Ügyszám: NAIH-1855-4/2022
Előzmény: NAIH-8855/2021

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 **Magyar Kétfarkú Kutya Párt** (székhely: 1071 Budapest, Damjanich utca 26/b 3/1.) (a továbbiakban: Ügyfél) 2021. június 26-án elektronikus úton 2A4E89072FB4FDC9D79327FA37F01AD azonosítószámon megtett adatvédelmi incidens bejelentésével kapcsolatban 2021. július 14. napján megindított hatósági ellenőrzés során feltárt körülmények miatt 2021. december 2. napján hivatalból megindított **adatvédelmi hatósági eljárásban**

1) megállapítja, hogy

a) Ügyfél megsértette 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) bekezdését és annak a)-b) pontjait, továbbá ezen cikk (2) bekezdését, amikor nem alkalmazott a pártszimpatizánsok, aktivisták adatai tárolásának kockázataival arányos adatbiztonsági intézkedéseket.

b) Ügyfél megsértette az általános adatvédelmi rendelet 5. cikk (2) bekezdését, mivel a Hatóság többszöri felhívásai ellenére sem igazolta teljes körűen, hogy milyen intézkedéseket tett az adatvédelmi incidens kockázatainak csökkentése érdekében.

2) Utasítja az Ügyfelet, hogy

a) az általános adatvédelmi rendelet 5. cikk (2) bekezdésére tekintettel igazolja azt a Hatóság felé, hogy az érintettek adatvédelmi incidensről való tájékoztatását az általános adatvédelmi rendelet 34. cikkének megfelelően mikor, milyen formában és tartalommal tette meg.

b) tájékoztassa arról a Hatóságot, hogy az incidensben érintett adatkezelést hogyan alakította át annak érdekében, hogy arra kockázatokkal arányos adatbiztonsági intézkedéseket alkalmazzon.

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

3.000.000 Ft, azaz hárommillió forint

adatvédelmi bírság megfizetésére kötelezi;

1055 Budapest
Falk Miksa utca 9-11.
Tel.: +36 1 391-1400
Fax: +36 1 391-1410
ugyfelszolgalat@naih.hu
www.naih.hu

4) **Elrendeli a végleges határozatnak** Ügyfél azonosító adatainak közzétételével történő **nyilvánosságra hozatalát.**

A fenti 3) pont szerinti 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-1855/2022 BÍRS. számra kell hivatkozni.

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

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

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

INDOKOLÁS

I. Előzmények és a tényállás tisztázása

1) Az Ügyfél 2021. június 26-án elektronikus úton 2A4E89072FB4FDC9D79327FA37F01AD azonosítószámon incidensbejelentést tett a Hatóságnál az adatkezelését érintő adatvédelmi incidenssel kapcsolatban, amelyről aznap szerzett tudomást.

Az incidensbejelentésben Ügyfél az alábbiakat közölte a Hatósággal:

Ügyfél 2021. június 26-án értesült arról, hogy összesen hat darab .xlsx kiterjesztésű, Excel fájl – amelyek korábban Ügyfél kezelésében voltak – közvetlenül, bárki számára hozzáférhető módon elérhetővé tettek a https://ufile.io/f/wn8iy linken keresztül. A linkre a https://kuruc.info/r/2/23220 címen keresztül elérhető cikk is hivatkozik. A fájlok a következőek voltak:

- *Rósáné2 szórólapküldés.xlsx*
- *PÁRTOLÓ TAGOK.xlsx*
- *Országfelosztás.xlsx*
- *MKKP kampányjelentkezők 2018 (Responses).xlsx*
- *MKKP Beszerzési Főosztály.xlsx*
- *kimicsinál (MKKP alkalmazottak, feadatkörök).xlsx*

Ügyfél bejelentése alapján a táblázatok pártoló tagjaik névsorát és működési adatokat tartalmaznak, továbbá azokban elérhetőségi adatok is szerepelnek (telefonszám, e-mail címek, lakcímek, személyi igazolvány számok). Az adatvédelmi incidensben Ügyfél bejelentése alapján kb. 2000 érintett személyes adatai érintettek, köztük a 2018-as választási kampányba jelentkezők adatai, a párt pártoló tagjainak pontos adatai, a párt belső koordinátorainak és segítőinek neve, a párt 2022-es választási jelöltjeinek névsora. Ügyfél a bejelentéskor nem tudta még egyértelműen megállapítani, hogy az adatok kiszivárgása külső cselekmény (pl. hackertámadás), vagy belső szivárogtatás eredménye. Az incidenst követően a hozzáférést a fájlok megtekintéséhez a társelnökök kivételével mindenkitől megvonták.

Ügyfél az adatvédelmi incidensről a bejelentéskor nem tájékoztatta az érintetteket, de azt a jövőben tervezi, mivel a kockázatok szempontjából „jelentősnek" ítélte azt. A tájékoztatás tervezett időpontjaként 2021. június 26-át jelölte meg.

2) A Hatóság az incidensbejelentés kapcsán 2021. július 14-én hatósági ellenőrzést indított annak megítélése céljából, hogy Ügyfél maradéktalanul eleget tett-e a bejelentett incidens kezelése során az általános adatvédelmi rendeletben foglalt előírásoknak. A Hatóság NAIH-5885-2/2021. ügyiratszámon tényállás tisztázó végzést küldött Ügyfélnek 2021. július 14-én és ennek keretei között adatszolgáltatásra szólította fel. A végzésre Ügyfél határidőben válaszolt.

Ügyfél elmondása szerint a táblázatokat hozzáférés korlátozásával védték, azokat Google Sheets táblázatként online kezelték. Korábban hozzáférést biztosítottak a táblázatokhoz a párt vezető tisztségviselői és aktivistái számára egy link segítségével. A táblázatok nyilvánosságra kerülése után a hozzáférést lekorlátozták a párt vezető tisztségviselőire. Korábban azért biztosítottak hozzáférést az aktivisták részére is, mivel a párt belső elvei szerint ők közvetlenül is tarthatják egymással a kapcsolatot.

A fájlokhoz való hozzáférésnapló elemzése kapcsán Ügyfél nem tudta azt megállapítani, hogy azokhoz illetéktelen külső támadó férhetett-e hozzá, vagy a fájlok nyilvánosságra hozatala belső szivárogtatás eredménye.

Az adatok kezelésének jogalapjaként Ügyfél az általános adatvédelmi rendelet 9. cikk (2) bekezdés d) pontját jelölte meg. Az adatokat az aktivistáktól való közvetlen adatfelvétellel gyűjtötték 2017-2018 között. Az adatok gyűjtésének és további kezelésének célja a párt politikai tevékenységében a saját akaratukból részt vevő aktivistákkal adott politikai tevékenységgel összefüggésben történő kapcsolattartás volt.

Ügyfél a fentieken túl felvette a kapcsolatot a fájlokat tároló ufile.io nevű fájlmegosztó oldallal és e-mailben, valamint telefonon is kérték a fájlok eltávolítását. Ügyfél a kuruc.info weboldal felé megkereséssel nem élt. A fájlok egyébként csak a közzétételtől számított 48 órán belül voltak nyilvánosan és ingyenesen letölthetőek. Ügyfél végül közölte, hogy ismeretei szerint nincsenek közérdekű vagy közérdekből nyilvános adatok a nyilvánosságra került személyes adatok között.

3) A Hatóság eljáró tagja által is leellenőrzésre került a bejelentésben is hivatkozott https://kuruc.info/r/2/230220 linken keresztül elérhető weboldal. A weboldalon keresztül elérhető egy sajtóhír, amely a bejelentő párt tevékenységére vonatkozik. A cikkben meghivatkozott https://ufile.io/f/wn8iy linken keresztül egy további weboldal nyílik meg, ahonnan az

incidensbejelentésben is hivatkozott .xlsx kiterjesztésű Excel fájlok voltak letölthetőek közvetlenül. A cikk, valamint a fájlokat tartalmazó honlap képéről, továbbá forráskódjáról .html formátumban mentés, továbbá képernyőfotók is készültek, valamint az adatbázisok lementésre kerültek az eredeti .xlsx formátumban. A honlap és fent felsorolt fájlok lementéséről külön-külön .sha kiterjesztésű hitelesítő fájlok készültek. Ezen folyamatokat a Hatóság NAIH-5885-2/2021. számú feljegyzésében dokumentálta.

A nyilvánosságra hozott táblázatokban az alábbi személyes adatok szerepelnek:

a) ***Rósáné2 szórólapküldés.xlsx*** fájlban:

Személyes adatok jellege, leírása	Érintettek száma
Tagok következő személyes adatai: átadó személy neve, átvevő személy neve, város megnevezése, ahol a szórólapot terjesztenék, város megnevezése, ahol a szórólapokat átveszik, cím, ahol a szórólapokat átveszik, szórólapokat átvevő személy telefonos elérhetősége	48

b) ***PÁRTOLÓ TAGOK.xlsx*** fájlban:

Személyes adatok jellege, leírása	Érintettek száma
„pártoló tag lista” fülön Pártoló tagok nyilvántartási száma, teljes neve, országos egyéni választókerület, címe, személyi igazolvány száma, telefonszáma, határozat száma és dátuma, kártya száma, jelentkezés dátuma, tagság dátuma, kilépés ténye, megjegyzés	509
„2022” fülön Pártoló tagok nyilvántartási száma, teljes neve, országos egyéni választókerület, címe, személyi igazolvány száma, telefonszáma, e-mail címe, tagság dátuma, elérhető-e a telefonszáma, aktivitási hajlandóság ténye és helyszíne, tevékenység leírása, megjegyzés	476

„Tagdíjasok” fülön tagsági szám, teljes név, jelentkezés dátuma, határozat dátuma, mikortól kell fizetnie, mikortól fizetett	35
„Tévesen értesített tagdíjasok” fülön sorszám, teljes név, telefon, e-mail cím, belépés dátuma, határozat dátuma, mikortól kell fizetnie	60
„ha passzivista is lenne, ide ir” fülön sorszám, teljes név, országos egyéni választókerület, címe, személyi igazolvány száma, telefonszáma, e-mail címe, dátum	20
„kártyaszámok” fülön kártya száma, teljes név, rendelések száma	495
„teendők” fülön teljes név, e-mail cím, telefonszám	12
„boríték” fülön teljes név, lakcím, néhány esetben értesítési cím	52
„Sheet7” fülön teljes név, országos egyéni választókerület, cím, személyi igazolvány száma, e-mail cím, telefonszám,	27

c) ***Országfelosztás.xlsx*** fájlban:

Személyes adatok jellege, leírása	Érintettek száma
„OEVK térképpel" fülön jelölt neve, segítő neve, koordinátor neve, e-mail cím, telefonszám, Facebook profil link	117
„Országfelosztva" fülön admin neve, megyei koordinátor neve, választásos koordinátor neve	56
„Sheet7" fülön jelölt neve	57

d) ***MKKP kampányjelentkezők 2018 (Responses).xlsx*** fájlban:

Személyes adatok jellege, leírása	Érintettek száma
név, e-mail cím, telefonszám, „merre kampányolnál", „miben tudsz segíteni?", „egyéb segítség"	417

e) MKKP Beszerzési Főosztály.xlsx fájlban:

A táblázatban eszközbeszerzések vannak vezetve, a projektfelelős nevével, összesen 6 esetben e-mail cím és telefonszám megadásával.

f) ***kimicsinál (MKKP alkalmazottak feladatok, feladatkörök).xlsx*** fájlban:

A fájl a párt 17 tagjának (több helyen csupán becenevekkel jelölve) feladatai elosztását tartalmazza. A fájl tartalmazza továbbá az *Országfelosztás.xlsx* táblázatot és abban lévő adatokat is egy külön fülön.

4) A Hatóság ezek után NAIH-5885-5/2021. ügyiratszámú végzéssel újabb adatszolgáltatásra szólította fel 2021. augusztus 31-én postai úton Ügyfelet, amelyet a visszaérkezett tértivevény szerint Ügyfél képviselője annak székhelyén 2021. szeptember 20-án átvett. A Hatóság által megszabott tíz napos válaszadási határidő ellenére a végzésre válasz a mai napig nem érkezett.

A Hatóság a válasz elmaradása miatt ismételten nyilatkozattételre hívta fel az Ügyfelet NAIH-5885-6/2021. számú végzésével 2021. október 25-én. Ezen végzést a Hatóság Ügyfél képviselőjének –

a korábban Ügyféltől beérkezett válaszra tekintettel – elektronikus úton kézbesítette, amelyet az a letöltési visszaigazolás alapján 2021. november 3-án átvett. A Hatóság által megszabott öt napos válaszadási határidő ellenére a végzésre válasz a mai napig nem érkezett.

5) A válaszadás ismételt elmaradása, a tényállás további tisztázása és az ügyben az általános adatvédelmi rendeletben foglalt kötelezettségek Ügyfél általi feltételezhető megsértésének további szükséges vizsgálata miatt az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 60. § (1) bekezdésére tekintettel, a Hatóság 2021. december 2-án adatvédelmi hatósági eljárás megindításáról döntött.

Az adatvédelmi hatósági eljárás megindításáról a Hatóság az Ügyfelet NAIH-8855-1/2021. ügyiratszámú végzésével értesítette, valamint további adatszolgáltatást kért tőle az elmaradt válaszokra és az adatkezelés körülményeinek további tisztázására is tekintettel. Ügyfél képviselője a végzést elektronikus úton a letöltési igazolás alapján 2021. december 6-án átvette, arra pedig a mai napig szintén nem válaszolt.

A Hatóság a fentiekre tekintettel NAIH-1855-1/2022. ügyiratszámú végzésével 2022. január 27-én a válaszok immár harmadszori elmaradása miatt 350.000 Ft eljárási bírságot szabott ki Ügyfélre az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 77. §-a alapján, mivel a tényállás feltárásához szükséges válaszok elmaradása érdemben akadályozza a Hatóságot tevékenységét, így az ügyben a tényállás teljes körű feltárását. A Hatóság továbbá Ügyfelet a korábbi végzésben foglaltak haladéktalan teljesítésére szólította fel.

Ügyfél az eljárási bírságot kiszabó, ismételt felszólító végzést hivatali kapuján keresztül a letöltési igazolás alapján 2021. január 28-án átvette, arra azonban továbbra sem válaszolt, az eljárási bírságot nem fizette meg, illetve jogorvoslattal sem élt az ellen a megszabott 30 napos határidőn túl sem. A Hatóság az eljárási bírságot kiszabó végzést tértivevényes postai küldeményként is megküldte Ügyfélnek a címére, a küldemény azonban „nem kereste” jelzéssel érkezett vissza 2022. február 18-án.

II. Alkalmazott jogszabályi rendelkezések

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

Az általános adatvédelmi rendelet 4. cikk 12. pontja határozza meg, hogy mi minősül adatvédelmi incidensnek, ez alapján „adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerint a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.

Az általános adatvédelmi rendelet 5. cikk (2) bekezdése határozza meg az „elszámoltathatóság alapelvét”, amely szerint az adatkezelő felelős a rendelet 5. cikk (1) bekezdésében foglalt alapelveinek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

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

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

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

Az általános adatvédelmi rendelet 34. cikk (1)-(2) bekezdései szerint 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.

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. 99. §-a alapján a hatóság – a hatáskörének keretei között – ellenőrzi a jogszabályban foglalt rendelkezések betartását, valamint a végrehajtható döntésben foglaltak teljesítését.

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 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.

Az általános adatvédelmi rendelet 83. cikk (5) bekezdés e) pontja szerint az 58. cikk (1) bekezdését megsértve a hozzáférés biztosítására vonatkozó rendelkezések elmulasztása esetén legfeljebb 20 000 000 EUR összegű, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összegű közigazgatási bírság szabható ki, azzal, hogy a kettő közül a magasabb összeget kell kiszabni.

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

III. Döntés

1. Az adatkezelés biztonságával kapcsolatos megállapítások

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

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

A Hatóság megítélése szerint az incidenssel érintett adatkezelés, így a politikai párt tagjai, szimpatizánsai és aktivistái személyes adatainak (pl. azonosító adatok, elérhetőségek, párttal kapcsolatos tevékenységek) kezelése magas kockázatúnak minősül. Ennek oka, hogy általános adatvédelmi rendelet (75) preambulumbekezdése az olyan adatkezelést, amely során politikai véleménnyel összefüggésbe hozható adatokat kezelnek alapvetően kockázatosnak tekinti. Ezzel összefüggésben szintén kockázatosnak tekinti, ha az adatkezelésből hátrányos megkülönböztetés fakadhat, továbbá ha az adatkezelés nagyszámú érintettre terjed ki. Végül az olyan adatok kezelését, amelyekből személyiség-lopás, vagy személyazonossággal való visszaélés (ilyenek jelen ügyben a táblázatokban szereplő azonosító adatok, így: név, lakcím, telefonszám, e-mail cím, személyazonosító igazolvány száma, Facebook profil link) fakadhat, szintén kockázatosnak tekintik a rendelet ezen előírásai.

A Hatóság megítélése szerint az összesen hat darab nyilvánosságra került táblázatban szereplő érintettek adatainak kezelése magas kockázatúnak tekinthető az általános adatvédelmi rendelet fenti előírásai alapján. A táblázatban szereplő adatkör alapján egyedileg nagyon könnyen beazonosíthatóvá válhatnak a párttal szimpatizáló, annak működése során különböző feladatokat ellátó érintettek az elérhetőségi adatoknak a nevekkel és pártszimpátiával való együttes kezelése miatt. Az adatok bizalmasságának sérülése magas kockázatokkal jár az érintettek magánszférájára nézve, mivel valamely politikai szervezethez tartozás – még ha esetleg múltbéli is – mindenképpen az adott személy politikai véleményét tükrözi.

A politikai véleményre vonatkozó adatok 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 nyilvánosságra hozatala, illetéktelen általi megismerése 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.

Az adatkezelés kockázatait végül az is növeli, hogy nagyszámú, több mint 2000 érintett személyes adatai kerültek együtt kezelésre a táblázatokban.

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

A Hatóság megítélése alapján az érintettekhez köthető azonosító adatok és politikai véleményt is tükröző adatok a Google Sheets online, ingyenesen elérhető szolgáltatás keretei közötti kezelése abban a formában, ahogy az jelen ügyben megvalósult, nem felel meg a magas kockázatú adatkezeléssel jelentett kockázatokkal arányos adatbiztonság szintjének.

A Google Sheets egy táblázatkezelő program, amely a Google által kínált ingyenes, webalapú Google Docs Editors csomag része. Az alkalmazás lehetővé teszi a felhasználók számára, hogy online hozzanak létre és szerkesszenek fájlokat, miközben valós időben együttműködnek más felhasználókkal. A módosításokat a felhasználók nyomon követhetik, a módosításokat bemutató verzióelőzményekkel. A szerkesztő pozíciója szerkesztőspecifikus színnel és kurzorral van kiemelve, és egy engedélyezési rendszer szabályozza, hogy a felhasználók mit tehetnek. A dokumentumokat egyszerre több felhasználó is megoszthatja, megnyithatja és szerkesztheti. A módosítások automatikusan mentésre kerülnek a Google szervereire, és a rendszer automatikusan megőrzi a verzióelőzményeket, így a korábbi módosítások megtekinthetők és visszaállíthatók. A fájlok különböző formátumokban exportálhatók a felhasználó helyi számítógépére, például PDF és Office Open XML formátumban.[1]

[1] Lásd: - https://www.google.hu/intl/hu/sheets/about/;
- https://en.wikipedia.org/wiki/Google_Sheets

A táblázatokban szereplő nagyszámú különleges személyes adat kezelése önmagában is nagyon komoly kockázatokkal jár az érintettek magánszférájára nézve. Az Ügyfél a magas kockázatú adatkezelés kapcsán hozzáférést biztosított a táblázatokhoz a párt vezető tisztségviselői és aktivistái számára egy link segítségével, mivel a párt belső elvei szerint az aktivisták közvetlenül is tarthatják egymással a kapcsolatot. A táblázatokhoz így akár több ezer érintett is hozzáférhetett egyszerre online egy egyszerű hivatkozás segítségével, egyéb korlátozás nélkül. Mivel a Google Sheets online szolgáltatásából a fájlok egyszerűen exportálhatóak és lementhetőek a felhasználók helyi számítógépére, ezért ilyen nagyszámú hozzáférés bármilyen egyéb jogosultságkontroll (pl. a táblázathoz való jelszavas hozzáférés) nélküli biztosítása esetén nagyon valószínű annak a bekövetkezése, hogy az adatokhoz akár jogosulatlan személyek is hozzáférnek, vagy az előzetesen arra jogosult személy azt továbbküldi másoknak is, esetleg azokat önmaga hozza nyilvánosságra. A fájlok bizalmasságának megőrzése érdekében titkosítás alkalmazására sem került sor.

A további megfelelő kontrollintézkedések alkalmazása nélkül nem lehet azt a tudomány és technológia állása szempontjából is elégséges szinten garantálni, hogy az ilyen nagyon laza hozzáférési intézkedések mellett kezelt személyes adatok ne kerüljenek előbb-utóbb nyilvánosságra. Az erősebb biztonsági intézkedések hiányának következményeire példa a jelen ügyben bekövetkezett adatvédelmi incidens is.

Csupán a fájlokhoz való hozzáférésnapló elemzése kapcsán Ügyfél sem tudta azt megállapítani, hogy azokhoz illetéktelen külső támadó férhetett-e hozzá, vagy a fájlok nyilvánosságra hozatala belső szivárogtatás eredménye-e.

A Hatóság megítélése szerint amennyiben az Ügyfél a fájlok tárolását valamilyen belső, megfelelő titkosítással és visszakövethető hozzáféréskontrollal (pl. jelszavas védelem melletti jogosultságkezelés és belső naplózás) ellátott rendszerben (pl. dedikált szerver) kezelte volna, úgy a bejelentés tárgyát képező adatvédelmi incidens is sokkal kisebb valószínűséggel következett volna be, valamint bekövetkezésének körülményeit is könnyebb lett volna rekonstruálni.

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

2. A bekövetkezett adatvédelmi incidens kezelése kapcsán megtett intézkedések

Az általános adatvédelmi rendelet 4. cikk 12. pontja alapján adatvédelmi incidensnek minősül a biztonság sérülése, amely a kezelt személyes adatok jogosulatlan közlését, vagy azokhoz való jogosulatlan hozzáférést eredményezi. A fogalom szempontjából így a biztonsági eseménnyel való kapcsolat kulcselemnek tekinthető. Egy személyes adatokat érintő esemény csak abban az esetben minősül adatvédelmi incidensek, ha az valamilyen biztonsági sérüléssel hozható összefüggésbe, ez a kiváltó oka és a kettő között okozati összefüggés áll fent. A biztonság sérülése fakadhat a személyes adatok védelme érdekében alkalmazott biztonsági intézkedések hiányos, nem megfelelő, esetleg elavult voltából vagy épp azok teljes hiányából.

Az adott ügyben a biztonsági sérülés abból adódott, hogy Ügyfél nem alkalmazott megfelelő technikai és szervezési intézkedéseket a pártszimpatizánsok adataival kapcsolatban azok

bizalmasságának megőrzése érdekében (lást a határozat III/1. pontjában foglaltakat). A megfelelő biztonsági intézkedések hiányában ezért a szimpatizánsok és tagok személyes adatait is tartalmazó táblázatok, Ügyfél által nem rekonstruálható és visszakövethető módon kikerültek a kezeléséből és nyilvánosságra hoztak ismeretlenek az interneten.

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

Az incidensben érintett szenzitív és pontos, különleges személyes adatnak minősülő adatkört magában foglaló adatkezelés során, a biztonsági intézkedések sérülése miatt bekövetkező adatvédelmi incidens magas kockázatúnak minősül. Ennek oka, hogy a politikai tevékenységre vonatkozó adatok nyilvánosságra kerülése után az adatkezelő ráhatása azok sorsára teljesen kikerül az ellenőrzése alól. Az adatok kezelésének további bizalmas jellegét nem lehetséges teljes mértékben a továbbiakban garantálni.

Ügyfél az adatok kezelése alóli kikerülése miatt, azok további sorsára vonatkozó, a kockázatokat teljesen elimináló intézkedéseket nem tud tenni, az adatok – adott esetben jogellenes – továbbkezelésével járó kockázatokat már nem tudja teljesen csökkenteni. A fájlmegosztó oldal (jelen ügyben: https://ufile.io) utólagos felhívása az adatok törlésére csökkenti viszont a kockázatokat, amelyet Ügyfél az incidenskezelés során meg is tett.

A Hatóság továbbá az adatvédelmi incidens által jelentett kockázatokat tovább növelő tényezőnek tekinti, hogy az érintettek különleges adatait tartalmazó táblázatokhoz hozzáférésvédelem (pl. jelszó) nélkül lehetett hozzáférni, csupán egy link birtokában. A megfelelő adatbiztonsági intézkedések alkalmazása csökkentette volna annak a kockázatát, hogy a különleges adatokat harmadik személyek jogosulatlanul ne ismerhessek meg és azok ne kerüljenek nyilvánosságra.

A különleges adatok nyilvánosságra kerülése összevetve az incidens körülményeivel a Hatóság megítélése szerint magas kockázatú adatvédelmi incidenst eredményezett.

A fentiek alapján a Hatóság megítélése szerint az adatvédelmi incidens magas kockázatúnak tekinthető, ezért amennyiben egy ilyen esetről az adatkezelő tudomást szerez, úgy azt be kell jelentenie az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján a felügyeleti hatóságnak.

A Hatóság a fentiekre tekintettel megállapítja, hogy az adatkezelő eleget tett az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján fennálló incidensbejelentési kötelezettségének, így ezzel kapcsolatban jogsértést nem állapított meg.

3. Az elszámoltathatóság elvével kapcsolatos megállapítások

Az általános adatvédelmi rendelet 5. cikk (2) bekezdése határozza meg az „elszámoltathatóság alapelvét”, amely szerint az adatkezelő felelős a rendelet 5. cikk (1) bekezdésében foglalt alapelveinek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

A Hatóság az incidensbejelentés kapcsán megindított hatósági ellenőrzés, majd hatósági eljárás során több alkalommal kísérelte meg nyilatkoztatni arról az Ügyfelet, hogy pontosan milyen intézkedéseket tett az incidens kezelése és az érintettekre jelentett kockázatok csökkentése kapcsán, azonban ezekkel kapcsolatban – Ügyfél értesülése ellenére – nem kapott válaszokat.

Ügyfél tehát a többszöri adatszolgáltatásra való felszólítás ellenére sem igazolta a Hatóság felé, hogy az adatvédelmi incidens kezelése kapcsán pontosan milyen intézkedéseket tett annak érdekében, hogy az általa folytatott adatkezelés megfeleljen a rendelet az ügy szempontjából releváns előírásainak. A Hatóság többek között annak igazolását várta Ügyféltől, hogy az incidensben érintett adatkezelést hogyan alakította át, hogy a továbbiakban a kockázatokkal arányos adatbiztonsági intézkedéseket alkalmazzon a hasonló incidensnek jövőbeli elkerülése érdekében (általános adatvédelmi rendelet 32. cikk), továbbá hogy az érintetteket a magas kockázatú adatvédelmi incidens kapcsán hogyan és milyen tartalommal tájékoztatta (általános adatvédelmi rendelet 34. cikk).

A Hatóság az Ügyfél általi igazolás elmaradása miatt ezért nem tudja azt megállapítani, hogy Ügyfél adatbiztonsági intézkedései a jövőben megfelelnek-e a kockázatokkal arányos szintnek, továbbá, hogy az érintettek incidensről való tájékoztatása kapcsán milyen intézkedéseket tett Ügyfél.

Az adatkezelő neki felróható elzárkózása miatt a Hatóság így szintén nem tudja érdemben ellenőrizni a személyes adatok kezelésével kapcsolatos körülményeket, ez pedig szintén az általános adatvédelmi rendelet által biztosított védelmi szint komoly csökkenéséhez vezet, amely végső soron az érintetteket hozza kiszolgáltatott helyzetbe.

Mivel a Hatóság felé az Ügyfél többszöri felszólítás ellenére sem igazolta a rendelet releváns előírásainak való megfelelés érdekében tett intézkedéseit, ezért megsértette az általános adatvédelmi rendelet 5. cikk (2) bekezdését.

4. Az alkalmazott szankció és indoklása

A Hatóság a tényállás tisztázása során megállapította, hogy Ügyfél megsértette az általános adatvédelmi rendelet

- 32. cikk (1) bekezdését és annak a)-b) pontjait, valamint (2) bekezdését,
- 5. cikk (2) bekezdését.

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

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

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

A bírságkiszabás szükségességének megállapítása során a Hatóság mérlegelte a jogsértések súlyosító, enyhítő és egyéb körülményeit az alábbiak szerint:

Súlyosító körülmények:

- Az adatbiztonsági hiányosságok nagyszámú érintett személyes adatait érintették. [általános adatvédelmi rendelet 83. cikk (2) bekezdés a) pont]

- Az adatbiztonsági hiányosságok olyan adatkezelés kapcsán merültek fel, ahol különleges, politikai véleményre vonatkozó adatokat kezeltek együtt elérhetőségi adatokkal. Ezen adatok jogellenes kezelése negatívan befolyásolhatja az egyén jó hírnevét, magán- és családi életét, hátrányos megkülönböztetés oka vagy indoka lehet az érintettel szemben, továbbá abból személyazonossággal való visszaélés is fakadhat. [általános adatvédelmi rendelet 83. cikk (2) bekezdés g) pont]

- A Hatóság a megállapított adatbiztonsági hiányosságokat rendszerszintű problémának tekinti, mivel az incidens nem egyszeri biztonsági hiányosságra, vagy sérülésre, hanem teljes adatbázisok jogsértő módon való kezelésére vezethető vissza. [általános adatvédelmi rendelet 83. cikk (2) bekezdés a) és d) pontok]

- Az Ügyfél neki felróhatóan nem működött együtt a Hatósággal az ügy kivizsgálása során. A többszöri, Ügyfél által igazoltan átvett adatszolgáltatási felszólítások és eljárási bírság ellenére sem válaszolt a Hatóság tényállás tisztázó végzéseire. A Hatóság így nem tudta teljes körűen ellenőrizni, hogy az érintettekre jelentett kockázatok megfelelően csökkentésre kerülte-e. [általános adatvédelmi rendelet 83. cikk (2) bekezdés f) pont]

- A Hatóság a bírság összegének meghatározása során figyelembe vette, hogy az Ügyfél által elkövetett jogsértés, így az általános adatvédelmi rendelet 5. cikk (2) bekezdésének megsértése a rendelet 83. cikk (5) bekezdése szerint a magasabb maximális összegű bírságkategóriába tartozó jogsértésnek minősül.

Enyhítő körülmények:

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

- A Hatóság figyelembe vette, hogy az Ügyféllel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést. [általános adatvédelmi rendelet 83. cikk (2) bekezdés e) pont]

Egyéb, figyelembe vett körülmények:

- A Hatóság a jogsértésről az Ügyfél az általános adatvédelmi rendelet 33. cikke szerinti incidensbejelentése alapján szerzett tudomást. A Hatóság e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – kifejezetten enyhítő körülményként nem értékelte. [általános adatvédelmi rendelet 83. cikk (2) bekezdés h) pont].

- Az eset körülményei és Ügyfél nyilatkozata alapján Ügyfél döntött a kockázatok szempontjából nem megfelelő adatbiztonságot garantáló technológiai megoldás alkalmazása mellett. A Hatóság azonban nem tudta azt ellenőrizni Ügyfél későbbi együtt nem működése miatt, hogy a technológia kiválasztására milyen megfontolások miatt került sor, illetve Ügyfél ezzel kapcsolatban végzett-e előzetes kockázatelemzést. Az adatbiztonsági jogsértés szándékos vagy gondolatlan jellegét ezért a Hatóság kifejezett súlyosító vagy enyhítő körülményként értékelni nem tudta. Az Ügyfél együtt nem működését viszont a súlyosító körülmények között értékelte. [általános adatvédelmi rendelet 83. cikk (2) bekezdés b) pont]

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

A Hatóság az Infotv. 61. § (2) bekezdés a), b) és c) pontja alapján a határozatnak az Ügyfél azonosító adatainak közzétételével történő nyilvánosságra hozatalát rendelte el, mivel az személyek széles körét érinti, azt a Hatóság közfeladatot ellátó szervezet tevékenységével kapcsolatban hozta, továbbá a különleges adatok érintettsége miatt a nyilvánosságot a jogsértés tárgyi súlya is indokolja.

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.

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, 2022. április 22.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár