Ügyszám: NAIH-5446-9/2024
NAIH-2186/2024
Ügyintéző:

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**) előtt **[…]Ügyvédi Iroda** […] által képviselt […] (a továbbiakban: Ügyfél) által 2024. január 24. napján e-papíron megtett szakaszos incidens bejelentésével kapcsolatban NAIH-2186/2024 számon indult hatósági ellenőrzésben, majd NAIH-5446/2024 szám alatt folyamatban lévő hivatalból indult adatvédelmi hatósági eljárásban feltárt tényállás alapján

1.) megállapítja, **hogy az Ügyfél**

a) 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) bekezdés d)** pontjában foglalt adatbiztonságra vonatkozó rendelkezést, azáltal, hogy az általa üzemeltetett […] nevű weboldalon a fejlesztői tesztkörnyezet alkalmazását, valamint a webszerver megfelelő konfigurációját elmulasztotta, így a weboldalon személyes adat szivárgás lépett fel, mely adatvédelmi incidenst eredményezett.

2.) Az 1.pont szerinti jogsértés miatt az Ügyfelet – azzal, hogy újabb adatvédelmi jogsértés megállapítása esetén a jogkövetkezmények megállapításakor a jelen jogsértést, mint előzményt fokozott súllyal veszi majd figyelembe –

figyelmeztetésben részesíti.

3.) A Hatóság az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 61. § (2) bekezdés a) pontja alapján hivatalból elrendeli a végleges határozatának az Ügyfél azonosító adatainak közzétételével történő nyilvánosságra hozatalát

a) a Hatóság honlapján, továbbá
b) az Ügyfél honlapjának nyitóoldalán, jól látható és könnyen hozzáférhető helyen, a határozat véglegessé válásától számított 30 napon belül, és ott legyen elérhető legalább 30 napon keresztül.

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[1], 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. Tényállás

Az Ügyfél 2024. január 24-én – meghatalmazott jogi képviselője útján – a Hatósághoz szakaszos incidensbejelentést tett, melyben előadta, hogy az általa üzemeltetett […] honlapon 2024. január 23-án adatvédelmi incidenst észlelt, melynek során a honlap egyes adminisztrátorok számára szánt aloldalai ideiglenesen az internetes keresőmotorok által szemlézhetővé váltak. Ennek következtében az Ügyfél által szervezett felnőttképzésekre jelentkező magánszemélyek adatai kiszivárogtak, ahhoz jogosulatlanul hozzáfértek. Az adatszivárgást egy konfigurációs hiba okozta, amely során egy beépülő bővítmény modul (a továbbiakban: bővítmény) felülírta az éles környezetben használt másik bővítmény konfigurációit. Ez előre nem látható inkompatibilitási problémát eredményezett, melynek következtében a felnőttképzésre jelentkező magánszemélyek személyes adatai az internetes keresőmotorok által listázhatóvá, így bárki által megismerhetővé váltak.

II. Eljárás menete

a) Adatvédelmi incidens bejelentés és hatósági ellenőrzés

A Hatósághoz az Ügyfél meghatalmazott jogi képviselőjétől 2024. január 24-én szakaszosként megjelölt incidens bejelentés érkezett az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján.

Az incidensbejelentésben foglaltak szerint az Ügyfél az általa üzemeltetett […] weboldalon adatvédelmi incidenst észlelt. Az incidens a honlap aloldalait érintette, mely miatt egyes, adminisztrátorok számára elérhető felületet ideiglenesen szemlézhetett a Google indexelője, így az Ügyfél által szervezett felnőttképzésekre jelentkező magánszemélyek adatai szivárogtak ki. Az incidens észlelésének időpontjaként az Ügyfél 2024. január 23 11 óra 50 percét jelölte meg.

Az incidens okaként az Ügyfél szervezeten belüli, rosszhiszeműnek nem minősülő cselekményt jelölt meg. Az Ügyfél előadása szerint az incidenssel érintett személyes adatok száma 10-50 közötti, melyek személyazonossági és elérhetőségi adatok. Az incidensben érintettek száma 10-50 fő, a weboldal felhasználói, illetve a képzésekre feliratkozók. Az Ügyfél az érintetteket 2024. január 23-24. között telefonon és e-mailen is értesítette az incidensről. Az Ügyfél az incidens következményeinek súlyosságát korlátozottnak értékelte.

[1] A közigazgatási per kezdeményezésére a NAIH_K01 elnevezésű űrlap szolgál: NAIH_K01 űrlap (2019.09.16.). Az űrlap az általános nyomtatványkitöltő program (ÁNYK program) alkalmazásával tölthető ki.

Az űrlap az alábbi linkről érhető el: https://www.naih.hu/kozig-hatarozat-birosagi-felulvizsgalata

A Hatóság a bejelentett adatvédelmi incidenssel kapcsolatban NAIH-2186-2/2024 számon hatósági ellenőrzést indított, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy az Ügyfél maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek.

Az Ügyfél a Hatóság felhívására NAIH-2186-3/2024 számú iratában az incidens bejelentést érintő dátumokat pontosította.

Ezt követően NAIH-2186-4/2024 számú iratában az Ügyfél tájékoztatta a Hatóságot arról, hogy az érintettek tájékoztatására az általános adatvédelmi rendelet 34. cikke alapján sor került, 2024. január 23-án telefonos úton, majd 2024. január 25-én e-mail útján. Igazolásul csatolta a 62 érintett részére a tájékoztatás megtörténtét.

A Hatóság kérdésére az Ügyfél akként nyilatkozott, hogy az incidenssel név, e-mail cím, telefonszám, motivációs videó, motivációs levél, publikus közösségi média fiókok elérési útvonalai voltak érintettek. Csatolta az incidens kezelési szabályzatot és az incidens nyilvántartást. Az érintettek számát végül 62 főben jelölte meg. A Hatóság kérdésére akként nyilatkozott, hogy sérülékenység vizsgálat végzésére még nem került sor, az a 2024-es évre egy későbbi időpontban volt betervezve.

Az ügyben az incidens következményeként az Ügyfélnél belső vizsgálat indult, mely megállapította, hogy egy bővítmény telepítésére került sor, mely inkompatibilitási problémákat eredményezett, az éles alkalmazást követően, ugyanis a korábbi bővítmény beállításokat felülírta, így a képzésekre vonatkozó jelentkezési adatok az internetes keresőmotorok által indexálhatóvá, így a nyílt internet felől kereshetővé váltak.

Az incidens bekövetkeztét követően az Ügyfél az adatfeldolgozót értesítette telefonos úton, és az incidens kapcsán részletes kockázatelemzést is végzett. Az ezzel kapcsolatos okiratokat szintén csatolta a Hatóság részére.

A hasonló incidensek megelőzésével kapcsolatos technológiai fejlesztésekre az Ügyfél akként nyilatkozott, hogy a keretrendszer adminisztrációjához kétfaktoros autentikáció bevezetését tervezi, az emelt jogosultsággal rendelkező felhasználók körét felülvizsgálja, továbbá a kiszolgáló környezetet érintően biztonsági funkciókat kíván bevezetni […], létrehozása a konfiguráció változások és tesztelések érdekében, a kiterjedt tesztelések jegyzőkönyvezésre kerülnek.

A kérdésekre történő válaszadással együtt az Ügyfél NAIH-2186-4/2024 számon megtette a teljes incidens bejelentést is.

A Hatóság NAIH-2186-5/2024 számú végzésével további tényállás tisztázást tartott szükségesnek, melyre az Ügyfél NAIH-2186-6/2024 számú iratával válaszolt. Előadta, hogy a weboldalt kiszolgáló környezet […] motorban van felépítve testreszabott sablonokból, valamint a működéshez szükséges pluginok használatával. Az oldal néhol tartalmaz egyedileg kódolt […] megoldásokat is. A kiszolgáló környezet offsite, datacenter hosting környezetben helyezkedik el bérelt […] szerveren. A szerver előtt egy […] tűzfal […] szűrést végez, majd […] irányítja a web forgalmat és végzi az SSL titkosítást. A VPS VLAN szegmentált hálózati környezetben helyezkedik el. A kiszolgálás […] r környezetben történik. A weboldal kiszolgáló motorja […], valamint a működéshez szükséges egyéb rendszerkomponensek.

A Hatóság kérdésére az Ügyfél előadta, a weboldal fejlesztő fejlesztési specifikáció alapján manuális módszerrel ellenőrzi a fejlesztések megfelelőségét a tesztrendszeren, majd automata webszerver és web applikáció sérülékenység és terhelés elemző rendszer […] specifikumait használja biztonsági ellenőrzésre. A weboldal fejlesztő kontrollált körülmények között ad verziót az élesre, majd ott ismételten megtörténik a már éles tesztelés. Éles hiba esetén az eredeti visszaállítási pontra tér vissza, majd kezdi ismét a teszt környezeten a tesztelést.

Az access controll-al kapcsolatban akként nyilatkozott, hogy a tűzfallal elszigetelt tesztkörnyezet védelmét VPN-nel és .htaccess alapú több faktoros azonosítással, valamint beépített jogosultság kezelési rendszerrel védi. Emellett az éles weboldal publikus adatait és a regisztrált felhasználók számára létrehozott aloldalakat határvédelemmel védi. A hozzáféréseket a weboldal jogosultság tekintetében egyedi szintekre felhasználói csoportokra bontva szabályozza, ahol szintén megkövetelt a két faktoros azonosítás. Külön csoportok tartalmazzák a teljes adminisztrátorokat, valamint a funkció adminisztrátorokat. A teljes adminisztrátorokat load balancerek védik. Ezek eléréséhez kliens VPN hozzáférés szükséges.

b) Hatósági eljárás

Tekintettel arra, hogy további vizsgálatot igényelt az, hogy az Ügyfél eljárása során betartotta-e az általános adatvédelmi rendelet **32. cikk** szerinti adatbiztonságra, valamint a **25. cikk** szerinti beépített és alapértelmezett adatvédelemre vonatkozó rendelkezéseket, a Hatóság 2024. április 17-én kelt NAIH-5446-1/2024 számú végzésével hivatalból adatvédelmi hatósági eljárást indított. A végzésben a Hatóság az Ügyfelet további tényállás tisztázásra hívta fel, melynek az Ügyfél NAIH-5446-2/2024 számú válasziratával tett eleget.

Ebben előadta, hogy az […] plugin telepítése okozta a konfigurációs problémát, amely felülírta a korábban használt és jelenleg is élesben használt […] bővítmény konfigurációit. A használatban lévő keretrendszer a […] volt az incidens bekövetkeztekor. Csatolta a weboldalon használt pluginok listáját.

Hivatkozott arra, hogy bár volt tesztkörnyezet, a keresőmotorok SEO működése nem reprodukálható, ezért fordulhatott elő az inkompatibilitásból eredő adatszivárgás az éles rendszeren.

A Hatóság NAIH-5446-3/2024 számon információbiztonsági szakértői véleményt készíttetett, amely megállapította, hogy az incidenst információ szivárgás (information disclosure) okozta. Kimondta, ez a fajta sérülékenység alapvetően nem súlyos IT biztonsági probléma, könnyen kontrollálható pl.: teszteléssel elszeparált környezetben, rendszeres auditálással, monitorozással és megfelelő webszerver konfigurációval (könyvtárlistázás letiltása, hozzáférés korlátozása).

Ezt követően a Hatóság NAIH-5446-4/2024 számú tényállás tisztázó végzésére az Ügyfél NAIH-5446-5/2024 számú iratával válaszolt. Hivatkozott arra, hogy az információ szivárgást előidéző […] plugin telepítésére 2023. december és 2024. január közötti időszakban került sor, azonban pontos információ e tekintetben nem áll rendelkezésére.

A Hatóság NAIH-5446-6/2024 számú iratbetekintésre felhívó végzésére az Ügyfél NAIH-5446-7/2024 számú iratával válaszolt, akként, hogy iratbetekintési jogával élni kívánt. A Hatóság az Ügyfél részére az iratbetekintési jogot NAIH-5446-8/2024 számú végzésével elektronikus úton biztosította.

III. 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 4. cikk 1. pont: *„személyes adat”: azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármilyen információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.”*

Általános adatvédelmi rendelet 4. cikk 2. pont: *„adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;*

Általános adatvédelmi rendelet 5. cikk (1) bekezdés a), b) és c) pont: *„A személyes adatok:*

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);

b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”);

c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”).“

Általános adatvédelmi rendelet 5. cikk (2) bekezdés *szerinti elszámoltathatóság elvéből fakadóan az adatkezelőnek képesnek kell lennie arra, hogy igazolja a személyes adatok kezelésére vonatkozó elveknek való megfelelést.*

Az általános adatvédelmi rendelet 57. cikk (1) bekezdés f) pontja alapján: „*Az e rendeletben meghatározott egyéb feladatok sérelme nélkül, a felügyeleti hatóság a saját területén ellátja a következő feladatokat: kezeli az érintett vagy valamely szerv, szervezet vagy egyesület által a 80. cikkel összhangban benyújtott panaszokat, a panasz tárgyát a szükséges mértékben kivizsgálja, továbbá észszerű határidőn belül tájékoztatja a panaszost a vizsgálattal kapcsolatos fejleményekről és eredményekről, különösen, ha további vizsgálat vagy egy másik felügyeleti hatósággal való együttműködés válik szükségessé.“*

Az általános adatvédelmi rendelet 32. cikk (1) bekezdése kimondja, hogy 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, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;
b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

Az általános adatvédelmi rendelet 32. cikk (2) bekezdése szerint, 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 33. cikk (2) bekezdése kimondja, hogy az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Az általános adatvédelmi rendelet 33 cikk (3) bekezdése szerint, az (1) bekezdésben említett bejelentésben legalább:

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

Az általános adatvédelmi rendelet 33. cikk (4) bekezdése kimondja, ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

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

Az általános adatvédelmi rendelet 34. cikk (1) bekezdése 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.

Ugyanezen cikk (2) bekezdése szerint, az (1) bekezdésben említett, 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 Infotv. 38. § (3) bekezdés a) pontja alapján a Hatóság a (2) és (2a) bekezdés szerinti feladatkörében az e törvényben meghatározottak szerint különösen bejelentés alapján és hivatalból vizsgálatot folytat.

Az Ákr. 101. § (1) bekezdés a) pontja alapján, ha a hatóság a hatósági ellenőrzés során jogsértést tapasztal, megindítja a hatósági eljárását. Az Infotv. 38. § (3) bekezdése és 60. § (1) bekezdése alapján a Hatóság az Infotv. 38. § (2) és (2a) bekezdés szerinti feladatkörében a személyes adatok védelméhez való jog érvényesítése érdekében hivatalból adatvédelmi hatósági eljárást folytat.

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

Az Ákr. 62. § (1) bekezdése kimondja, hogy ha a döntéshozatalhoz nem elegendőek a rendelkezésre álló adatok, a hatóság bizonyítási eljárást folytat le.

Az Ákr. 62. § (2) bekezdése szerint a hatósági eljárásban minden olyan bizonyíték felhasználható, amely a tényállás tisztázására alkalmas. Nem használható fel bizonyítékként a hatóság által, jogszabálysértéssel megszerzett bizonyíték.

Az Ákr. 62. § (4) bekezdése kimondja, hogy a hatóság szabadon választja meg a bizonyítás módját, és a rendelkezésre álló bizonyítékokat szabad meggyőződése szerint értékeli.

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 Infotv. 58. § (2) bekezdés a) pontja szerint az (1) bekezdés szerinti esetben szükséges további intézkedésként a Hatóság a 60. §-ban foglaltak szerint adatvédelmi hatósági eljárást indít, illetve indíthat.

Az Infotv. 60. § (1) bekezdése alapján a személyes adatok védelméhez való jog érvényesülése érdekében a Hatóság az érintett erre irányuló kérelmére adatvédelmi hatósági eljárást indít és hivatalból adatvédelmi hatósági eljárást indíthat.

Az általános adatvédelmi rendelet 58. cikk (2) bekezdés b) és i) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva elmarasztalja az adatkezelőt vagy adatfeldolgozót, ha adatkezelési tevékenysége megsértette a rendelet rendelkezéseit, illetve a 83. cikknek megfelelően közigazgatási bírságot szab ki, az adott eset körülményeitől függően az e bekezdésben említett intézkedéseken túlmenően vagy azok helyett. Ugyanezen cikk (2) bekezdés d) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva utasítja az adatkezelőt vagy az adatfeldolgozót, hogy adatkezelési műveleteit – adott esetben meghatározott módon és meghatározott időn belül – hozza összhangba a rendelet rendelkezéseivel.

Az általános adatvédelmi rendelet 83. cikk (1) bekezdése kimondja, hogy az e cikk alapján kiszabott közigazgatási bírságok hatékonyak, arányosak és visszatartó erejűek legyenek.

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

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

IV. Döntés

A Hatóságnak a jelen eljárás során két – egymással szorosan összefüggő – kérdést kellett megvizsgálnia: egyrészről az Ügyfél incidens kezelését, másrészről az Ügyfél adatbiztonsággal, valamint beépített és alapértelmezett adatvédelemmel kapcsolatos követelményeknek történő megfelelését a […] weboldal üzemeltetése során.

A Hatóság az Ákr. 62. § (4) bekezdésében foglaltak szerint a rendelkezésre álló bizonyítékok értékelése alapján a felsorolt részkérdésekben az alábbi ténymegállapításokat teszi:

a) Incidenskezelés

A Hatóságnak a jelen ügyben először abban kellett állást foglalnia, hogy az Ügyfél incidens kezelése megfelelt-e az általános adatvédelmi rendelet 33-34. cikkében foglalt követelményeknek.

A Hatóság az incidensről való tudomásszerzés időpontjaként az Ügyfél által előadottakkal egyezően elfogadta 2024. január 23. napját.

Megállapítható, hogy az általános adatvédelmi rendelet 33. cikk (1) bekezdésében foglalt 72 órán belül, vagyis 2024. január 24-én az Ügyfél – jogi képviselője útján e-papíron – az incidens bejelentési kötelezettségének szakaszos incidens bejelentés keretében eleget tett a Hatóság felé.

A bejelentés tartalmi követelményei megfelelnek az általános adatvédelmi rendelet 33. cikk (3) bekezdésében foglaltaknak.

Az Ügyfél az érintettek tájékoztatását 2024. január 23-án telefonos úton, majd 2024. január 25-én e-mail útján megtette. Ennek igazolására csatolta a 62 érintett részére a tájékoztatás megküldését.

Az érintettek tájékoztatása akkor szükséges, amennyiben az általános adatvédelmi rendelet 34. cikk (1) bekezdésében foglaltak szerint az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Jelen esetben az adatvédelmi incidens magas kockázata nem volt megállapítható, de az Ügyfél az érintetteket ennek ellenére tájékoztatta, amely jó gyakorlatnak tekinthető.

Az incidens valószínűsíthető következményeit az Ügyfél korlátozottként értékelte. Az incidenssel érintett adatok: név, e-mail cím, telefonszám, motivációs videó, motivációs levél, publikus közösségi média fiókok elérési útvonalai; az incidens összesen 62 főt érintett.

Az Ügyfél csatolta a 2024. január 23-án kelt, „Jegyzőkönyv adatvédelmi incidens kockázatelemzéséről” elnevezésű dokumentumot. A dokumentumban bemutatásra kerülnek az incidenssel kapcsolatos körülmények, valamint az incidens lehetséges kockázataival kapcsolatos ténymegállapítások. A kockázat mértékének megállapításánál az érintett adatkörök, az érintettek száma (10-50 fő körül, melyet utóbb az Ügyfél 62 főben jelölt meg), érintettek beazonosíthatósága, illetve az a tény, hogy az érintett személyi kör nem tartozik sérülékeny csoporthoz, alapján az Ügyfél arra a következtetésre jutott, hogy az incidens lehetséges kockázata korlátozott.

Az általános adatvédelmi rendelet az adatvédelmi incidenseket a természetes személyek jogaira és szabadságaira való hatásuk szerint különböző kockázati szintekbe sorolja. Eszerint

kockázatmentes, kockázatos vagy magas kockázatúnak kell az incidenst az adatkezelőnek besorolnia.

A Hatóság az Ügyfél korlátozott kockázatú besorolását a fenti szempontok szerint úgy értelmezte, hogy azt az Ügyfél legalább kockázatosnak tekinti. Ennek megfelelően az incidenst a felügyeleti hatóságnak köteles bejelenteni, melynek az Ügyfél eleget tett. A Hatóság az érinettek azonosíthatóságát az incidensben kockázatnövelő tényezőként értékelte.

A Hatóság az Ügyfél fenti incidens kockázatelemzésével kapcsolatos érvelését, valamint a csatolt incidenskezelési szabályzatban foglalt eljárásrendet elfogadta.

A Hatóság az érintettek tájékoztatásával kapcsolatos okiratokat megvizsgálta, s megállapította, hogy azok megfelelnek az általános adatvédelmi rendelet 34. cikk (2) bekezdésében foglalt tartalmi követelményeknek.

Az Ügyfél az incidens hosszú távú orvoslásaként előadta, hogy a hasonló incidensek megelőzésével kapcsolatos technológiai fejlesztések tekintetében a keretrendszer adminisztrációjához kétfaktoros autentikáció bevezetését tervezi, az emelt jogosultsággal rendelkező felhasználók körét felülvizsgálja, továbbá a kiszolgáló környezetet érintően biztonsági funkciókat kíván bevezetni […] környezet létrehozása a konfiguráció változások és tesztelések érdekében, a kiterjedt tesztelések jegyzőkönyvezésre kerülnek.

A Hatóság a fentiek összegzéseként megállapította, hogy az Ügyfél az incidens kezelésével kapcsolatban az általános adatvédelmi rendelet 33-34. cikkében foglaltak szerint megfelelően járt el.

b) Adatbiztonsági követelmények vizsgálata

Ezt követően a Hatóság a jelen incidenssel összefüggésben az általános adatvédelmi rendelet 32. cikkében foglalt adatbiztonságra vonatkozó követelményeket vizsgálta meg.

Az általános adatvédelmi rendelet 32. cikk (1) bekezdése szerint az adatkezelőnek, illetve az adatfeldolgozónak több körülményt együttesen kell mérlegelnie a megfelelő szintű adatbiztonság garantálása érdekében, majd ezt követően kell különböző adatkezelés specifikus technikai és szervezési intézkedéseket meghoznia. A mérlegelésre szoruló körülmények többek között 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 mértéke szerepel. A megfelelő szintű adatbiztonság tehát a fenti körülményektől függően az egyes adatkezelők esetében eltérő lehet, ugyanakkor nem is egy állandó fogalom, hiszen a tudomány és technológia folyamatos változása miatt folyamatos újraértékelésre szorul az adatkezelő által. Ez a rendszeres újraértékelési tevékenység az adatkezelő felelőssége.

Az adatkezelő által megtett technikai intézkedésnek minősül pl.: jelszó policy, antivírus, tűzfal, többfaktoros hitelesítés stb., míg szervezési intézkedés pl.: belső szabályzatok megalkotása és elfogadása, adatvédelmi tudatosság oktatás, megfelelő dokumentáció biztosítása stb.

A technikai és szervezési intézkedések köre igen széles, alkalmazásukat az adatkezelő szabad belátása szerint, mindig az adott szervezet működésére tekintettel, szervezetspecifikusan mérlegeli és dönti el.

A Hatóság ezeknek a technikai és szervezési intézkedéseknek a meglétét, illetve megfelelőségét mindig esetről-esetre vizsgálja és értékeli. Az adatkezelőnek az elszámoltathatóság elve alapján biztosítania kell azt, hogy az alkalmazott technikai és

szervezési intézkedéseket szükség esetén bemutassa és azok megalapozottságát hitelt érdemlően dokumentumokkal is igazolja.

A Hatóság e körben az Ügyfél által tett nyilatkozatok, a csatolt okiratok, valamint a NAIH-5446-3/2024 szám alatt készített információbiztonsági szakértői vélemény alapján az alábbi megállapításokat teszi:

A Hatóság számára a vizsgálat időpontjában, 2024. január 26-án az említett weboldal már elérhetetlen volt, ugyanis az „oldal karbantartás alatt áll" volt olvasható az oldalon, így a tényállást megállapítani elsősorban az Ügyfél által előadottak, valamint a megküldött dokumentumok alapján lehetséges.

Az Ügyfél által üzemeltetett […] weblap működése során 2024. január 23-án bekövetkezett adatvédelmi incidens oka igazolhatóan az információ szivárgás (information disclosure) volt.

Az információ szivárgást az idézte elő, hogy az […] plugin telepítése konfigurációs problémát okozott, amely felülírta a korábban használt és jelenleg is élesben használt […] bővítmény konfigurációit. […] bővítmény telepítésére 2023. december és 2024. január közötti időszakban került sor, azonban pontos információ nem állt az Ügyfél rendelkezésére.

Az információ szivárgás egy olyan esemény, amikor valamilyen érzékeny vagy titkos információ nem szándékosan illetéktelen személyek vagy szervezetek számára jut hozzáférhetővé. Ez az információ lehet üzleti titok, személyes adat, szoftver forráskód, vagy bármilyen más adat. Jelen esetben az adatvédelmi incidens következett be, mivel az Ügyfél által szervezett képzésekre jelentkezők különböző személyes adatai voltak érintettek.

A szakértői vélemény megállapította, hogy ezekben az esetekben valószínű, hogy az adott URL hozzáférési szabályai nem megfelelően vannak konfigurálva, vagy egyszerűen nincsenek megfelelően beállítva. Ez azt jelenti, hogy a dokumentumokhoz bárki hozzáférhet, aki ismeri az URL-t, anélkül, hogy megfelelő jogosultságokkal rendelkezne.

Ez a fajta sérülékenység alapvetően nem súlyos informatikai biztonsági probléma, könnyen kontrollálható pl.: teszteléssel elszeparált környezetben, rendszeres auditálással, monitorozással és megfelelő webszerver konfigurációval (könyvtárlistázás letiltása, hozzáférés korlátozása).

A sérülékenység felismerése és megfelelő kezelése, valamint az általános adatvédelmi rendelet 32. cikke szerinti technikai és szervezési intézkedések megtétele az Ügyfél, vagyis az Adatkezelő, a weboldal üzemeltetőjének a feladata.

A Hatóság álláspontja szerint az alábbi intézkedések megtételével az incidens elkerülhető lett volna:

- **Tesztelés elszeparált környezetben**: A bővítmény egy külön fejlesztői vagy tesztkörnyezetben való tesztelése, hogy nem okoz-e problémát a rendszerben, mielőtt kikerül az éles rendszerre.
- **Rendszeres auditálás és monitorozás**: Naplózás és eseményfigyelés, rendszeres biztonsági auditok és sebezhetőségi vizsgálatok végzése, vagy soron kívüli vizsgálat, ha új rendszerelem kerül be.
- **Webszerver konfigurációja - könyvtárlistázás letiltása, hozzáférés korlátozása**: pl.: htaccess fájlok használata az érzékeny könyvtárak és fájlok hozzáférésének korlátozására. Azon tényt, hogy a webszerver konfiguráció nem volt megfelelő, egyebekben az Ügyfél sem vitatta.

A fent említett eljárások a tudomány és technológia állása, a megvalósítás költsége, valamint az adatkezelés jellegét figyelembe véve általánosan elvárható intézkedések egy személyes adatokat kezelő, magasabb látogatottságot élvező honlapot üzemeltető adatkezelő esetében, továbbá nem igénylik aránytalan erőfeszítés, valamint pénzügyi és humán erőforrás igénybevételét sem.

A fentiek alapján a Hatóság a rendelkezésre álló bizonyítékokból megállapította, hogy az Ügyfél az általános adatvédelmi rendelet 32. cikk (1) bekezdés d) pontjában foglalt kötelezettségét megszegte, mert az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást nem biztosította, azáltal, hogy az általa üzemeltetett […] nevű weboldalon a fejlesztői tesztkörnyezet alkalmazását, valamint a webszerver megfelelő konfigurációját elmulasztotta, így a weboldalon információ szivárgás lépett fel, mely adatvédelmi incidenst eredményezett.

V. Alkalmazott szankció és indoklása

A Hatóság hivatalból megvizsgálta, hogy a fenti jogsértések miatt indokolt-e Ügyféllel szemben adatvédelmi bírság kiszabása, ezért a GDPR 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az összes körülményt.

A Hatóság enyhítő körülményként vette figyelembe, hogy az incidens (2023. december - 2024. január) viszonylag rövidebb ideig állt fenn [általános adatvédelmi rendelet 83.cikk (2) bekezdés a) pont].

A Hatóság enyhítő körülményként vette figyelembe, hogy Ügyfél elmarasztalására az általános adatvédelmi rendelet megsértése miatt még nem került sor [általános adatvédelmi rendelet 83. cikk (2) bekezdés e) pont], illetve a jogsértés nem érint érzékeny személyes adatokat.

A Hatóság szintén enyhítő körülményként vette figyelembe az Ügyfél együttműködő magatartását, ennek keretében a weboldal működésével kapcsolatos technikai és szervezési intézkedések átgondolását [általános adatvédelmi rendelet 83. cikk (2) bekezdés f) pont], valamint azt, hogy érintetteket ez idáig semmilyen kár nem érte a felmerült adatvédelmi incidenssel összefüggésben [általános adatvédelmi rendelet 83. cikk (2) bekezdés a) pont].

A Hatóság a fenti súlyosító és enyhítő körülmények együttes mérlegelését követően arra a következtetésre jutott, hogy jelen esetben a jogsértés megállapításán túl a figyelmeztetés alkalmazása is elegendő, kellő visszatartó erővel bíró jogkövetkezménynek tekinthető. A figyelmeztetéssel a Hatóság rosszallását fejezi ki az általa megállapított szabályszegés elkövetése miatt, és újabb szankció kilátásba helyezésével felszólítja az Ügyfelet, hogy a jövőben tartózkodjon az adatvédelmi szabályszegés elkövetésétől.

A Hatóság egyúttal felhívja az Ügyfél figyelmét arra, hogy egy újabb adatvédelmi jogsértés megállapítása esetén a jogkövetkezmények megállapításakor a jelen jogsértést, mint előzményt fokozott súllyal veszi majd figyelembe.

A Hatóság kiemeli, jelenleg és a jövőben is nyomatékos célkitűzése, hogy ösztönözze Ügyfelet arra, adatkezelési tevékenységét, tevékenységeit tudatosan folytassa, és ehhez kapcsolódó technikai és szervezési intézkedések meghozatalát és betartását tartsa szem előtt.

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

A Hatóság az Infotv. 61.§ (2) bekezdés a) pontjában foglaltak alapján a rendelkező részben

foglaltak szerint elrendelte a jelen határozat közzétételét a Hatóság honlapján, továbbá az Ügyfél honlapjának nyitóoldalán, jól látható és könnyen hozzáférhető helyen, a határozat véglegessé válásától számított 30 napon belül, és ott legyen elérhető legalább 30 napon keresztül. A közzététel indoka az, hogy a jelen eljárás tárgyát képező incidens a sajtóhírekben szerepelt, sajtónyilvánosságot kapott kérdés, mely személyek szélesebb körét érinti, ezért a közérdek az, hogy a nyilvánosság a döntés tartalmát megismerhesse.

VI. Egyéb kérdések

A Hatóság hatáskörét az Infotv. 38. § (2) és (2a) bekezdése határozza meg, illetékessége az ország egész területére kiterjed.

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

A közigazgatási per szabályait a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) határozza meg. A Kp. 12. § (1) bekezdése alapján a Hatóság döntésével szembeni közigazgatási per törvényszéki hatáskörbe tartozik, a perre a Kp. 13. § (3) bekezdése 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 – ha törvény eltérően nem rendelkezik – a keresetlevél benyújtásának a közigazgatási cselekmény hatályosulására halasztó hatálya nincs.

A Kp. 29. § (1) bekezdése és erre tekintettel a polgári perrendtartásról szóló 2016. évi CXXX. törvény 604. § szerint alkalmazandó, a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (a továbbiakban: Digiáptv.) 19. § (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. 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.

Kelt: Budapest, „az elektronikus aláírás és időbélyeg szerint”

Dr. habil. Péterfalvi Attila
elnök
c. egyetemi tanár