi incidens volt."

Az Intézetvezetőnek három típusú, három különböző felhasználói névhez kapcsolt jogosultsága volt a rendszerekben tárolt adatok vonatkozásában:

1) a betegellátásban ellátott feladatok teljesítése érdekében az általa Intézetvezetőként irányított szervezeti egységben ellátott betegek személyes adataihoz;
2) külön engedély alapján, tudományos kutatás érdekében egy konkrét szervezeti egység (az Aneszteziológiai és Intenzív Terápiás Intézet) valamennyi osztályain ellátott betegek személyes adataihoz, a kutatási engedélyben meghatározott időtartamban;
3) külön engedély alapján, tudományos kutatás érdekében négy szervezeti egység (Sebészeti Klinika, Reumatológiai Klinika, Gyermekgyógyászati Klinika, Aneszteziológiai és Intenzív Terápiás Intézet, Sürgősségi Betegellátó Önálló Osztály) valamennyi osztályain ellátott betegek személyes adataihoz, a kutatási engedélyben meghatározott időtartamban.

A naplófájlokat tartalmazó dokumentum alapján a Kérelmezők személyes adatait az Intézetvezető az 1) és 3) típusú hozzáférési jogosultságához tartozó felhasználónevek használatával ismerte meg. A Kérelmezők személyes adatait összesen 82 alkalommal lekérte, megtekintette, és a számítógépe vágólapjára helyezte. A Kérelmezők személyes adataihoz való, Intézetvezető általi hozzáférésekre a Kérelmezők által rendelkezésre bocsátott, naplófájlokat tartalmazó táblázat tanúsága alapján 2016. június és 2017. október közötti időszakban került sor. A Kérelmezők erről a 2018. július 5-én kelt hozzáférési kérelmükre az Adatkezelő által adott válasz mellékletét képező, az információs rendszerek naplófájljait tartalmazó táblázatokból szereztek tudomást.

A Kérelmezők a fentiek alapján 2018. augusztus 28-án írásban panaszt tettek, mely alapján az Adatkezelő adatvédelmi tisztviselője 2018. szeptember 6-án személyes meghallgatást tartott, melynek nyomán a rektor belső vizsgálatot rendelt el. A vizsgálat során az Adatkezelő a panaszosok személyes meghallgatásával, illetve az adatkezeléseket rögzítő naplófájlok áttekintésével próbálta meg feltárni a körülményeket. Ezek alapján megállapításra került (az Adatkezelő 2020. január 6-i válaszának 7. számú mellékletét képező dokumentumban), hogy az Intézetvezető „több alkalommal a belépési kereteit túllépve nyert ki adatot a MedSolution rendszerből, az ügy összes körülményeit figyelembe véve, vélhetően erre irányuló munkaköri kötelezettség, vagy erre irányuló kutatási engedély nélkül. Ezzel a magatartásával megszegte nemcsak a Szegedi Tudományegyetem Szent-Györgyi Albert Klinikai Központ és Általános Orvostudományi Kar Adatvédelmi Szabályzat 1. sz. kiegészítésének (a továbbiakban: MedSolution Szabályzat) előírását, hanem annak alapvető kereteit meghatározó belső Adatvédelmi Szabályzatok, valamint az adatvédelmi jogszabályok által deklarált előírásokat is. Magatartását vélhetően tovább súlyosbítja, hogy ezen adatokat jogosulatlanul nyilvánosságra is hozta, munkatársai elmondása szerint ezen információkat az emberi méltósággal össze nem egyeztethető módon fel is használta."

A belső vizsgálat eredményeit összefoglaló, az Adatkezelő adatvédelmi tisztviselője által tett megállapításokat tartalmazó dokumentumban az esetet adatvédelmi incidensnek minősítette a tisztviselő, amelyet súlyosnak ítélt meg. A GDPR 33-34. cikkeiben foglalt kötelezettségekkel kapcsolatban a tisztviselő rögzítette, hogy azok nem alkalmazandók, mivel az adatokhoz való jogellenes hozzáférésre a GDPR alkalmazandóvá válását, 2018. május 25-ét megelőzően került sor. Ezért a rektornak címzett összefoglalóban azt a következtetést vonta le, hogy az incidens bekövetkezésekor hatályban lévő Infotv. alapján nem áll fenn az Adatkezelőnek kötelezettsége az incidens Hatóság felé történő bejelentésére, ugyanakkor szükséges felvezetni azt az incidens-nyilvántartásba. Emellett rögzíti, hogy az érintettek tájékoztatására is sor került.

A belső vizsgálat eredményeként, a személyes adatokkal vélhető visszaélés okán az Adatkezelő az illetékes nyomozóhatóság felé a rektor bűncselekmény alapos gyanúját bejelentette, illetve az Intézetvezető vezetői megbízatása, munkaviszonya megszüntetésre került. Emellett a rektor intézkedett a MedSolution, illetve eMedSolution rendszerek felülvizsgálata iránt is, amelynek eredményeként összeállítottak egy elvárás listát, melyet a rendszer fejlesztőjének, üzemeltetőjének is megküldtek.

Az esettel kapcsolatban a Kérelmezőket, a panasz benyújtását követően első alkalommal 2018. augusztus 29-én tájékoztatta az Adatkezelő, melyben közölte, hogy a panasz nyomán vizsgálatot folytat le. 2018. szeptember 28-án is sor került a Kérelmezők tájékoztatására, melyben az Adatkezelő arról tájékoztatta Őket, hogy „az ügyet kivizsgálta, és a szükséges munkáltatói intézkedést megtette. A vizsgálat során megállapítást nyert, hogy a panaszukban leírtak túlmutatnak az Egyetem Rektorának hatáskörén, így a Szegedi Tudományegyetem a nyomozóhatóság irányába bejelentéssel élt.” 2018. október 3-án az Adatkezelő adatvédelmi tisztviselője is tájékoztatta a Kérelmezőket arról, hogy az Intézetvezető „vélhető jogellenes adatkezelése tekintetében Prof. Dr. Rovó László Rektor Úr belső vizsgálatot rendelt el. A belső vizsgálat során adatvédelmi szempontból, a vizsgálatban részt vevő szervezeti egységekkel együtt az ügy általunk, hatáskörön belül vizsgálható kérdéseket áttekintettük.” A tisztviselő is tájékoztatta emellett a Kérelmezőket arról, hogy az illetékes nyomozóhatóság felé az Adatkezelő bejelentette a bűncselekmény alapos gyanúját.

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 vizsgált adatkezelésre az általános adatvédelmi rendeletet kell alkalmazni.

Az általános adatvédelmi rendelet 5. cikk (1) bekezdés f) pontja alapján, az adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

Az általános adatvédelmi rendelet 4. cikk 7. pontja alapján „adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az

adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.”

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 32. cikk (1) bekezdése értelmében az adatkezelő és az adatfeldolgozó a tudomány és 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 kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, (a b) pont értelmében) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét. Ugyanezen cikk (2) bekezdése alapján, 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.

A 32. cikk (4) bekezdése továbbá előírja, hogy „az adatkezelő és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.”

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.

A GDPR 33. cikk (3) bekezdése tartalmazza, hogy a Hatóság felé tett bejelentésnek melyek a minimális tartalmi elemei, ezek a következők:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az általános adatvédelmi rendelet 33. cikk (5) bekezdése úgy rendelkezik, hogy „az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.”

Az általános adatvédelmi rendelet 34. cikke 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 érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a 33. cikk (3) bekezdésének b), c) és d) pontjában említett információkat és intézkedéseket.

A 33. cikk (3) bekezdés b), c) és d) pontjában található információk a következők:

a) „közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
b) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
c) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.”

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2016. június és 2017. október közötti időszakban hatályban lévő 3. § 26. pontja alapján: „*adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.”*

Ugyanezen jogszabály 7. §-a az alábbiakat tartalmazta:

„7. § (1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

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

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

(4) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja

a) a jogosulatlan adatbevitel megakadályozását;

b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;

c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;

d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;

e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és

f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek."

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüaktv.) 1999. VII. 13-tól hatályos 6. §-a alapján: " *az egészségügyi és személyazonosító adatok kezelése és feldolgozása során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.*"

Az Infotv. 2. § (2) bekezdése szerint az általános adatvédelmi rendeletet az ott megjelölt rendelkezésekben foglalt kiegészítésekkel kell alkalmazni.

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 Infotv. 60/A. § (1) bekezdése alapján az adatvédelmi hatósági eljárásban az ügyintézési határidő százötven nap.

Az Ákr. 51. § b) pontja alapján, ha a hatóság az ügyintézési határidőt túllépi – és függő hatályú döntés meghozatalának nem volt helye – az eljárás lefolytatásáért illetéknek vagy díjnak megfelelő összeget, ennek hiányában tízezer forintot megfizet a kérelmező ügyfélnek, aki mentesül az eljárási költségek megfizetése alól is.

Az Ákr. 35. § (1) bekezdése szerint a kérelem az ügyfél olyan nyilatkozata, amellyel hatósági eljárás lefolytatását, illetve a hatóság döntését kéri jogának vagy jogos érdekének érvényesítése érdekében.

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 GDPR 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.

III. Döntés

III.1. A kérelem tartalma, a hatósági eljárás tárgya

A kérelemben a Kérelmezők azt kifogásolták, hogy a személyes adataik Adatkezelő általi kezelése során megvalósult adatvédelmi incidenst az Adatkezelő nem minősítette ekként, és azzal összefüggésben nem teljesítette kötelezettségeit, így például nem jelentette be azt a Hatóságnak. A Hatóság, a kérelem elbírálása érdekében, az eljárás során megvizsgálta, hogy a vizsgált eset megvalósított-e a Kérelmezők személyes adataira vonatkozóan adatvédelmi incidenst, és amennyiben igen, azzal kapcsolatban teljesítette-e ez Adatkezelő a számára a GDPR által előírt kötelezettségeket. A Kérelmezők általánosságban az incidens esetén fennálló kötelezettségek Adatkezelő általi teljesítésének hiányát kifogásolták, így a Hatóság a GDPR 33-34. cikkében foglaltak szerint folytatta le az adatvédelmi vizsgálatot a kérelem keretei között.

A Hatóság nem vizsgálta azt, hogy az Intézetvezető általi hozzáférések időpontjában az Adatkezelő teljesítette-e a MedSolution és eMedSolution rendszerekkel összefüggésben végrehajtott adatkezelésre vonatkozóan az akkor hatályban lévő jogszabályokban fennálló, a személyes adatok biztonságának garantálására irányuló kötelezettségeit, illetve meghozta-e és alkalmazta-e a tőle elvárható intézkedéseket. A Hatóság, annak vizsgálatára, hogy ezekre a jelenleg is használt rendszerekre vonatkozóan megfelelő technikai és intézkedések vannak-e érvényben az Adatkezelőnél az adatbiztonság garantálására, a jelen eljárástól elkülönülten, hivatalból indíthat vizsgálati vagy hatósági eljárást.

A Hatóság emellett nem vizsgálta jelen eljárásban azt sem, hogy az Intézetvezető elkövetett-e jogellenes adatkezelést a Kérelmezők személyes adataihoz való hozzáféréssel, tárolásával, illetve harmadik személyekkel való közlésével. Ennek vizsgálata során az Intézetvezető minősülne adatkezelőnek, mivel ezen adatkezelés (például a lekérdezett adatok tárolása, közlése) célját, és körülményeit ő maga határozta meg.

Tekintettel arra, hogy a Kérelmezők kérelme kizárólag az Adatkezelő adatvédelmi incidenssel kapcsolatos kötelezettségeinek teljesítésére vonatkozott, a Hatóság jelen eljárása csak ennek vizsgálatára terjedt ki.

III.2. Adatkezelő kiléte

A Kérelmezők kérelmükben a Szegedi Tudományegyetemet jelölték meg, mint Kérelmezett adatkezelőt, amelyet a Kérelmezett válaszaiban nem vitatott. Az esettel érintett MedSolution, illetve eMedSolution rendszerekben történő adatkezelés vonatkozásában tehát a Kérelmezett minősül adatkezelőnek.

III.3. Adatvédelmi incidens bekövetkezése

Az Adatkezelő az eljárás során azt nyilatkozta, hogy az eset nem valósított meg adatvédelmi incidenst, ezzel kapcsolatban hivatkozott arra is, hogy az eljárásuk helyességét támasztotta alá a Hatósággal 2019. április 8-án folytatott konzultáció is, ahol „megerősítést kapott” a Hatóság részéről jelenlévőktől, hogy „az esemény nem adatvédelmi incidens volt.” A Hatóság hangsúlyozza, hogy a megbeszélés általános adatvédelmi kérdésekre terjedt ki, azon a Hatóság a konkrét esettel kapcsolatban hivatalos álláspontot nem alakított ki. Az ennek során, a körülmények pontos ismerete nélkül megfogalmazott vélemény nem minősül a Hatóság hivatalos álláspontjának, a GDPR 5. cikk (2) bekezdése, illetve 24. cikke alapján az adatkezelő felelős az

adatkezelésre vonatkozó elveknek való megfelelésért, illetve a megfelelés igazolásáért, valamint olyan intézkedéseket kell hoznia, amelyek alkalmasak arra, hogy biztosítsa és bizonyítsa azt, hogy az adatkezelés a GDPR-ban foglaltaknak megfelelően történik.

Az Intézetvezető általi hozzáférésekre a GDPR alkalmazandóvá válása, 2018. május 25. előtt került sor (a naplófájlokat tartalmazó táblázat tanúsága alapján 2016. június és 2017. október közötti időszakban), arról az Adatkezelő a Kérelmezők 2018. augusztus 28-án kelt panasza alapján szerzett tudomást.

„Amikor az adatkezelő egyéntől, médiaszervezettől vagy más forrásból először értesül esetleges adatvédelmi incidensről, vagy saját maga észlel biztonsági incidenst, rövid vizsgálatot folytathat annak megállapítása érdekében, hogy valóban sérültek-e adatok."[1] Az Adatkezelőnek akkor kell megállapítania, hogy adatvédelmi incidens következett-e be, amikor ezzel kapcsolatos információ jut tudomására. A vizsgált ügyben az Adatkezelőnek tehát a Kérelmezők jelzését követően kellett megállapítania, hogy történt-e adatvédelmi incidens.

Annak vizsgálata során, hogy történt-e adatvédelmi incidens, a GDPR 4. cikk 12. pontjából kell kiindulni, amely szerinti a „biztonság sérülése" esetén lehet adatvédelmi incidens bekövetkezését megállapítani, 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.[2]

A biztonság sérülése körében a Hatóság arra a kérdésre fókuszált, hogy az Adatkezelőtől elvárható volt-e olyan adatbiztonsági intézkedés meghozatala, amely megakadályozta volna az Intézetvezető általi jogosulatlan hozzáférést, vagy ilyen jogosulatlan hozzáférésről megfelelő időben jelzést küldött volna az Adatkezelő számára. Ha ugyanis ilyen intézkedés nem volt elvárható az Adatkezelőtől, akkor nem beszélhetünk a "biztonság sérüléséről", illetve ennek hiányában pedig adatvédelmi incidensről, és kizárólag az Intézetvezető jogellenes adatkezelését lehetne vizsgálni. Amennyiben elvárható erre irányuló adatbiztonsági intézkedés az Adatkezelőtől, akkor viszont megállapítható a "biztonság sérülése", melyből az következik, hogy az Intézetvezető tevékenységével megvalósuló eset az Adatkezelő adatkezelése során megvalósuló adatvédelmi incidensnek minősül.

Szükséges azt a sajátosságot is rögzíteni, hogy az Adatkezelőtől elvárható adatbiztonsági intézkedések esetében a 2016. június és 2017. október közötti időszakban hatályos Infotv. rendelkezéseit kell alkalmazni. Ennek oka az, hogy a Kérelmezők által megküldött, naplófájlokat tartalmazó táblázat tanúsága alapján az Intézetvezető 2016. június és 2017. október közötti időszakban fért hozzá a MedSolution, illetve eMedSolution rendszerben a Kérelmezők személyes adataihoz. Ezért az adatbiztonsági követelmények tekintetében az Infotv. ebben az időszakban hatályos rendelkezéseit, illetve az ezen időszakban fennálló egyéb – például ágazati jogszabályban megállapított, a 29-es Munkacsoport[3] iránymutatásaiban, véleményeiben, illetve a Hatóság ezen időszakban keletkezett döntéseiben megfogalmazott – adatvédelmi követelményeket kell vizsgálni.

[1] WP250 rev.01. A. 2. pont

[2] A Hatóság itt jegyzi meg, hogy amennyiben az esetet az Adatkezelő a tudomásszerzést követően a jogosulatlan hozzáférések időpontjában hatályos Infotv. 3. § 26. pontja alapján ítéli meg, akkor is ugyanarra az eredményre kellett volna, hogy jusson a két jogszabály fogalommeghatározásának hasonlósága miatt.

[3] A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv 29. cikke szerint létrehozott adatvédelmi Munkacsoportnak

Az Infotv. adatbiztonságra vonatkozó rendelkezései magas szintű adatbiztonságot követeltek meg az adatkezelőktől, amely intézkedésekkel nem csak az Infotv.-nek, hanem más jogszabályoknak való megfelelést is biztosítania kellett az adatkezelőknek. Ez azért lényeges az Adatkezelő esetében, mivel egészségügyi szolgáltatónak minősül, ezért az egészségügyi adatok kezelése tekintetében az Eüaktv.-re is figyelemmel kell lennie. Ez utóbbi, 6. §-ában megerősíti az Infotv. adatbiztonságra vonatkozó rendelkezéseit, és külön hangsúlyozza ennek fontosságát az egészségügyi adatok tekintetében.

Ahogy azt a Hatóság 2013. november 7.-én kelt, NAIH-559-26/2013/H. számú határozatában az Infotv. 7. § (6) bekezdését illetően megfogalmazta, " [az adatkezelőktől] – *tekintettel gazdasági súlyukra és arra, hogy több mint 50 ezer érintett személyes adatát kezelték – elvárható volt, hogy ennek a kikötésnek úgy tesznek eleget, hogy a rendelkezésre álló adatbiztonsági technikák közül a leghatékonyabbat alkalmazzák*." Ezen túlmenően a Hatóság ugyanezen határozatában kimondta azt is, hogy "*meg kell említeni azt a nemzetközi gyakorlatban is számon kért elvárást, amely szerint az ügyek elbírálása során tekintettel kell lenni az érintette elvárásaira, várakozásaira személyes adataik (magánszférájuk) védelmével kapcsolatban.*" A Hatóság régóta következetes álláspontja szerint általános elvárás az adatkezelőkkel szemben, hogy az adatbiztonság szintjének meghatározása során figyelemmel legyenek gazdasági súlyukra, illetve az érintettek számára, az érintettek elvárásaira és várakozásaira. A korábban hivatkozott ügyben a Hatóság hangsúlyozta, hogy külön nyomatékot ad a megfelelő adatbiztonsági intézkedéseknek az is, hogy ennek hiányában az adatkezelő felelős lehet az adatvédelmi incidensben: "*az adatbiztonsági intézkedések hiányossága révén adatvédelmi jogi értelemben tehát egyértelműen megragadható az adatkezelő jogellenes közrehatása abban, hogy az egyébként szintén jogellenes hackertámadás elérje célját, és a személyes adatok nyilvánosságra kerüljenek*."[4]

A 29-es Munkacsoport 3/2014. számú véleményében kiemeli annak fontosságát, hogy az adatkezelők proaktívak legyenek és megfelelően tervezzék meg az adatbiztonsági intézkedéseiket, és hangsúlyozza azt, hogy az adatkezelőknek értékelni kell az adatkezelés kockázatait, és ezekre tekintettel kell meghozniuk a szükségesnek tartott adatbiztonsági intézkedéseket.

Figyelemmel tehát az Adatkezelőre vonatkozó jogszabályokra, a Hatóság gyakorlatára, és a 29-es Munkacsoport véleményére, az Adatkezelőtől elvárható (volt), hogy a rendszerrel összefüggő adatkezelésre vonatkozó adatbiztonsági intézkedések megtervezése, alkalmazása során figyelemmel legyen az alábbiakra:

- az általa végzett tevékenységre: egészségügyi szolgáltatás nyújtása, amely kiemelt felelősséggel jár;
- az adatkezelés nyilvánvaló körülményeire, így például arra, hogy nagyszámú érintettre vonatkozóan, nagy számban kezel különleges adatokat (egészségügyi adatokat);
- azon reális, valós kockázatokra, amelyekkel az Adatkezelő tevékenységét illetően ésszerűen számolni lehet (így például azzal, hogy hozzáférési jogosultsággal rendelkező személy ezen helyzetéből fakadóan könnyen túl tud terjeszkedni a hozzáférési jogosultságának terjedelmén);
- figyelembe kell venni azt is, hogy az érintettek egy egészségügyi szolgáltatótól azt várják el, hogy nem kell attól tartaniuk, hogy a magánszféra, emberi méltóság szempontjából rendkívül fontos, az egészségi állapotra vonatkozó adatokat különösebb kontroll nélkül tudják megismerni bizonyos személyek.

[4] https://www.naih.hu/files/559_2013_hatarozat_anonim.pdf

Ezen túlmenően, amennyiben az Adatkezelő ezen értékelése alapján az az eredmény születne, hogy több adatbiztonsági intézkedés is megfelelő lehet, akkor az Infotv. 7. § (6) bekezdése alapján ezek "*közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek*."

A Hatóság értékelése szerint az Adatkezelőtől tehát elvárható volt egy olyan kontroll vagy jelzőrendszer beépítése a MedSolution, illetve eMedSolution rendszerbe, amely megfelelő védelmet jelentett volna hosszan tartó vagy túlzott mértékű jogosulatlan hozzáféréssel szemben. 2016-ban is elvárás volt egy különleges adatokat nagy számban kezelő rendszerrel szemben, hogy gyakori, illetve ismétlődően visszatérő lekérdezések esetén jelezzen a rendszer üzemeltetője felé, hiszen ilyen jelzés nélkül sem a külső, sem a belső rosszindulatú támadás sem szűrhető ki, előzhető meg. Emellett az Adatkezelőtől az is elvárható volt, hogy szervezési, adminisztratív intézkedéseket hozzon a jogosulatlan hozzáférés megelőzése, illetve kiszűrése érdekében, amely biztosítja, hogy rendszeresen, vagy legalább szúrópróbaszerűen ellenőrizze, hogy a rendszerben tárolt adatokhoz valóban csak az arra jogosultak férnek hozzá, és a felhasználók hozzáérési jogosultságukkal nem élnek vissza.

Az adatbiztonságot garantáló intézkedések körébe tartoznak ugyanis azok a technikai és szervezési intézkedések is, amelyeknek az a célja, hogy garantálják a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét, vagyis azt, hogy azt, hogy az erre feljogosított személyek az adatokhoz hozzá férjenek, módosíthassák vagy törölhessék azokat. Az intézkedéseknek azt is garantálni kell, hogy az erre feljogosított személyek csak a részükre adott jogosultsági keretek között, az adatkezelő utasításainak megfelelően járhassanak el, vagyis csak az arra jogosult, hozzáféréssel rendelkező személyek férhessenek hozzá az általa kezelt személyes adatokhoz, és csak abból a célból, amelyre az adatkezelő utasítást, felhatalmazást adott.

Annak feltérképezése, megállapítása, hogy milyen technikai és szervezési intézkedésekkel lehet, illetve lehetetett volna biztosítani a kezelt személyes adatok biztonságát, (például annak megakadályozását, hogy a munkakör ellátásához nem szükséges személyes adatokhoz is hozzáférjenek a munkavállalók, illetve az ilyen hozzáférést kellő időben fel lehessen ismerni), csakúgy, mint az ilyen intézkedések hatékony alkalmazása, az Adatkezelő kötelezettsége.

A Hatóság ilyen adatbiztonsági intézkedésként azonosította például, hogy a betegek személyes adatainak nyilvántartására szolgáló rendszerhez kapcsolódó hozzáférési jogosultság igénylése során rögzítve van az igénylőlapon a jogosultság célja (az Intézetvezető esetében betegellátás, illetve tudományos kutatás), valamint azt is, hogy a rendszerre vonatkozó szabályzat egyértelműen lefekteti a használat szabályait, amelyből megállapítható, hogy milyen esetekben, milyen szabályok mellett kerülhet sor a rendszerben tárolt adatok megismerésére, kezelésére.

A Hatóság szerint, az ilyen, az adatok biztonságát szolgáló intézkedések hiánya, vagy ilyen intézkedések gyakorlati alkalmazásának mellőzése miatt – például egy munkavállaló szándékos magatartása által – tehát megvalósult a személyes adatok biztonságának sérülése.[5]

[5] Ahogy az korábban kifejtésre került, jelen eljárás nem terjedt ki annak vizsgálatára, hogy a MedSolution és eMedSolution rendszerekben megvalósuló adatkezelés vonatkozásában érvényben voltak-e, illetve vannak-e megfelelő szervezési és technikai intézkedések, amelyek garantálják a kezelt személyes adatok biztonságát. Ennek vizsgálatára a jelen ügytől elkülönülő, hivatalból indított hatósági eljárásban kerülhet sor.

A Kérelmezők, illetve az Adatkezelő által rendelkezésre bocsátott bizonyítékok, dokumentumok alapján megállapítható, hogy az Intézetvezető számos (a három Kérelmező esetében összesen 82) alkalommal megtekintette, illetve vágólapra helyezte a Kérelmezőkkel kapcsolatban a rendszerben rögzített dokumentumokat, információkat (például leletek, esetadatok, ambuláns adatlapok, beteg alapadatok, esetinformációk), amelyek személyes adatokat tartalmaznak. A személyes adataikat az Intézetvezető a számára betegellátási, illetve kutatási célból biztosított hozzáférési jogosultsághoz tartozó felhasználónevek használatával ismerte meg, helyezte vágólapra, vagyis végzett azokon adatkezelési műveletet.

A Hatóság megállapította, hogy – ahogy azt az Adatkezelő belső vizsgálatában tett megállapítások, illetve a Kérelmezők nyilatkozatai is alátámasztják, – az Intézetvezető annak ellenére fért hozzá a Kérelmezők egészségügyi ellátásaival összefüggésben, az Adatkezelő tevékenysége során keletkezett személyes adataihoz, hogy konkrétan ezen adatok megismerésére nem volt jogosult, hiszen ezen adatokhoz való hozzáférésre nem a munkájához szükséges, betegellátási vagy kutatási célból került sor.

A biztonság sérülése tehát a vizsgált esetben azt eredményezte, hogy a Kérelmezők személyes adataihoz az Intézetvezető jogosulatlanul hozzáfért, megismerte azokat.

A fentiek alapján tehát a Kérelmezők személyes adataival kapcsolatban az adatok bizalmas jellegét érintő adatvédelmi incidens következett be.

III.4. Az incidenssel összefüggő adatkezelői kötelezettségek teljesítése

Az Adatkezelő 2018. augusztus 28-án, a Kérelmezők írásbeli panasza alapján értesült az Intézetvezető magatartásáról, illetve a jogosulatlan, illetve jogellenes hozzáférés gyanújáról. A belső vizsgálata során tehát ekkor meg kellett volna állapítania, hogy sérült az adatok biztonsága, és legkésőbb a vizsgálat lezárultával az Adatkezelő teljes bizonyossággal tudomást szerezhetett volna az adatvédelmi incidensről (nem kizárt, hogy vizsgálat során már korábban erre a felismerésre jutott volna).

A GDPR 33-34. cikkeiben foglalt kötelezettségek adatkezelő általi alkalmazása akkor merül fel, amikor az adatvédelmi incidens az adatkezelő tudomására jutott, az incidens bekövetkezésének időpontja e kötelezettségek szempontjából nem releváns. Az említett cikkekben rögzített kötelezettségek vonatkozásában tehát nem az incidens bekövetkezése, hanem az adatkezelő erről való tudomásszerzésének időpontja a releváns, az alkalmazandó jogszabály szempontjából meghatározó tény. Mivel erre egyértelműen 2018. május 25-ét követően (legkorábban 2018. augusztus 28-án) került sor, ezért az adatvédelmi incidenssel kapcsolatban a 33-34. cikkben foglalt kötelezettségek vonatkozásában alkalmazandó a GDPR.

Az Adatkezelőnek tehát annak megállapítását követően, hogy a biztonság sérülése személyes adatokhoz való jogosulatlan hozzáférést eredményezett, vagyis adatvédelmi incidens következett be, eleget kellett volna tennie a GDPR 33-34. cikkeiben foglalt kötelezettségeknek.

A Kérelmezők személyes adataival összefüggésben, az Adatkezelő által a MedSolution, illetve eMedSolution rendszerekben megvalósuló adatkezelése során bekövetkezett adatvédelmi incidens a Hatóság álláspontja szerint magas kockázattal járt az érintettek jogaira és szabadságaira nézve. A GDPR (75) preambulumbekezdésében foglaltaknak megfelelően, a kockázatok megítélése során a Hatóság figyelembe vette, hogy a Kérelmezők egészségügyi személyes adatait érintette az incidens, vagyis személyes adatok különleges kategóriáit. Emellett az adatvédelmi incidens során a szakmai titoktartási kötelezettség által védett személyes adatok

bizalmas jellege sérült, valamint kiszolgáltatott személyek adatainak kezelése során következett be – az egyik Kérelmező ugyanis gyermek volt, egy másik pedig alá-fölérendeltségi viszonyban állt az adatokat jogosulatlanul megismerő Intézetvezetővel. Az incidens továbbá a Kérelmezőkre vonatkoztatva nagy mennyiségű személyes adatot érintett. Tekintettel arra, hogy a felsorolt kategóriákból több egyszerre volt jelen az incidens esetében, ezért összességében a kockázat magasnak tekinthető.

A Hatóság álláspontja szerint az adatvédelmi incidenst be kellett volna jelentenie az Adatkezelőnek a Hatóság felé, legalább az említett cikkekben előírt adattartalommal. Az Adatkezelőnek indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával az Adatkezelő általi tudomásszerzést követően kellett volna bejelentenie az illetékes felügyeleti hatóság részére az adatvédelmi incidenst. A bejelentési kötelezettség csak abban az esetben nem terhelte volna az Adatkezelőt, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ahogy az fentebb megállapításra került, az eljárás tárgyát képező incidens kockázattal járt az érintettek jogaira és szabadságaira nézve.

A Kérelmezett emellett nem tett eleget azon kötelezettségének sem, mely alapján nyilván kell tartania az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. A Kötelezett az eljárás tárgyát képező incidenst tartalmazó, az általános adatvédelmi rendelet 33. cikk (5) bekezdése szerinti nyilvántartást nem bocsátott a Hatóság rendelkezésére az eljárás során, 2019. szeptember 23-án kelt válaszában úgy nyilatkozott, hogy az „ügyet nem vette nyilvántartásba, mert a megtörtént eseményt nem minősítette incidensnek.”

A Hatóság az általános adatvédelmi rendelet 34. cikkében fennálló kötelezettséggel kapcsolatban megállapította, hogy a Kérelmezők értesültek az adataikhoz való jogosulatlan hozzáférés tényéről, hiszen éppen az általuk benyújtott GDPR 15. cikke szerinti hozzáférési kérelem teljesítését követően, az ő jelzésük alapján szerzett arról tudomást maga az Adatkezelő. A 34. cikk (2) bekezdése azonban az incidens tényén túlmenően egyéb információkat is előír, amelyeket az Adatkezelőnek a Kérelmezők rendelkezésére kell bocsátani, amennyiben az adatvédelmi incidens magas kockázattal jár.

Ahogy a Hatóság fentebb kifejtette, álláspontja szerint a Kérelmezők személyes adataival kapcsolatban bekövetkezett adatvédelmi incidens magas kockázatot jelent az érintettek jogaira és szabadságaira nézve, ezért a Kötelezett köteles lett volna a Kérelmezőket haladéktalanul tájékoztatni az adatvédelmi incidensről, az általános adatvédelmi rendelet 34. cikk (2) bekezdésében előírt tartalommal. A magas kockázatú incidenseknél az érintettek tájékoztatásának indoka, hogy ők is meg tudják tenni az általuk szükségesnek vélt egyéb óvintézkedéseket a magánszférájukra jelentett kockázatok mérséklése céljából.

Bár a Kérelmezett a panasz nyomán értesítette a Kérelmezőket több alkalommal is, ezek a tájékoztatások nem tartalmazták ezeket, az általános adatvédelmi rendelet 34. cikk (2) bekezdésében meghatározott további tartalmi elemeket, így például azt, hogy melyek az incidens valószínűsíthető következményei, milyen, az incidens orvoslására tett intézkedéseket hozott, illetve az incidens körülményeire sem tért ki ezekben.

A fentiek alapján a Hatóság a kérelemnek helyt ad, és megállapítja, hogy az Adatkezelő megsértette az általános adatvédelmi rendelet 33-34. cikkeiben előírt kötelezettségeit, ezért a GDPR 58. cikk (2) bekezdés b) pontja alapján elmarasztalja.

IV. Jogkövetkezmények

A Hatóság megvizsgálta, hogy indokolt-e a Kötelezettel 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. Tekintettel az ügy körülményeire, a Hatóság megállapította, hogy a jelen eljárás során feltárt jogsértések esetében a figyelmeztetés nem arányos és nem visszatartó erejű szankció, így bírság kiszabása szükséges.

A Hatóság ennek megítélése során az alábbi tényezőket vette figyelembe:

A Kötelezett által elkövetett jogsértés a GDPR 83. cikk (4) bekezdés a) pontja szerint az alacsonyabb összegű bírságkategóriába tartozó jogsértésnek minősülnek, illetve az Infotv. 61. § (4) bekezdés b) pontja alapján a bírság mértéke százezertől húszmillió forintig terjedhet, mivel a Kötelezett, a Szegedi Tudományegyetem költségvetési szerv.[6]

A Hatóság a bírságkiszabás során súlyosító körülményként vette figyelembe a következőket:

A Kérelmezett nem első alkalommal sérti meg a személyes adatok kezelésére vonatkozó előírásokat, a Hatóság korábban NAIH/2020/2356 számú határozatban megállapította, hogy az Adatkezelő nem tett eleget a GDPR 32. cikk (1) bekezdés b) pontjában foglalt kötelezettségnek, és emiatt figyelmeztetésben részesítette.

A vizsgált adatvédelmi incidens különleges, egészségügyi személyes adatokat érint, az incidens egy ilyen kategóriájú személyes adatok kezelésével járó adatkezelés során következett be. [GDPR 83. cikk (2) bekezdés a) pont]

A Hatóság a konkrét jogsértésről a kérelem alapján szerzett tudomást, a Kérelmezett nem tett eleget az incidenssel kapcsolatban a bejelentési kötelezettségének [GDPR 83. cikk (2) bekezdés h) pont].

Az iratok alapján megállapítható, hogy hasonló incidensekre sor került már az adatkezeléssel összefüggésben, mivel az Intézetvezető jogosulatlan hozzáférését más érintettek is jelezték a Kérelmezett felé a részükre megküldött naplófájlok alapján. A kérelem alapján az eljárás a további esetleges incidensek bejelentésének elmulasztására nem terjedt ki, de megállapítható, hogy más érintettek vonatkozásában is bekövetkezett adatvédelmi incidens, amelyeket szintén nem jelentett be a Hatóság részére a Kérelmezett. [83. cikk (2) bekezdés k) pont]

A Hatóság enyhítő körülményként vette figyelembe a következőket:

Az ügyben vizsgált adatvédelmi incidensben érintettek száma alacsony, három fő. [GDPR 83. cikk (2) bekezdés a) pont]

A jelen ügyben az eset jogi szempontból történő bizonytalan megítélése, értelmezése okozta azt, hogy a GDPR-ban rögzített kötelezettségeknek nem tett eleget a Kérelmezett. Mivel nem incidensként azonosította az esetet, ezért nem teljesítette a GDPR 33-34. cikkeiben foglalt kötelezettségeket, azonban az esetet követően, megtették a szükséges intézkedéseket az incidens orvoslása céljából. Ezek a tényezők arra utalnak, hogy a jogsértés, vagyis a GDPR 33-34. cikkeinek figyelmen kívül hagyása nem szándékos volt. [83. cikk (2) bekezdés b) pont]

[6] 34909/2018. számú Alapító Okirat

Az esetet követően tettek intézkedéseket az incidens orvoslása céljából, és az érintetteket a Kérelmezett tájékoztatta az esettel összefüggésben, a tájékoztatásnak bizonyos, a 34. cikkben előírt elemei hiányoztak a fentiek miatt. [GDPR 83. cikk (2) bekezdés k) pont]

A Hatóság a fentiek figyelembevételével arra a megállapításra jutott, hogy a bírság kiszabása arányos szankciónak tekinthető, azonban a Kötelezett számára egy alacsonyabb összegű bírság is kellő visszatartó erővel bír.

A Hatóság az alkalmazott jogkövetkezmények megállapítása során nem tartotta relevánsnak a GDPR 83. cikk (2) bekezdés c), f), i), j) pontja szerinti szempontokat, mivel azok a konkrét ügy kapcsán nem értelmezhetők.

V. Az ügyintézési határidő túllépése

A Hatóság az eljárás során túllépte az Infotv. 60/A. § (1) bekezdése szerinti százötven napos ügyintézési határidőt, ezért az Ákr. 51. § b) pontja alapján tízezer forintot fizet a Kérelmezőknek – Kérelmezők írásban megjelölendő választása szerint – bankszámlára utalással vagy postai utalvánnyal.

VI. 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 Kp. 27. § (1) bekezdése 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.) 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: Rendelet) 35. §-a szerint, ha e rendelet eltérően nem rendelkezik, a veszélyhelyzet a határidők folyását nem érinti.

A Rendelet 41. § (1) bekezdés a)-c) pontja 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. 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 9.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár