Ügyszám:
NAIH/3974
-1/2021.
Előzmény
ügyszám:
NAIH/2020
/789/V.:
Ügyintéző: […]

Tárgy: hivatalból induló adatvédelmi hatósági eljárás, elmarasztalás

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) a […] ([…]) (a továbbiakban: Adatkezelő) által 2018. november 16. napján bejelentett adatvédelmi incidenssel kapcsolatban indított hatósági ellenőrzést a mai napon lezárja, egyben az ellenőrzés során feltárt körülmények miatt hivatalból megindított **adatvédelmi hatósági eljárásban meghozta a következő**

határozatot.

A Hatóság

1. **megállapítja**, hogy az Adatkezelő informatikai eszközei beállításainak vonatkozásában nem tett eleget a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendelet (a továbbiakban: általános adatvédelmi rendelet) 32. cikk (1) bekezdés b) pontjában foglalt kötelezettségének, és

2. az 1. pontban foglaltak miatt **elmarasztalja** az Adatkezelőt.

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

A Hatóság az adatvédelmi incidenssel kapcsolatban - az általános adatvédelmi rendelet 33-34. cikkében foglalt kötelezettségek tárgyában - 2018. november 28. napján hatósági ellenőrzés megindításáról döntött, egyben a bejelentésben szereplő információk pontosítása, kiegészítése végett három alkalommal tényállás tisztázó végzést küldött az adatkezelő részére, amelyekre az határidőben válaszolt.

Az eredeti bejelentésből, valamint a tényállás tisztázó végzésekben feltett kérdésekre adott válaszokból kiderül, hogy az adatkezelő egy munkavállalója 2018. november 2. napján bizonyítékot is tartalmazó, komolyan vehető megkeresést kapott egy etikus hackertől, melyből az adatkezelő adatbázisának feltörésére lehetett következtetni. Tekintettel arra, hogy kizárólag a megkeresés és néhány

bizonyítékként csatolt adat állt rendelkezésre, az adatkezelő meg kívánt győződni arról, hogy valóban jogosulatlan belépés történt a rendszerbe, és nem más forrásból szerezte meg a megkereső az adatokat.

Ezért az adatkezelő még aznap vizsgálatot indított, majd 2018. november 3. és 4. napján további adatszivárgás lokalizálást kíséreltek meg a kollégái. Ennek eredményeképpen sikerült azonosítani az adatbázist, ahonnan az adatok vélhetően származtak. 2018. november 5-7. napjai között külsős szakértőt bízott meg egy sérülékenységi vizsgálat elvégzésével, majd 2018. november 9. napján […] sérülékenység vizsgálatot kezdeményezett, melyről az előzetes jelentést 2018. november 13. napján vette kézhez, a végleges jelentés 2018. december 1. napján került átadásra.

A vizsgálat során sikerült azonosítani, hogy az adatszerzés a […] weboldalon keresztül […] módszerrel történt, valamint a szerzett információk alapján egyértelművé vált, hogy a rendszerbe a megkereső valóban jogosulatlanul lépett be.

Az érintett adatbázisok különböző operatív alkalmazásokhoz kapcsolódnak, többek között dolgozók (pl. név, e-mail cím, felhasználói név, kódolt jelszó), szponzori együttműködésre jelentkező atléták (pl. név, magasság, születési adat, súly), […] nyertesek (e-mail cím, név, cím), honlapon érdeklődők (levél szövege, e-mail cím, város, telefonszám, név) vagy boltos állásra jelentkezők adatait (név, e-mail, telefon) tartalmazzák, összesen kb. 80 érintettje lehet az incidensnek. Az adatvédelmi incidens érintettjei között több, más tagállamban (Lengyelország – 10 fő, Franciaország – 8 fő, Spanyolország – 3 fő, Németország – 2 fő, Portugália – 1 fő, Dánia - 1 fő) tartózkodó természetes személy is van.

A naplózási adatokból az látszik, hogy a megkereső csak egy-két adatsort hívott le 17 különböző adattáblából, kvázi bizonyítékként arra, hogy valóban sérülékenységet fedezett fel az informatikai rendszer tekintetében. A megkereső nem zsarolta, vagy fenyegette az adatkezelőt, az adatokat nem hozta nyilvánosságra, és adattovábbításról sincs tudomása az adatkezelőnek, a megkereső az adatkezelő informatikai rendszerének sérülékenységét vizsgálta egy jövőbeni együttműködés reményében.

Az adatkezelő az incidens bekövetkezte előtt adatvédelmi tisztviselőt nevezett ki, valamint Incidenskezelési Szabályzatot is fogadott el, ennek megfelelően az incidenskezelési folyamatban az IT Osztály, az adatvédelmi tisztviselő és a felsővezetés is részt vett. A megtámadott területek tűzfallal, határvédelemmel voltak ellátva, csak meghatározott IP címekről volt lehetséges az adatbázisokhoz történő direkt hozzáférés, és 3 havonta történő jelszó-módosítási kötelezettség is érvényben volt.

Az incidensről való tudomásszerzést követően az adatkezelő a webszolgáltatótól bekért naplózási adatok elemzése alapján inaktiválta azokat a funkciókat, melyeken keresztül betörést kíséreltek meg. A betörés ellen új technikai módszert keresett, és alkalmaz: […] védelem által ([…]) a betöréssel érintett oldalak, valamint a weboldal betöréssel nem érintett felületeinek mindegyike védelmet élvez már. A belsős felhasználók (dolgozók) hitelesítése a […] saját szerverein történik, ún. […] rendszer keretében, a további jelszavak esetében pedig […] kódolást használ az adatkezelő. Ezen túlmenően az adatkezelő a megkereső részére kiküldött egy, a lehívott adatsorok haladéktalan törlésére vonatkozó felszólítást. Az adatkezelő az incidens óta eltelt időben panaszt egyetlen érintettől sem kapott, az adatokkal való visszaélésről pedig szintén nincs tudomása.

A Hatóság az ellenőrzést lezárta, és mivel a hatáskörébe tartozó jogsértést tapasztalt, megindította hatósági eljárását, amelyben a jelen határozatot hozta.

II. Alkalmazott jogszabályi rendelkezések

Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 99. §-a alapján a hatóság – a hatáskörének keretei között – ellenőrzi a jogszabályban foglalt rendelkezések betartását, valamint a végrehajtható döntésben foglaltak teljesítését.

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

Az 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.

A hatósági ellenőrzés lefolytatására az Ákr. 7. § (1) bekezdése és 98. §-a alapján a hatósági eljárásra vonatkozó rendelkezéseket kell alkalmazni az Ákr. VI. fejezetében írt eltérésekkel. Az Ákr. 100. § (1) bekezdése alapján a hatósági ellenőrzés hivatalból indul meg, azt a hatóság a hivatalbóli eljárás szabályai szerint folytatja le.

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. 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 e törvényben meghatározottak szerint a Hatóság gyakorolja.

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

Az Ákr. 104. § (1) bekezdés a) pontja szerint a Hatóság az illetékességi területén hivatalból megindítja az eljárást, ha az eljárás megindítására okot adó körülmény jut a tudomására; ugyanezen bekezdés (3) bekezdése alapján a hivatalbóli eljárás az első eljárási cselekmény elvégzésének napján kezdődik, megindításáról az ismert ügyfél értesítése mellőzhető, ha az eljárás megindítása után a hatóság nyolc napon belül dönt.

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

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 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.

III. Döntés

A feltárt tényállás alapján a bekövetkezett adatvédelmi incidenssel összefüggésben a Hatóság az alábbi döntésre jutott.

Az adatkezelés biztonságára vonatkozóan az általános adatvédelmi rendelet 32. cikke határoz meg általános követelményeket. Ez alapján, az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania annak érdekében, hogy a kockázat mértékének megfelelő adatbiztonságot garantáljon. Egy konkrét adatkezelésre vonatkozóan tehát az adatkezelő feladata – figyelembe véve a tudomány és technológia állását, a megvalósítás költségeit, illetve az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett kockázatot – meghatározni, hogy milyen intézkedések szükségesek az adatok biztonságának garantálásához. Ez következik az általános adatvédelmi rendelet 5. cikk (1) bekezdés f) pontjában rögzített elvből is, mely előírja, hogy az adatkezelést olyan módon kell végezni, hogy biztosítva legyen a személyes adatok megfelelő biztonsága, ideértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.

A feltárt tényállás alapján a Hatóság megállapította, hogy az Adatkezelő nem tett eleget az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontjában foglalt, a kockázat mértékének megfelelő szintű adatbiztonság garantálását célzó, *megfelelő technikai és szervezési intézkedések végrehajtására vonatkozó kötelezettségének,* melynek eredményeképpen a támadó hozzáférhetett az adatkezelő különböző operatív alkalmazásokhoz kapcsoló adatbázisaihoz, illetve az azokban tárolt személyes adatokhoz.

Tekintettel azonban arra, hogy
a) a megkereső nem zsarolta, vagy fenyegette az adatkezelőt, az adatokat nem hozta nyilvánosságra, és adattovábbításról sincs tudomása az adatkezelőnek, a megkereső csupán az adatkezelő informatikai rendszerének sérülékenységét vizsgálta egy jövőbeni együttműködés reményében;
b) az adatkezelő az incidensre a tudomására jutását követően gyorsan, és a megfelelő intézkedésekkel reagált;
c) a tényállás tisztázása során az Adatkezelő bemutatta, hogy az incidensről való tudomásszerzést követően milyen intézkedéseket tett a hasonló jellegű támadások elleni védelem megerősítése, illetve a kezelt személyes adatok biztonságának garantálása érdekében, és ezeket az intézkedéseket a Hatóság megfelelőnek találta;
a Hatóság megelégszik a jogsértés megállapításával és az adatkezelő elmarasztalásával.

A fentiek alapján a Hatóság a rendelkező részben foglaltak szerint döntött.

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. § (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.

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, 2021. április ’ ’

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár