Ügyszám: NAIH/2019/2668/2
Előzmény: NAIH/2018/5457/V

Tárgy: hivatalból induló adatvédelmi hatósági eljárás lezárása

H A T Á R O Z A T

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) a Demokratikus Koalíció (székhely: 1132 Budapest, Victor Hugo u. 11-15.) (a továbbiakban: Ügyfél) adatkezelését érintő adatvédelmi incidenssel kapcsolatban 2018. november 21. napján megindított **adatvédelmi hatósági eljárásban**

1) megállapítja, hogy

a) az Ügyfél nem tett eleget az általános adatvédelmi rendelet 33. cikke alapján fennálló incidensbejelentési kötelezettségének,

b) az Ügyfél nem tett eleget az általános adatvédelmi rendelet 34. cikke alapján fennálló érintetti tájékoztatási kötelezettségének sem a bekövetkezett adatvédelmi incidenssel kapcsolatban,

2) utasítja az Ügyfelet, **hogy a jelen határozat véglegessé válásától számított 15 napon belül**

a) **tájékoztassa az érintetteket** a bekövetkezett incidens tényéről és körülményeiről, az érintett személyes adatok köréről és az elhárítás érdekében megtett intézkedésekről,

b) **rögzítse az adatvédelmi incidens** tényét, annak hatásait és az orvoslására tett intézkedéseket az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján vezetett **nyilvántartásában,**

3) az 1) pont szerinti jogsértés miatt **kötelezi az Ügyfelet, hogy a jelen határozat véglegessé válásától számított 30 napon belül fizessen meg**

11.000.000 Ft adatvédelmi bírságot.

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

A 2) pontban *előírt* intézkedések megtételét az Ügyfélnek az intézkedés megtételétől számított 15 napon belül kell írásban – az azt alátámasztó bizonyítékok előterjesztésével együtt – igazolnia a Hatóság felé.

A bírságot a ***Hatóság központosított bevételek beszedése célelszámolási forintszámlája (10032000-01040425-00000000)*** **javára kell megfizetni. Az összeg átutalásakor** a NAIH/2019/2668 BÍRS. számra kell hivatkozni.

Ha az 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 2) pont szerinti kötelezettségek, illetve a bírság és a késedelmi pótlék meg nem fizetése esetén a Hatóság elrendeli a határozat végrehajtását.

Jelen határozattal szemben közigazgatási úton jogorvoslatnak nincs helye, de az a közléstől számított 30 napon belül a Fővárosi Törvényszékhez címzett keresettel közigazgatási perben megtámadható. A keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak. A tárgyalás tartása iránti kérelmet a keresetben jelezni kell. A teljes személyes illetékmentességben nem részesülők számára a bírósági felülvizsgálati eljárás illetéke 30.000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

INDOKOLÁS

I. tényállás, előzmények

A Hatósághoz 2018. augusztus 23-án közérdekű bejelentés érkezett, amely arra hívja fel a figyelmet, hogy az Ügyfél által üzemeltetett http://web.dkp.hu honlaphoz köthető, személyes adatokat tartalmazó felhasználói adatbázis nyilvánosan elérhető az interneten a https://defuse.ca/b/DIOCGRER7ZE1qVeDyVKpg1 címen.[1] Az adatbázis felhasználói e-mail címeket, felhasználói neveket és titkosított formában a belépéshez szükséges jelszavakat tartalmaz. Az adatbázis úgy kerülhetett nyilvánosságra, hogy egy ismeretlen támadó, aki erről egy blogbejegyzésben beszámolt,[2] ahhoz a honlap sérülékenységét kihasználva hozzáfért, majd azt feltöltötte az említett https://defuse.ca/b/DIOCGRER7ZE1qVeDyVKpg1 címre.

A Hatóság a közérdekű bejelentés alapján 2018. szeptember 14-én hatósági ellenőrzést indított annak ellenőrzése érdekében, hogy az Ügyfél maradéktalanul eleget tett-e az általános adatvédelmi rendelet 33-34. cikkében foglalt kötelezettségeinek, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) hatályos előírásainak, amiről az Ügyfelet értesítette. Az értesítést az Ügyfél a tértivevény tanúsága alapján 2018. szeptember 19-én vette kézhez. A Hatóság NAIH/2018/5457/3/V., majd később NAIH/2018/5457/5/V. és NAIH/2018/5457/8/V. számú végzéseiben a tényállás tisztázása céljából nyilatkozattételre hívta fel az Ügyfelet, amelyre az mindhárom alkalommal határidőben válaszolt. Az ellenőrzés során tapasztaltak alapján az ügyben az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerinti különleges adatok (politikai véleményre, pártállásra vonatkozó adatok) érintettsége miatti valószínű magas kockázat, illetve a rendelet 33. cikk (1) bekezdésének megfelelő bejelentési kötelezettség elmulasztása miatt – az Infotv. 60. § (1) bekezdésére tekintettel –, a Hatóság 2018. november 21-én adatvédelmi hatósági eljárást indított, amelyről az Ügyfelet értesítette. Az eljárás során a tényállás további tisztázása érdekében a Hatóság a NAIH/2018/5754/11/V számú végzésével az Ügyfél újabb megkereséséről és nyilatkoztatásáról döntött, amely végzésre az Ügyfél az előírt határidőben válaszolt. A Hatóság később kiterjesztette az adatvédelmi hatósági eljárás tárgyát az általános adatvédelmi rendelet 33-34. cikkei megsértésének vizsgálatára is, amelyről az Ügyfelet 2019. március 8-án NAIH/2019/2668 ügyiratszámon értesítette.

---

[1] Az adatbázist a Hatóság lementette, majd az adatbázist tartalmazó „DK adatbázis.xlsx" nevű és kiterjesztésű fájlról generált hitelesítő kulccsal együtt azt kiírta egy CD lemezre NAIH/2018/5457/7/V. iktatószám alatt. Erről külön feljegyzés is készült.

[2] A támadó által ismertetett módszerek leírása elérhető: https://h4x0rd0t.wordpress.com/2018/08/22/dkpwn-elkurtuk-nem-kicsit-nagyon/. A támadó a cikket 2018. augusztus 22-én publikálta. A Hatóság a cikket az ügy 2018/5457/2/V. iktatószámú ügyiratának (információbiztonsági szakértői vélemény) mellékleteként mentette le és kezeli.

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

A támadást végrehajtó hacker honlapján (a fent hivatkozott blogbejegyzésben) elérhető információk alapján a támadás egy a honlap beállításaiból adódó adatbázis-sérülékenység miatt valósulhatott meg, amely abban állt, hogy a támadó képes volt a weboldalon át kapcsolatba lépni közvetlenül az adatbázissal, így annak utasításokat adhatott.

Az Ügyfél szerint a sérülékenységet, amelyen keresztül hozzá tudott férni a támadó a tesztadatbázishoz, a honlapot érintő egyik átirányítás hibája okozta. Ennek a hibának a lényege, hogy az Ügyfél által a honlap üzemeltetésére is használt virtuális hosting[3] szolgáltatás (röviden: vhost) elvárt működése, hogy a dkp.hu (fő)domaint átirányítja a web.dkp.hu aldomainre. Itt a kiszolgáló szerver redirect (átirányítás) parancsában az incidens bekövetkezésének idején nem volt megfelelően szabályozva, hogy a dkp.hu domain mögé írt egyéb útvonalak is átirányításra kerüljenek. A dkp.hu (fő)domain mögé – akár manuálisan – írt egyéb útvonalakra mutató kérések alapértelmezetten minden esetben a vhost könyvtárra mutattak. A kiszolgáló az ilyen egyéb kérések teljesítésénél azt vette alapértelmezettnek, ami a listában az első helyen szerepel. A listában pedig első helyen egy 2013-as tesztrendszer fájljai voltak, benne a felhasználói adatokkal. Amennyiben tehát egy támadó a dkp.hu (fő)domain mögé egyéb útvonalra mutató kérést írt be, úgy a hibás beállításnak köszönhetően hozzá tudott férni a nyilvánosságra hozott felhasználói adatbázist is tartalmazó fájlokhoz.

Az Ügyfél nem tudta azt pontosan meghatározni, hogy maga a sérülékenység mióta állt fent a rendszerében. A vhost konfigurációs fájljai 2018. augusztus 23-án (azt követően, hogy az Ügyfél saját maga által is elismerten értesült az incidensről) 09:15-kor kerültek oly módon módosításra, hogy a fájlokhoz már ne lehessen kívülről hozzáférni. Az Ügyfél nyilatkozata szerint a hiba ezen javítását követően a szakemberei segítségével átvizsgálta a rendszert, további olyan jellegű hibát, amely a hacker blogbejegyzésében is ismertetésre került, már nem lehetett a javítást követően generálni.

A támadónak a sérülékenység miatt sikerült kinyernie az adatbázisszerveren található, a tesztrendszerben tárolt összes felhasználó adatát. A támadó az általa használt parancsot is publikálta. A publikált parancs segítségével, egy informatikai szempontból alacsonyan képzett ember számára is lehetőség nyílt így arra, hogy kihasználhassa ezt a hibát, és az adatbázist megszerezhesse.

A nyilvánosságra került adatbázis tartalmazza a regisztrált felhasználók teljes nevét, a regisztráció során megadott felhasználónevét, e-mail címét, illetve – titkosítva – a belépéshez szükséges jelszót.

A jelszavak az adatbázis szerveren MD5 elnevezésű algoritmussal voltak elkódolva (titkosítva), amely titkosítás azonban nagyon gyenge védelmet jelent, mivel percek alatt vissza lehet fejteni 1-1 jelszót, akár az interneten bárki számára elérhető, ingyenes weboldalakat és alkalmazásokat használva, vagy akár erre megírt célprogram segítségével. A Hatóság IT biztonsági szakértője próbaképpen megkísérelt visszafejteni néhány jelszót a hacker által nyilvánosságra hozott és a

[3] A virtuális host (röviden: vhost) szolgáltatás használata képessé tesz egy egyedülálló szervergépet arra, hogy akár több domain-t is kiszolgálni tudó webszerver legyen.

Hatóság által lementett adatbázisból, és kivétel nélkül sikerrel járt. Ezt a Hatóság 2018/5457/2/V. számú IT biztonsági szakértői véleményben dokumentálta.

Az adatbázis összesen 11 614 darab rekordot tartalmazott. Ezek közül vannak olyan sorok, ahol nem mindegyik előbbiekben felsorolt adat volt megtalálható, de a sorok többségében szerepel valamilyen adat ezen adattípusok közül. Az adatok között megtalálhatóak olyan rekordok is, amelyekből a rendszergazdai felhasználóra lehet következtetni.

Az Ügyfél nyilatkozata szerint a nyilvánosságra került adatbázis nem a web.dkp.hu honlapon aktuálisan regisztrált felhasználók adatait, hanem egy korábbi, 2013 év végén készült tesztrendszer adatait tartalmazza, amelyet egy belső nyilvántartó rendszer készítése során, teszt célból hoztak létre. Ez a nyilvántartó rendszer azonban sohasem készült el teljesen, így végleg tesztfázisban maradt. Ezt a tesztadatbázist ugyanakkor véletlenszerűen kiválasztott, jogszerűen gyűjtött valós, természetes személyekhez tartozó adatokkal töltötték fel, és az nem fiktív, kitalált, véletlenszerűen generált adatokat tartalmaz.

Az Ügyfél tájékoztatta arról is a Hatóságot, hogy a bevezetésre végül nem került tesztrendszer célja az lett volna, hogy a felhasználóinak a pártban lévő tagsági viszonyukról és azzal kapcsolatos információkról adott volna tájékoztatást, mint tagdíjegyenlegek, befizetések stb. A tesztrendszerben a felhasználói fiókok számának maximalizálása érdekében a teszteléséhez felhasznált adatok az addig jogszerűen, így (jellemzően 2012-ben zajlott) aláírásgyűjtéseken szerzett kontaktinformációkból lettek véletlenszerűen kiválasztva.

A Hatóság kérésére továbbá az Ügyfél elvégzett a nyilvánosságra került adatbázisban egy ellenőrzést. Ennek alapján szűkítette az adatok körét és kivette a táblázatból azokat a sorokat, ahol az e-mail cím üres volt / ékezetes betűt tartalmazott / nem tartalmazott pontot / duplikált volt (vagyis kétszer szerepelt az adatbázisban). Kivette továbbá azokat a sorokat ahol a név mező üres volt. Ezek alapján összesen 6987 darab érintett személyes adatai szerepelnek az adatbázisban.

A Hatóság kérésére az Ügyfél a táblázatban azt is megjelölte, hogy melyek azok a személyek, akik bármikor a múltban vagy jelenleg a pártban
- bármilyen tisztséget töltöttek be,
- a párt országgyűlési képviselői,
- a párt önkormányzati képviselői,
- országgyűlési vagy önkormányzati választások során a párt jelöltjeként indultak, vagy
- bármilyen más okból a párttal való kapcsolatuk miatt nevük közérdekből nyilvános.

A fenti kritériumoknak megfelelően összesen 505 esetben minősültek az Ügyfél szerint az adatbázisban szereplő személyek nevei körérdekből nyilvánosnak.

A tesztrendszer adatbázisában összesen három kategóriába lehet az adatok forrása alapján az érintetteket osztani:
- tagok,
- regisztrált támogatók,
- szimpatizánsok.

A tagi és regisztrált támogatói adatbázisba két féle módon kerülnek rögzítésre a személyek: interneten keresztül vagy papír alapon. Az első esetben a regisztracio.dkp.hu weboldalon az adott érintett kitölti a kért adatokat és nyilatkozik arról, hogy ő a továbbiakban mint tag vagy mint regisztrált támogató szeretne belépni a pártba. A regisztrációt kitöltő személyből így lesz tag-, illetve regisztrált támogató-jelölt. Ezek után az online regisztráció megküldése után az informatikai

rendszer automatikusan besorolja az érintettet, így a lakcím szerinti választókerületi elnökhöz kerül az adott személy regisztrációs kérelme. A választókerületi elnök ezután taggyűlésen terjeszti elő az új tag felvételét. Végül a választókerületi elnök jelzi az adatkezelői csoport számára az új tag felvételét, akik őt rögzítik az adatbázisba.

Papír alapon úgy kerültek tagként vagy támogatóként rögzítésre egyes személyek, hogy a tag-, illetve a regisztrált támogató-jelölt papír alapon, lezárt borítékban küldte meg az adataival kitöltött jelentkezési lapot a pártnak. Ezek után az adatkezelői csoport dolgozza fel a megadott adatokat és rögzíti a regisztrációs kérelmet. A kérelem az informatikai rendszer automatikusan besorolása után a lakcím szerinti választókerületi elnökhöz kerül. A kérelem feldolgozása ezek után ugyanúgy történik, mint az internetes felületen.

Mindkét esetben a regisztrációs folyamat lezárulása után az érintett egy üdvözlő e-mailt kap. Ebben az e-mailben található a www.dkp.hu-n lévő felületre a belépéshez szükséges, a rendszer által automatikusan generált felhasználónév. A belépéshez szükséges jelszót a tag / regisztrált támogató az első belépés után adja meg. A szimpatizánsok nem tudnak belépni a honlap online felületére.

Az Ügyfél tájékoztatása szerint a szimpatizánsi adatbázisba a következő három módon lettek rögzítve a személyek:

- alairas.dkp.hu oldalon az aláírásgyűjtések közül valamelyiket online felületen történő aláírás az adatok megadásával,
- papír alapú aláírásgyűjtő íven az adatok megadásával és aláírásával az adatkezelésbe való beleegyezés révén, és
- a Robocall, telefonos felmérés során az adott személy által a megfelelő nyomógomb megnyomásával.

Az adatok önkéntes megadása után kizárólag az adatkezelői csoport rögzíthet szimpatizánsokat az adatbázisba.

A tesztadatbázisba így a párt fenti módszerrel, a tagoktól, regisztrált támogatóktól és szimpatizánsoktól gyűjtött adatai kerültek be próbaképpen. Ezek közül sem az összes, hanem véletlenszerűen kiválasztva azok egy része. Mivel a rendszer sosem élesedett, ezért a tesztfelhasználóknak sosem volt lehetőségük a rendszerbe belépni.

Az incidens (az adatok illetéktelenek általi elérésének, illetve elérhetőségének lehetősége) konkrét időpontja nem ismert. Az incidensre vonatkozó blogbejegyzés szerint a sérülékenység észlelése a blogot vezető hacker által már 2018. áprilisában megtörtént, és erről már akkor értesítette is az Ügyfelet. Erre vonatkozóan azonban a blogbejegyzésen kívül nem állnak rendelkezésre más egyértelmű és hitelt érdemlő bizonyítékok. Az Ügyfél azt nyilatkozta, hogy az incidensről az első jelzést 2018. augusztus 22-én este kapta meg e-mail üzenetben, és ebből értesült a támadás tényéről. Az üzenet küldőjét az Ügyfél egyebekben nem nevezte meg. Az Ügyfél az incidensről az érintetteket nem tájékoztatta. Ennek indokaként azt jelölte meg, hogy az érintett adatok régiek, elavultak, így a párt jelenlegi szimpatizánsainak, tagjainak a párt által tárolt és kezelt adatait szerinte nem érintette az incidens. Az Ügyfél az incidenst ugyanezen megfontolás miatt nem vette az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján nyilvántartásba, arra hivatkozva, hogy az eset nem érintette az élő adatbázisát.

II. Alkalmazott jogszabályi rendelkezések

Az általános adatvédelmi rendelet 2. cikk (1) bekezdése alapján a bejelentett incidenssel érintett adatkezelésre az általános adatvédelmi rendeletet kell alkalmazni. Az általános adatvédelmi rendelet 99. cikk (2) bekezdése alapján a rendelet 2018. május 25-étől alkalmazandó.

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

Az általános adatvédelmi rendelet 33. cikk (1) 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 33. cikk (5) bekezdése előírja, hogy az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket olyan módon, hogy az lehetővé teszi a felügyeleti hatóságnak, hogy ellenőrizze a 33. cikk követelményeinek való megfelelést.

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

Az általános adatvédelmi rendelet 9. cikk (1) bekezdése alapján a politikai véleményre vonatkozó személyes adat a személyes adatok különleges kategóriájába tartozó, s mint ilyen, magasabb szintű védelmet igénylő személyes adat (különleges személyes adat), figyelemmel a rendelet (53) preambulumbekezdésére is figyelemmel.

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

Az Infotv. 60. § (1) bekezdése alapján a személyes adatok védelméhez való jog érvényesülése érdekében a Hatóság hivatalból adatvédelmi hatósági eljárást indíthat. Az adatvédelmi hatósági eljárásra az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) szabályait kell alkalmazni az Infotv.-ben meghatározott kiegészítésekkel és az általános adatvédelmi rendelet szerinti eltérésekkel.

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

Az Infotv. 61. § (1) bekezdés a) pontja szerint az adatvédelmi hatósági eljárásban hozott határozatában a Hatóság az Infotv. 2. § (2) bekezdésében meghatározott adatkezelési műveletekkel összefüggésben az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja. Az általános adatvédelmi rendelet 58. cikk (2) bekezdés b) pontja szerint a felügyeleti hatóság elmarasztalja az adatkezelőt vagy az adatfeldolgozót, ha

adatkezelési tevékenysége megsértette e rendelet rendelkezéseit, illetve ugyanezen bekezdés d) pontja értelmében a felügyeleti hatóság korrekciós hatáskörében eljárva utasítja az adatkezelőt, hogy adatkezelési műveleteit – adott esetben meghatározott módon és meghatározott időn belül – hozza összhangba e rendelet rendelkezéseivel.

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

A közigazgatási bírság kiszabására vonatkozó feltételeket az általános adatvédelmi rendelet 83. cikke tartalmazza. Az általános adatvédelmi rendelet 32–34. cikkének megsértése esetén a kiszabható bíróság felső határa az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja alapján a kiszabható legmagasabb bírság 10 000 000 eurónak (EUR) megfelelő összeg.

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

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

III. Döntés

a) Az adatvédelmi incidens bejelentésének elmulasztása

Az adatvédelmi incidensről az Ügyfél legkésőbb 2018. augusztus 22-én este szerzett tudomást. Az incidens bejelentésére a mai napig annak ellenére nem került sor, hogy a Hatóság megindította hatósági ellenőrzését, majd a jelen hatósági eljárást az Ügyféllel szemben.

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 Ügyfél a bejelentés elmulasztása indokaként felhozott azon indokolása, miszerint az adatvédelmi incidens nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, nem állja meg a helyét. Az, hogy az adatbázis adott esetben régi, elavult adatokat tartalmazott, hogy csak egy úgynevezett tesztadatbázis lett volna, illetve hogy az Ügyfél a jelenlegi, élő adatbázisait nem érintette, azokhoz semmilyen belépési lehetőség nem állt fenn, nem elfogadható.

Az ügyben az érintettekre jelentett kockázat értékelése szempontjából nincs annak jelentősége, hogy az adatok mikor keletkeztek és azokat az Ügyfél milyen célból és milyen rendszer részeként gyűjtötte eredetileg. Az adatkezelő az általa kezelt személyes adatok kezelésére vonatkozó követelményeknek az adatkezelés teljes időszakában köteles eleget tenni. Az pedig, hogy az adott incidenssel érintett adatalanyok esetében a kérdéses – egyébként nem vitatottan valós –

személyes adat esetleg már nem aktuális, önmagában nem jelenti azt, hogy az akár személyes adat jellegét, akár különleges adat jellegét elvesztette volna.

Különösen nem állja meg a helyét ez az ügyféli hivatkozás a személyazonosításra alkalmas adatok (név, e-mail cím, felhasználónév, jelszó) nyilvánosságra kerülése vonatkozásában, amelyek esetén az érintett magánszférájára jelentett kockázat jellemzően magas. Ezen adatok birtokában ugyanis könnyen elkövethető személyazonossággal visszaélés.

Az érintettek jogaira jelentett magas kockázati besorolást továbbá önmagában is megalapozza az, hogy az incidens olyan személyes adatokat érintett, amelyekből az érintett politikai véleményére vonatkozó következtetést lehet levonni. Nincs annak jelentősége az érintettre jelentett kockázat megítélése szempontjából, hogy ez a következtetés az adatbázis alapján nem a legpontosabb, legaktuálisabb, hiszen valamely politikai szervezethez tartozás – még ha esetleg múltbéli is – mindenképpen az adott személy politikai véleményét tükrözi. Ráadásul az adatbázisból – nem függetlenül az alább tárgyalt hiányosságtól – semmilyen módon nem derül ki az adatok nem aktuális vagy nem valós jellege – sőt, az Ügyfél nyilatkozatával megerősítetten az adatok valós személyek valós adatai voltak. Végül a magas kockázati besorolás mellett szóló érv, hogy ezek a különleges adatok az érintettek nagy részénél nem voltak más forrásból kideríthetőek, azok kizárólag jelen incidens kapcsán kerültek nyilvánosságra.

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 Ügyfél nyilatkozatai alapján az adatvédelmi incidenssel érintett rendszerben kezelt személyes adatok a párt tagjaitól, regisztrált támogatóitól és szimpatizánsaitól származtak.

A szimpatizánsok politikai véleménynyilvánítással kapcsolatos aláírásgyűjtéseken, illetve telefonos megkeresések révén kerülhettek be az adatbázisba. Az adatok megadása mindegyik esetben önkéntes volt, az adatkezelés kifejezetten a párt politikai tevékenységéhez kapcsolódott a szimpatizánsi adatbázis gyűjtésével. A szimpatizánsok nem tudtak belépni a párt www.dkp.hu oldalára, esetükben az Ügyfél így nem kezelt felhasználóneveket és jelszavakat.

A párt tagjainak és regisztrált támogatóinak adatait interneten, vagy papír alapon gyűjtötte az Ügyfél, az adatbázisba történő bekerülés előtt pedig azt minden esetben jóvá kellett hagynia a párt illetékes választókerületi elnökének. A regisztrációhoz szükséges adatok ezek után kerültek kiküldésre e-mailben az érintett számára, aki később létre tudta hozni a www.dkp.hu honlapra a belépéshez szükséges felhasználónév és jelszó párost.

A fenti módon és célból gyűjtött személyes adatok kerültek be később a tesztadatbázisba, amelyet az adatvédelmi incidens érintett. A hacker által nyilvánosságra hozott adatok politikai véleményre vonatkozó adatnak minősülnek, mivel az érintett személyek egyértelműen kapcsolatba hozhatóak a párt tevékenységével, azok a párt szimpatizánsai, támogatói és tagjai voltak. Az adatbázisba való bekerülés egy bonyolultabb regisztrációs, kiválasztási folyamat része, amely során az Ügyfélnek közvetlen ráhatása van arra, hogy mely személyek kerülhetnek be az általa üzemeltetett adatbázisba. Az adatbázisban kezelt személyes adatok bekerülése során fontos a politikai

vélemény, a pártpreferencia megléte az érintett részéről. Ezek az adatok ezért kivétel nélkül különleges személyes adatnak minősülnek.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak is alátámasztják, hogy ha olyan személyes adatok kezelése történik, amelyek politikai véleményre utalnak, úgy az alapvetően kockázatosnak minősül.

Végül magas kockázatúnak tekinthető az incidens azért is, mert – az alább ismertetettek szerint – az adatbázisban alkalmazott elavult titkosítási módszerek miatt a felhasználókhoz tartozó, és az átlagos felhasználók körében meglehetősen gyakori szokás szerint nem kizárhatóan más (leginkább online, de akár offline) szolgáltatás igénybevétele során is használt felhasználónév-jelszó párosok is megismerhetővé válhattak.

Erre tekintettel az Ügyfélnek az incidenst a tudomásszerzést követő 72 órán belül be kellett volna jelentenie a Hatóságnak. Mivel ezen kötelezettségének nem tett eleget, megsértette az általános adatvédelmi rendelet 33. cikk (1) bekezdését.

b) Az érintettek tájékoztatásának kötelezettsége és az incidens nyilvántartása

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

Az incidensről való tájékoztatásra a Hatóság megítélése szerint kifejezetten azért is van szükség, mivel az érintett magánszférájára jelentett kockázat a személyazonosításra alkalmas adatok (név, e-mail cím, felhasználónév, jelszó) nyilvánosságra kerülése esetén olyan jellegű (ezen adatok birtokában elkövethető személyazonossággal visszaélés), amelynek kockázatai csak úgy mérsékelhetők eredményesen, ha az érintettek erről tudomással bírnak, és megtehetik az általuk szükségesnek tartott további intézkedéseket. Ezen felül a politikai véleményre vonatkozó személyes adatok érintettsége is jellemzően magas kockázatú adatvédelmi incidenst eredményez, mivel ezek ismerete alapot szolgáltathat hátrányos megkülönböztetésre, de akár az érintett magán- és családi életét is befolyásolhatja, ami miatt szintén indokolt az érintettek tájékoztatása.

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

A Hatóság végül megjegyzi, hogy az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján az adatkezelőknek a kockázati besorolástól függetlenül minden adatvédelmi incidenst nyilván kell tartaniuk. Ebben fel kell tüntetni az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. Az Ügyfél így nem hivatkozott arra jogszerűen, hogy azért nem vette nyilvántartásba az incidenst, mivel az elavult adatokat érintett és szerinte ezért az nem kockázatos.

c) Az adatbiztonsági intézkedésekkel kapcsolatos megállapítások

Az incidens kezelésének, bejelentésének és annak keretében az incidens kockázatának vizsgálatával összefüggésben feltártak alapján a Hatóság megvizsgálta azt is, hogy az Ügyfél mennyiben tett eleget az adatbiztonsági követelményeknek. Ennek keretében viszont elsősorban

az incidens kezelésével közvetlenül összefüggő adatbiztonsági követelmények érvényesülését vizsgálta az incidens által jelentett kockázat megítélése céljából.
Az eljárás tárgyát ugyan nem képezte az Ügyfél általános adatvédelmi rendelet 32. cikkében (az adatkezelés biztonsága) foglaltaknak való megfelelésének vizsgálata, azonban az incidens kockázati besorolása és a bejelentési kötelezettség indokoltságának vizsgálata miatt mindenképpen szükséges volt ezen kérdésekre is kitérni. Jelen ügyben ugyanis az incidens kockázatának értékelése elválaszthatatlanul összefügg bizonyos adatbiztonsági kérdésekkel.

Ezzel kapcsolatban a Hatóság álláspontja, hogy általánosságban adatbiztonsági szempontból kockázatot csökkentő tényező lehet ugyan, hogy az adatok elavultak és már nem tesznek lehetővé semmilyen, az adatkezelő által üzemeltetett élő rendszerbe történő belépést, különösen akkor, ha az adatkezelő megfelelő titkosítást használt azokkal kapcsolatban, ám a jelen esetben nem ez a helyzet.

Jelen ügyben a jelszavak titkosítása ugyanis egy olyan elavult technológiával történt az Ügyfél részéről, amelyet a technika jelen állása szerint már egyszerűen, ingyenesen elérhető eszközökkel is bárki vissza tud fejteni. Az általános adatvédelmi rendelet 32. cikk (1) bekezdésében foglaltak alapján az adatkezelő a tudomány és technológia állásának megfelelő technikai és szervezési intézkedéseket kell, hogy végrehajtson a kockázat mértékének megfelelő adatbiztonság garantálása érdekében. Ide érti a rendelet a 32. cikk (1) bekezdés a) pontja alapján a személyes adatok megfelelő titkosítását is. Amennyiben az alkalmazott titkosítás különösebb szakértelem, idő és költségráfordítás nélkül, bárki által visszafejthetővé válik, úgy az már nem felel meg a tudomány és technológia állásának megfelelő szintnek. Az alkalmazott technológia elavulása értelemszerűen a titkosított adatokra jelentett kockázat növekedésével jár együtt. Ez egy esetleges incidensnél is mindenképpen kockázatnövelő tényező.

A felhasználók szempontjából szinte minden esetben magas kockázatú körülményként kell értékelni a Hatóság megítélése szerint, ha egy rendszerbe történő belépést szolgáló, nem megfelelően, vagy elavultan titkosított felhasználónév és jelszó páros kerül nyilvánosságra. Ennek fő oka, hogy a felhasználók ugyanezeket az adatokat esetleg más (leginkább online, de akár offline) szolgáltatás használata során is használhatják akár a mai napig. A felhasználók jellemzően nem generálnak minden egyes internetes szolgáltatáshoz önálló felhasználónevet és jelszót, hanem nagyon sokszor ugyanazokat (vagy bizonyos változatait) használják.

Az Ügyfél által az adatbiztonság garantálására hozott intézkedések az alkalmazott technológia elavulása miatt ezért az incidensnek az érintettek jogaira és szabadságaira vonatkozó kockázatát is növelték.

A visszafejtett jelszavakból továbbá egyértelműen kiderült, hogy az adott szerver esetében nem volt jelszó komplexitást validáló algoritmus. A Hatóság IT biztonsági munkatársa talált olyan felhasználót, melynek a visszafejtett jelszava csupa kisbetűből állt.[4] Adatbiztonsági szempontból a Hatóság nem tartja megfelelő gyakorlatnak, ha a jelszavakat a felhasználók nem egy előre meghatározott olyan magasabb biztonsági követelményeket felállító szabályrendszer szerint kötelesek kitalálni, amelyet az adott rendszer ki is kényszerít a jelszó megadása során (pl. jelszó kötelező hossza, kötelezően megadandó különleges karakterek stb.). Ennek oka, hogy nem megfelelően erős jelszóvalidálási rendszer esetén a felhasználók jellemzően minél egyszerűbb és rövidebb jelszavakat fognak használni. Az egyszerűbb jelszavakat azonban könnyebben tudja egy külső támadó visszafejteni, vagy kikövetkeztetni. Ezzel kapcsolatban megjegyzi a Hatóság, hogy

[4] Lásd: 2018/5457/2/V. iktatószámú ügyiratban megállapítottak (információbiztonsági szakértői vélemény).

ha ez a jelszógenerálási és erős jelszavakat nem kikényszerítő gyakorlat az Ügyfél szervezetén belül más informatikai rendszerekben sincs szabályozva, akkor ennek felülvizsgálata mielőbb indokolt.

d) Alkalmazott szankció és indokolása

A Hatóság a tényállás tisztázása során megállapította, hogy az Ügyfél megsértette az általános adatvédelmi rendelet 33. cikk (1) és (5) bekezdéseit, valamint a 34. cikk (1) bekezdését. A fentiekre tekintettel a rendelkező részben foglaltak szerint a Hatóság utasította az Ügyfelet az adatvédelmi incidens belső nyilvántartásban történő rögzítésére, továbbá az érintettek tájékoztatására.

A Hatóság hivatalból vizsgálta az általános adatvédelmi rendelet 58. cikk (2) bekezdés i) pontja alapján az adatvédelmi bírság kiszabásának szükségességét a rendelet 83. cikkére tekintettel.

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

Abban a kérdésben, hogy indokolt-e az adatvédelmi bíróság kiszabása, a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése alapján mérlegelte az ügy összes körülményeit. A Hatóság szükségesnek tartja a bírság kiszabását, mivel az Ügyfél nem tett eleget az incidensbejelentési kötelezettségének egy magas kockázatú, különleges adatokat is érintő incidenssel összefüggésben és arról az érintetteket sem tájékoztatta, lényegében teljes egészében mellőzte a vonatkozó jogszabályi követelményekből következő feladatai teljesítését. Erre tekintettel a Hatóság csupán az Infotv. 75/A. §-a szerinti figyelmeztetés alkalmazását nem tartotta megfelelőnek.

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

A Hatóság a bírság kiszabása során figyelembe vette az általános adatvédelmi rendelet 83. cikk (2) bekezdése szerinti szempontokat és a jogsértés jellegét (adatvédelmi incidens kezelésével kapcsolatos kötelezettség elmulasztása).

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

Súlyosító körülmények:

- Az adatvédelmi incidens kifejezetten magas kockázattal járt: politikai véleményre vonatkozó, különleges személyes adatokat érintett, nagy számú érintettre vonatkozott, az érintettek egyéni azonosítását is lehetővé tevő, rájuk nézve további incidensek kockázatát hordozó adatok váltak megismerhetővé.
- Az Ügyfél tudomással bírt az incidensről, az érintett adatok különleges személyes adat jellege nyilvánvaló, mégsem tette meg a Hatóság részére a bejelentéssel, valamint az érintettek tájékoztatásával kapcsolatos intézkedéseket, így magatartása kifejezetten magas fokon felróható.
- Az elavult titkosítási technológia az incidensnek az érintettek jogaira és szabadságaira nézve fennálló kockázatát kifejezetten megnövelte.
- Az incidenssel érintettek viszonylag magas száma (összesen több mint hatezer érintett).

Enyhítő körülmények:

- Az adatkezelő által a kockázat enyhítésére tett intézkedések: Az Ügyfél az incidensről való tudomásszerzést követően azonnal intézkedéseket tett az incidens kiváltó okának megszüntetése érdekében.

A Hatóság azt a tényt, hogy az eljárás során az Ügyfél a Hatóság adatközlésre felhívó végzéseinek határidőben eleget tett – figyelemmel arra, hogy e körben az Ügyfél magatartása nem ment túl a jogszabályi kötelezettségei teljesítésén – önmagában enyhítő körülményként nem értékelte.

A bírság kiszabása során a Hatóság végül figyelembe vette, hogy az Ügyfélnek 2017 évi beszámolója szerint 269.361.000 HUF bevétele volt. Az Ügyfél 2018 évi költségvetése szerint 415.000.000 HUF bevételt irányzott előre. A jogsértés súlyára és az Ügyfél gazdálkodási adataira tekintettel a kiszabott bírság mértéke ezért a Hatóság megítélése szerint arányosnak tekinthető.

IV. Egyéb kérdések

Az Infotv. 38. § (2) és (2a) bekezdése szerint a Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése. Az általános adatvédelmi rendeletben a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében az általános adatvédelmi rendeletben és az Infotv.-ben meghatározottak szerint a Hatóság gyakorolja. A Hatóság illetékessége az ország egész területére kiterjed.

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

* * *

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

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

A keresetlevél benyújtásának idejét és helyét a Kp. 39. § (1) bekezdése határozza meg. A tárgyalás tartása iránti kérelem lehetőségéről szóló tájékoztatás a Kp. 77. § (1)-(2) bekezdésén alapul. A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény

(továbbiakban: Itv.) 44/A. § (1) bekezdése határozza meg. Az illeték előzetes megfizetése alól az Itv. 59. § (1) bekezdése és 62. § (1) bekezdés h) pontja mentesíti az eljárást kezdeményező felet.

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

Budapest, 2019. március 21.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár