Ügyszám: NAIH/2020/1137
Előzmény: NAIH/2019/4152

Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban

H A T Á R O Z A T

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) a **[…]-t** (székhely: […]) (a továbbiakban: Ügyfél) érintő adatvédelmi incidenssel kapcsolatban 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) 32-34. cikkében foglalt kötelezettségei teljesítésének elmaradása tárgyában hivatalból megindított **adatvédelmi hatósági eljárásban**

1. **megállapítja**, hogy

   a. az Ügyfél megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdését, így nem alkalmazott az adatkezelés biztonsága körében megfelelő technikai és szervezési intézkedéseket, azzal, hogy az ügyfélkapus hozzáférési adatokat tartalmazó fájlt nyomtatott formában is tárolta, amely így közvetlenül lehetővé tette az adatvédelmi incidens bekövetkezését.

   b. Az Ügyfél megsértette az általános adatvédelmi rendelet 24. cikk (1)-(2) bekezdéseiben foglaltakat, amikor a belső adatvédelmi incidenskezelési szabályzatában nem szabályozta a felügyeleti hatóságnak történő bejelentési kötelezettség esetkörét.

2. **kötelezi** az Ügyfelet, hogy

   a. az érintettektől beszerzett ügyfélkapus hozzáférési adatokat tartalmazó adatbázist ne tárolja papíralapon, csupán elektronikus formában, és az adatbázis egyes verzióiról is elektronikus formában készítsen biztonsági másolatot.

   b. Módosítsa belső adatvédelmi incidenskezelési szabályzatát úgy, hogy abban térjen ki a felügyeleti hatóságnak történő bejelentési kötelezettség esetkörére is.

3. a fenti jogsértés miatt az Ügyfelet a **jelen határozat véglegessé válásától számított 30 napon belül**

   500.000,- Ft, azaz ötszázezer forint

   adatvédelmi bírság megfizetésére kötelezi;

4. **elrendeli** a végleges határozatnak az adatkezelő azonosító adatainak közzététele nélküli **nyilvánosságra hozatalát.**

A bírságot a Hatóság központosított bevételek beszedési célelszámolási forintszámlája (10032000-01040425-00000000 Központosított beszedési számla IBAN: HU83 1003 2000 0104 0425 0000 0000) javára kell átutalással megfizetni. Az összeg átutalásakor a NAIH/2019/4152 BÍRS. számra kell hivatkozni.

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

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

Jelen határozattal szemben közigazgatási úton jogorvoslatnak nincs helye, de az a közléstől számított 30 napon belül a Fővárosi Törvényszékhez címzett 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.

I N D O K O L Á S

I. Előzmények, a tényállás tisztázása

a. A Hatósághoz érkezett közérdekű bejelentés

A Hatósághoz egy magánszemélytől közérdekű bejelentés érkezett, amelyben a bejelentő leírta, hogy birtokába került egy lista, amely természetes személyek és vállalkozások (kb. 100 db) különböző adatait tartalmazza. A lista az érintettek teljes nevét, adóazonosítóját, TAJ számát, születési adatait, édesanyjuk nevét, továbbá a magyarorszag.hu honlapon keresztül elérhető ügyfélkapus felhasználói neveiket és titkosítatlan jelszavaikat tartalmazza.

A beadványt előterjesztő elmondása szerint a lista úgy került a birtokába, hogy azt a […] alatti ingatlanjának kertjében szedte össze […] a szél által odafújt egyéb papírszemetekkel együtt. A megtalált listát a beadványozó eredetben továbbította a Hatóság részére.

A Hatóság a bejelentés kapcsán NAIH/2019/1332 ügyszámon hatósági ellenőrzést indított, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy az ügyfélkapu üzemeltetésében résztvevő NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.) maradéktalanul eleget tett-e 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 rendeletben (a továbbiakban: általános adatvédelmi rendelet) foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak.

A Hatóság a hatósági ellenőrzés során NAIH/2019/1332/2. ügyiratszámú, 2019. február 1-én kelt végzésével nyilatkozattételre és iratszolgáltatásra szólította fel a NISZ Zrt-t. A NISZ Zrt. megerősítette, hogy a listában valóban az Ügyfélkapuhoz tartozó adatok szerepelnek, amelyek két cég és egy egyéni vállalkozó kivételével valósak és a jelen állapotot tükrözik. Az Ügyfélkapuhoz

tartozó felhasználónevek és jelszavak a Központi Ügyfél-regisztrációs Nyilvántartásban (a továbbiakban: KÜNY) vannak nyilvántartva, amely adatok tekintetében egyébként nem a NISZ Zrt., hanem a Belügyminisztérium (a továbbiakban: BM) az adatkezelő. A BM-en belül a feladatot a Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság Személyi Nyilvántartási és Igazgatási Főosztálya látja el. A KÜNY az Ügyfélkapu esetén a következő személyes adatokat tartalmazza: igénylő személy természetes személyazonosító adatai, állampolgársága, egyedi azonosító száma, kapcsolati kód, felhasználói név, a belépési jelszó visszafejthetetlen lenyomata és az érintett elektronikus levelezési címe. A NISZ Zrt. elmondása szerint ezért a megtalált listában szereplő jelszavakat még a BM sem kezeli, csupán azok visszafejthetetlen lenyomata szerepel a nyilvántartásukban. A jelszót csak az a személy ismerheti, aki a regisztrációt elvégezte.

A NISZ Zrt. véleménye szerint a lista valószínűleg egy könyvelő által vezetett ügyfél adatbázis lehet, mivel abban szerepel még az adóazonosító, a TAJ szám és ÜCC kód is, amely adatok nem kapcsolódnak a KÜNY-höz.

A fentiekre tekintettel a NISZ Zrt. az adatvédelmi incidensről nem bírt tudomással és az semmilyen módon nem hozható összefüggésbe sem az ő, sem a KÜNY vezetésére jogosult BM adatkezelési tevékenységével. A Hatóság ezért megállapította NAIH/2019/1332/7. ügyiratszámon, hogy a rendelkezésre álló információk alapján nem a NISZ Zrt-nél történt adatvédelmi incidens.

A nyilvánosságra került lista alján azonban utalás történik egy […] megnevezésű szervezetre, valamint arra, hogy „a nevük alatt regisztrált cégek/személyek saját ügyfélkapujukon adunk be mindent.”

A […] (az Ügyfél) könyveléssel foglalkozik, székhelye pedig megegyezik a listát a Hatósághoz eljuttató panaszos lakcímével: […]. Tekintettel ezen körülményre a Hatóság külön ügyszám alatt, NAIH/2019/4152/2 ügyiratszámon, 2019. május 16-án új hatósági ellenőrzés megindítását határozta el az Ügyfél adatkezelésével kapcsolatban, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy az Ügyfél maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak.

b. A Hatóság által a hatósági ellenőrzés során küldött tényállás-tisztázó végzésekre adott válaszok

1) A Hatóság NAIH/2019/4152/2. számú végzésével nyilatkozattételre hívta fel az Ügyfelet a tényállás tisztázása érdekében. A végzésben feltett kérdésekre az Ügyfél határidőben válaszolt.

Az Ügyfél válaszában elismerte, hogy a közérdekű bejelentő által megtalált és a Hatóságnak is megküldött listában valóban az Ügyfél által kezelt, ügyfeleihez tartozó személyes adatok találhatóak. Ezen listán lévő adatok kezelésének célja a társaság és ügyfelei között létrejött számviteli, könyvvizsgálói és adószakértői tevékenységre irányuló szerződésekben foglalt kötelezettségek teljesítése, illetve az ügyfelekkel való kapcsolattartás. Ezeket az adatokat a társaság ügyfelei önként hozzák annak tudomására, az egyes megbízási szerződések aláírása során egyben hozzájárulásukat is adják az adatok ilyen célú kezeléséhez.

A listán található személyes adatokat az Ügyfél saját irodai szerverén tárolja, amelyhez kizárólag az alkalmazottak és az IT feladatok ellátásával megbízott személy férhet hozzá. A tárhely jelszóval védett. A listát az Ügyfél az adatok esetleges változása esetén frissíti. A frissítés során a lista egy példányban kinyomtatásra kerül azzal, hogy azon a nyomtatás dátumát kézírással rögzítik és a többi listával együtt, időrendben lefűzve egy elzárt mappában őrzik. Erre a későbbi esetleges

adatellenőrzésekre tekintettel van szüksége elmondása szerint az Ügyfélnek. Ha esetleg véletlenül további példányok is kinyomtatásra kerülnének a listából, úgy azt iratmegsemmisítővel kell „ledarálni”.

A lista kikerüléséről a kezeléséből a Hatóság végzésének kézhezvételéig nem volt tudomása az Ügyfélnek. Az Ügyfél megítélése szerint a lista valószínűleg rosszhiszemű belső cselekmény révén kerülhetett ki a kezeléséből, mivel annak elektronikus és papír alapú tárolása is védett, elzárt helyen történik. Korábban az Ügyfél ezért nem állapította meg az adatvédelmi incidens bekövetkezését, mivel nem volt tudomása arról. A lista kikerülésével kapcsolatban az Ügyfél büntető feljelentés megtételét tervezi. A fentieken túl a lista kikerülésének pontos körülményeiről az Ügyfél nem bír tudomással.

2) A Hatóság újabb tényállás tisztázó végzést küldött az Ügyfél részére NAIH/2019/4152/4. számon, amire az Ügyfél határidőben válaszolt. Ebben kifejtette, hogy az adatok gyűjtése kapcsán külön adatvédelmi tájékoztatóval rendelkezik, amelyek aláírásával adják hozzájárulásukat az ügyfelek adatait fentiekben kifejtett célokból történő kezeléséhez. A tájékoztató egy példányát az Ügyfél megküldte a Hatóság részére.

A listán található adatokhoz az Ügyfél szerverén az irodában dolgozó alkalmazottak, összesen 9 fő férhetett hozzá. Ők a szerződések teljesítése és kapcsolattartási célokból férhetnek hozzá az adatokhoz. A fájlhoz való hozzáférések nem kerülnek naplózásra. A szerverhez való hozzáférés jelszavai kialakításánál nincs kialakítva különösebb kikényszerített jelszó házirend, azokat a felhasználó egyénileg, szabadon adja meg.

Az Ügyfél közölte, hogy a Hatóság első végzéséből az incidensről való tudomásszerzés után 12 órán belül személyesen és telefonon értesítették valamennyi érintettet.

A Hatóság kérdésére az Ügyfél közölte továbbá, hogy rendelkezik adatvédelmi incidens nyilvántartással. Az incidenseket egy szintén a központi szerveren található szöveges .doc kiterjesztésű dokumentumban vezetik. Jelen ügyben készített bejegyzést a nyilvántartásból továbbította a Hatóságnak az Ügyfél.

c. Adatvédelmi hatósági eljárás indítása az ügyben és a tényállás további tisztázása

Az ügyben a hatósági ellenőrzés során megállapítottakon túl az általános adatvédelmi rendelet 32-34. cikkeiben foglalt kötelezettségek Ügyfél általi feltételezhető megsértése miatt, az Infotv. 60. § (1) bekezdésére tekintettel, a Hatóság adatvédelmi hatósági eljárás megindításáról döntött 2019. július 16. dátummal.

1) Az ügyben a hatósági ellenőrzés során megállapítottakon túl a tényállás további tisztázása vált szükségessé, ezért a Hatóság az Ügyfél újabb megkereséséről, nyilatkoztatásáról és iratszolgáltatásra történő felhívásáról döntött NAIH/2019/4152/7. számon.

Az Ügyfél a fenti végzésre határidőben válaszolt. Az irodai szerver eléréséhez szükséges jelszavak képzésével kapcsolatban csupán annyit válaszolt, hogy azok erősségüket tekintve megfelelnek „az általános követelményeknek”. Az eszközökön és a rendszerben még nincs automatikusan ellenőrzött és vezérelt jelszó házirend kialakítva, annak folyamatát az incidenst követően azonban elindították, ez azonban jelentős anyagi és időráfordítást igényel.

A Hatóság ezirányú kérdésére közölte az Ügyfél, hogy az általa használt szerver jelenleg fájlszerverként működik. Az új jelszó házirend kialakítása érdekében ún. tartomány vezérlővé kell előléptetni a szervert és ennek megfelelően átalakítani a rendszer egyéb elemeit is. Ennek során lesz kialakítva a fokozott biztonságot adó jelszó házirend. Ezen túlmenően az egyes felhasználók belépésének és adatokhoz való hozzáférésének naplózása is kialakításra kerül. Ezen felül az egyes fájlokhoz való hozzáférések felhasználói jogosultságkezelése és korlátozása is részletesebben beállításra kerülhet a rendszerben.

Az Ügyfél megküldte a Hatóságnak a belső adatvédelmi szabályzatát, amelynek részét képezik az adatvédelmi incidensek kezelésére vonatkozó rendelkezések is. A szabályzat kitér az incidensek kezelésével kapcsolatban azok nyilvántartásba vételére, illetve magas kockázatuk esetén az érintettek tájékoztatására, azonban nem tartalmaz az általános adatvédelmi rendelet 33. cikk (1) bekezdése szerinti bejelentési kötelezettséggel kapcsolatos rendelkezéseket.

Az ügyfélkapus adatok érintettektől való bekérésével kapcsolatban az Ügyfél továbbá azt nyilatkozta, hogy minden könyveléssel kapcsolatos napi kommunikáció (adatszolgáltatás, bevallások, lekérdezések) a központosított elektronikus ügyintézés keretében, az ügyfélkapun keresztül történik a jelenlegi rendszerben. A tranzakciók során keletkezett, az érintett ügyfelekkel kapcsolatban felhasznált információk a könyvelői irodában keletkeznek, vagy itt van szükség a felhasználásukra. Egyszóval az Ügyfél szerint mindenképpen a könyvelői irodában dől el, hogy milyen intézkedésre van szükség, ezért szükségesek az ügyfélkapus belépéshez és ügyintézéshez az adatok. A könyvelőiroda tehát az ügyfél nevében az ügyfélkapun keresztül jár el a belépési adataik kezelésével. Az Ügyfél szerint minden könyvelőiroda így működik. A jövőben az Ügyfél viszont egy új, külön nyilatkozatban fogja bekérni a belépési adatokat az érintettektől, amelyben részletesebben lesznek leírva az adatok felhasználásával kapcsolatos feltételek.

2) A Hatóság a fentiek után NAIH/2019/4152/9. számon újabb nyilatkozattételre hívta fel az Ügyfelet, amelyre az határidőben válaszolt.

A Hatóság azirányú kérdésére, hogy az ügyfélkapus hozzáféréseket tartalmazó .doc kiterjesztésű fájl bármilyen hozzáférés védelemmel (pl. jelszó) el volt-e látva az Ügyfél nem válaszolt érdemben. Itt csak megismételte azt a korábban tett nyilatkozatát, hogy a fájlok – így az említett .doc fájl – is egy fájlszerveren van tárolva. Ezt a szervert pedig az egyes számítógépek önálló jelszavakkal tudják elérni.

Az Ügyfél továbbá azt nyilatkozta, hogy jelenleg nem rendelkezik informatikai biztonsági szabályzattal, de annak kialakítása – az incidens bekövetkezésére való tekintettel is – folyamatban van.

Az Ügyfél álláspontja szerint az érintettek ügyfélkapus jelszavainak periodikus megváltoztatására való felhívás nem feladatuk, az az adott felhasználó privilégiuma. Ettől függetlenül az Ügyfél az incidensről való tudomásszerzést követően haladéktalanul tájékoztatta arról az incidenssel érintetteket, hogy változtassák meg az ügyfélkapus jelszavaikat. Ezen felül tájékoztatták arról is az érintetteket, hogy ha az incidensből adódóan bármilyen kár érné őket, azért az Ügyfél teljes felelőssége tudatában helyt áll.

A fentiekben ismertetett tényállás alapján a Hatóság az Ügyfélnél jogsértést állapított meg, ezért az ügyben meghozta jelen határozatot.

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

Az általános adatvédelmi rendelet 24. cikk (1)-(2) bekezdései alapján:
(1) az adatkezelő 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 biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.
(2) Ha az az adatkezelési tevékenység vonatkozásában arányos, az (1) bekezdésben említett intézkedések részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.

Az általános adatvédelmi rendelet 32. cikk (1) és (2) bekezdései szerint 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 […]. 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)-(2) és (4)-(5) bekezdései szerint az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek. Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők. 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 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 információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 61. § (1) bekezdés a) pontja alapján a Hatóság a 2. § (2) és (4) bekezdésében meghatározott adatkezelési műveletekkel összefüggésben az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja.

Az általános adatvédelmi rendelet 58. cikk (2) bekezdés b) és i) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva elmarasztalja az adatkezelőt vagy adatfeldolgozót, ha adatkezelési tevékenysége megsértette a rendelet rendelkezéseit, illetve a 83. cikknek megfelelően közigazgatási bírságot szab ki, az adott eset körülményeitől függően az e bekezdésben említett intézkedéseken túlmenően vagy azok helyett. 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.

A közigazgatási bírság kiszabására vonatkozó feltételeket az általános adatvédelmi rendelet 83. cikke tartalmazza. 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.

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.

III. Döntés

a. Az eset adatvédelmi incidens jellege és az adatkezelő által megtett intézkedések

1) A Hatóság a feltárt tényállás alapján megállapította, hogy a bekövetkezett adatvédelmi incidensről az Ügyfél saját elmondása szerint legkorábban akkor szerzett tudomást, amikor 2019. május 20-án az ügy ezirányú részleteiről is értesült a Hatóság NAIH/2019/4152/2. számú tényállás tisztázó végzéséből. Az esetet az Ügyfél korábban nem minősítette adatvédelmi incidensnek, mivel elmondása szerint az ügyfélkapus adatokat tartalmazó papírlap kikerüléséről egyáltalán nem volt tudomása. A Hatóság megkeresésére az Ügyfél az esetet szinte rögtön adatvédelmi incidensnek minősítette és a megkeresésre való válasz részeként csatolta az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján vezetett incidens-nyilvántartásából a bejegyzés másolatát, továbbá a tudomásszerzéstől számított 12 órán belül felvette a kapcsolatot valamennyi érintettel és őket az incidensről tájékoztatta.

Az általános adatvédelmi rendelet 33. cikk (1) bekezdése szerint fő szabályként az incidenst be kell jelenteni a felügyeleti hatóságnak. A rendelet ezen bekezdése és a (85) preambulumbekezdése is kimondja, hogy a bejelentéstől az adatkezelő csak abban az esetben tekinthet el, ha az elszámoltathatóság elvével[1] összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Mivel a főszabály az incidens hatóságoknak való bejelentése, az ez alóli kivétel is szűken értendő.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből – így jelen ügyben az eszközök rendeltetésszerű használatából – személyazonosság-lopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül. Az Ügyfél kezeléséből kiszivárgott listán található adatok (érintett teljes neve, adóazonosítója, TAJ száma, születési adatai, édesanyjuk neve, a magyarorszag.hu honlapon keresztül elérhető ügyfélkapus felhasználói nevek és titkosítatlan jelszavaik) ismeretében pedig elkövethető személyazonosság-lopás, vagy személyazonossággal visszaélés, az érintett ügyfélkapus hozzáférésének tudta nélküli használata, ott tárolt egyéb adatok jogosulatlan megismerése.

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

Az Ügyfél úgy nyilatkozott, hogy a hatósági ellenőrzés megindítása kapcsán szerzett csak tudomást az incidens bekövetkezéséről, ezért a Hatóság szerint az Ügyfél általi hivatalos tudomásszerzésnek ez az időpont minősül. A Hatóság megítélése szerint a tudomásszerzés idejének megítélése szempontjából elég, ha olyan érdemi ügyintéző / elöljáró tudomására jut az incidens bekövetkezésének ténye az adatkezelőnél, aki azt nem szándékosan maga okozta, és akinek minden lehetősége és eszköze megvolt a releváns döntéshozók, tisztviselő értesítésére. Ezt az értelmezést alátámasztja a 29. cikk szerinti Adatvédelmi Munkacsoport iránymutatása is az adatvédelmi incidens bejelentéséről, amely alapján „tudomásszerzésnek az minősül, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.”[2]

A Hatóság eltekint ezért az Ügyfél az incidens utólagos bejelentésére való felszólításától, mivel a hatósági ellenőrzés, majd eljárás során sikerült tisztázni az incidens körülményeit és a megtett intézkedéseket. Jelen ügyben az érintettek jogai és szabadságainak védelmét nem növelné az incidens bejelentésére való utólagos felszólítás az azzal kapcsolatos hatósági eljárás lezárulta után.

2) Az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján továbbá 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. A rendelet (86) preambulumbekezdése szerint a tájékoztatás fő célja, hogy az érintett is megtehesse a szükséges óvintézkedéseket az incidensből fakadó kockázatok

[1] általános adatvédelmi rendelet 5. cikk (2) bekezdés: Az adatkezelő felelős az (1) bekezdésnek [alapelvek] való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

[2] Lásd: 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, 10. oldal.

mérséklése érdekében. A Hatóság jelen ügyben az incidenst, olyan magas kockázatú incidensnek tekinti, amely indokolja az érintettek tájékoztatását.

Az incidensről való tájékoztatásra a Hatóság megítélése szerint kifejezetten azért is van szükség, mivel az érintett magánszférájára jelentett kockázat a személyazonosításra alkalmas adatok közül különösen a felhasználónév és titkosítatlan jelszó párok nyilvánosságra kerülése esetén olyan jellegű (ezen adatok birtokában nagyon könnyen elkövethető személyazonossággal visszaélés), amelynek kockázatai csak úgy mérsékelhetők eredményesen, ha az érintettek erről tudomással bírnak, és megtehetik az általuk szükségesnek tartott további intézkedéseket.

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

Mivel azonban Ügyfél helyesen mérte fel már a Hatóság első végzésének kézhezvétele során az incidens magas kockázatát és a tudomásszerzéstől számított 12 órán belül felvette a kapcsolatot valamennyi érintettel, ezért a Hatóság megítélése szerint eleget tett az általános adatvédelmi rendelet 34. cikkéből fakadó kötelezettségeinek. Ezen körülménnyel kapcsolatban így a Hatóság további felszólítást nem tesz.

3) 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 a tudomásszerzés után nyilvántartásba vette az adatvédelmi incidenst.

Az Ügyfélnek a Hatóság ellenőrzése előtt nem volt tudomása arról, hogy a lista kiszivárgott, így személyes adatok juthatnak illetéktelen kezekbe. Az Ügyfél a tudomásszerzés után azonban felvette az érintettekkel a kapcsolatot, tájékoztatta őket a körülményekről és kárfelelősséget is vállalt az esetleges következmények után. Az okozott incidens kezelése kapcsán így az Ügyfél a Hatóság megítélése alapján a szükséges intézkedéseket megtette, további felszólítás irányába ezért nem indokolt.

b. Az ügyfélkapus adatok tárolásával és az incidenskezeléssel kapcsolatos adatbiztonsági intézkedések

1) Az Ügyfél a Hatóság tényállás tisztázó végzéseiben megismert körülmények ismeretében átvizsgálta belső folyamatait és adatbiztonsági intézkedéseit is korszerűsítette (pl. fájlok tárolása, jelszavak használata a szerver eléréséhez stb.). A Hatóság ezeket az intézkedéseket nagyrészt elfogadja, azonban néhány intézkedéssel kapcsolatban megállapításokat tesz.

Az incidens bekövetkezése előtt, és az annak hatására megtett adatbiztonsági intézkedésekkel kapcsolatban a Hatóság az alábbi megállapításokat teszi.

Az általános adatvédelmi rendelet 4. cikk 12. pontja alapján adatvédelmi incidensnek a biztonsági sérülésekből adódó, személyes adatokat érintő jogellenes műveletek minősülnek. A fogalom szempontjából így a biztonsági eseménnyel való kapcsolat kulcselemnek tekinthető.

Az adatkezelés biztonságával kapcsolatban a rendelet 32. cikk (1) bekezdése kimondja, hogy többek között a tudomány és technológia állása és a felmerülő kockázatok figyelembe vételével az adatkezelő feladata, hogy az adatok biztonságát megfelelő technikai és szervezési intézkedésekkel garantálja. Ezen cikk (1) bekezdés b) pontja alapján az adatbiztonsági intézkedések hivatottak arra is, hogy a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét garantálják. A 32. 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.

Az Ügyfél úgy nyilatkozott az eljárás során, hogy a listán található személyes adatokat saját irodai szerverén tárolja, amelyhez kizárólag az alkalmazottak és az IT feladatok ellátásával megbízott személy (összesen 9 fő) férhet hozzá. Maga a fájl nem, csupán a szerverhez hozzáférő kliens számítógépek kerültek jelszavas védelemmel ellátásra. Az adatok tárolásának célja a könyvelőiroda ügyfeleivel kötött szerződések teljesítése. A listát az Ügyfél az adatok esetleges változása esetén frissíti. A frissítés során a lista egy példányban kinyomtatásra kerül azzal, hogy azon a nyomtatás dátumát kézírással rögzítik és a többi listával együtt, időrendben lefűzve egy elzárt mappában őrzik. Erre a későbbi esetleges adatellenőrzésekre tekintettel van szüksége elmondása szerint az Ügyfélnek.

A Hatóság álláspontja szerint az adatkezelés biztonságát csökkentő intézkedésnek tekinthető az, ha az adatkezelő a szerverén tárolt fájlban szereplő ügyféladatokat a fenti módszerrel minden egyes adatfrissítés esetén kinyomtatja és azokat lefűzi egy mappába. Ezzel a módszerrel a fájlban tárolt ügyféladatok, köztük az érzékeny és kockázatos adatkezelést eredményező ügyfélkapus adatok illetéktelen, jogosulatlan megismerésének esélye növekszik. A listák kinyomtatása azonban az adatok kezelésének célja és biztonsága szempontjából semmilyen plusz, értékelhető hozzáadott értéket nem képvisel, gyakorlatilag egy felesleges további adatkezelési műveletet eredményez. A lista kinyomtatása és lefűzése ezért az általános adatvédelmi rendelet 32. cikk (1) bekezdésében és különösen annak b) pontjában előírt bizalmasság garantálása ellen ható intézkedés.

A Hatóság megítélése szerint az ügyféladatok tisztán elektronikus tárolása és azokról tisztán elektronikus biztonsági mentés készítése jobban garantálja az adatbiztonság követelményét és így a 32. cikk (1) bekezdésének való megfelelést. Ezzel az intézkedéssel az ügy tárgyát képező incidensek bekövetkezésének esélye és az adatkezelés kockázata is csökkenthető, így az Ügyfél a 32. cikk (2) bekezdésében foglaltaknak is megfelelőbb módon tud eleget tenni.

A lista kinyomtatása ellen szóló további érv, hogy a papír alapú adatkezelésből fakadó adatvédelmi incidens pontos körülményeit, így hogy a lista pontosan hogyan kerülhetett ki az Ügyfél kezeléséből, azóta sem sikerült teljes körűen feltárni. Ezen papír alapú adatkezelés így az esetlegesen az Ügyfélnél előforduló más, hasonló adatvédelmi incidensek észlelését és pontos okaik feltárását is hátráltathatta.

A Hatóság ezért megállapította, hogy az Ügyfél nem tett eleget az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseiben foglaltaknak, amikor a kezelt személyes adatok bizalmassága ellen ható felesleges intézkedésként az elektronikusan rendelkezésre álló és naprakész ügyféladatokat papír alapon is tárolta visszamenőleg.

2) A Hatóság végül az ügy kapcsán azt is megállapítja, hogy az Ügyfél adatvédelmi incidenskezelési szabályzata hiányos tartalommal került elfogadásra. Az incidenskezelési szabályzat ugyanis nem tartalmazza egyáltalán, hogy az észlelt adatvédelmi incidenseket mely esetekben kell bejelenteni a felügyeleti hatóságnak.

Az adatvédelmi incidensek kezelésével kapcsolatban az általános adatvédelmi rendelet 33. cikk (1) bekezdése azt mondja, hogy azokat fő szabály szerint be kell jelenteni a felügyeleti hatóságnak, kivéve, ha az incidens nem jár kockázattal az érintettek jogaira és szabadságaira nézve. Az incidenskezelési szabályzatból a bejelentési kötelezettséggel kapcsolatos intézkedések nem hiányozhatnak, mivel a rendelet a bejelentést fő szabállyá teszi és attól csak kivételes esetekben lehet eltérni. Az Ügyfél által elfogadott szabályzat ettől függetlenül tartalmazza az incidensek kezelésének belső rendjét, a nyilvántartásba vételt és az érintettek tájékoztatására vonatkozó előírásokat, így csak a bejelentési kötelezettséggel kapcsolatban tekinthető hiányosnak.

Az Ügyfél tehát azzal, hogy kialakította belső incidenskezelési szabályzatát, értékelhető erőfeszítéseket tett az általános adatvédelmi rendelet 24. cikk (1)-(2) bekezdéseinek való megfelelés érdekében. Ennek keretében az adatkezelési tevékenységei vonatkozásában arányos, az adatkezelés biztonságának garantálása érdekében megtett technikai és szervezési intézkedések részeként belső incidenskezelési szabályzatot alkalmazott. A Hatóság értékeli ezen erőfeszítéseket, azonban a szabályzat a fentiekben kifejtettek alapján kiegészítésre szorul a 33. cikk (1) bekezdésében foglaltaknak való megfelelés érdekében.

A Hatóság ezért megállapította, hogy az Ügyfél nem teljeskörűen tett eleget az általános adatvédelmi rendelet 24. cikk (1)-(2) bekezdéseiben foglaltaknak, amikor a belső adatvédelmi incidenskezelési szabályzatában nem szabályozta a felügyeleti hatóságnak történő bejelentési kötelezettség esetkörét. Ezzel az Ügyfél megsértette a rendelet ezen rendelkezéseit.

c. Az érintettek ügyfélkapus hozzáférési adatai kezelésének célja, jogalapja, arányossága

Az Ügyfél által kezelt ügyfélkapus hozzáférési adatok kezelésének jogalapja, célja, az adatkezelés arányossága, illetve az érintetti tájékoztatás megfelelősége nem képezte a jelen eljárás tárgyát. Jelen határozat tárgya kizárólag az Ügyfél által alkalmazott adatbiztonsági és incidenskezelési kérdésekre terjed ki a bekövetkezett konkrét incidenssel kapcsolatban. Az Ügyfél és általánosságban más könyvelőirodák ügyfeleinek ügyfélkapus hozzáférési adatainak kezelése (mint az Ügyfél által állított bevett piaci gyakorlat) és az azzal kapcsolatban felmerülő további adatvédelmi kérdések a későbbiekben külön hatósági vizsgálat tárgyát képezhetik.

d. Az alkalmazott szankcióval kapcsolatos megállapítások.

A Hatóság megvizsgálta, hogy az Ügyféllel szemben milyen típusú szankciót kíván alkalmazni a feltárt jogsértések miatt és hogy indokolt-e vele szemben adatvédelmi bírság kiszabása. E körben a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján, figyelemmel az Infotv. 61. § (5) bekezdésére is, mérlegelte az ügy összes releváns körülményét és megállapította, hogy a jelen eljárás során feltárt jogsértés esetében az Ügyfél figyelmeztetése és

felszólítása önmagában nem arányos és visszatartó erejű szankció, indokolt tehát a bírság kiszabása. A bírságkiszabás szükségességének megállapítása során a Hatóság azt vette mindenekelőtt figyelembe, hogy az Ügyfélnél bekövetkezett adatvédelmi incidens egy olyan adatbiztonsági hiányosságra vezethető vissza, amely nem csak a konkrétan nyilvánosságra került személyes adatok, hanem valamennyi az ügyfél által papír alapon kezelt ügyfélkapus elérhetőségek és egyéb ügyféladatok biztonságát veszélyeztethette. A Hatóság ezért az ügyfelek belépési egy más személyes adatainak nem biztonságos kezelését, és a vonatkozó adatbiztonsági intézkedések elégtelen voltát rendszerszintű problémának tekinti, amely alapján a jogsértő helyzet már az incidens bekövetkezése előtt is fennállt az adatkezelő Ügyfélnél.

Az adatvédelmi incidenskezelési szabályzat bejelentéssel kapcsolatos hiányossága szintén olyan rendszerszintű problémának tekinthető, amely hátráltathatta más, a hatósági ellenőrzés és eljárás megindítása előtt bekövetkezett incidensnek az általános adatvédelmi rendeletnek megfelelő kezelését. Ennek keretében különösen azt, hogy a Hatóság a kockázatos megítélésű, az Ügyfélnél bekövetkezett incidensekről a rendelet 33. cikk (1) bekezdése alapján tudomást szerezzen.

A Hatóság a bírság összegének meghatározása során figyelembe vette, hogy az Ügyfél által elkövetett jogsértések az általános adatvédelmi rendelet 83. cikk (4) bekezdése szerint az alacsonyabb maximális összegű bírságkategóriába tartozó jogsértésnek minősülnek. Emellett a bírság összegének meghatározása során az alábbi releváns tényezőket vette figyelembe.

A bírság összegének megállapítása során figyelembe vette a Hatóság, hogy az Ügyfélnek a 2018. január 1. – 2018. december 31. közötti általános üzleti évet záró beszámolója alapján ebben az évben összesen […] nettó árbevétele volt. A fentiek alapján a kiszabott bírság összege a jogsértés súlyával arányban áll.

A Hatóság az Ügyféllel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést.

Enyhítő körülményként vette figyelembe a Hatóság, hogy a bekövetkezett adatvédelmi incidensről való értesülése után az Ügyfél az incidens kezelésével kapcsolatos szinte valamennyi, az általános adatvédelmi rendelet 33-34. cikkei által előírt intézkedést azonnal megtette, így az incidenst kivizsgálta, további adatbiztonsági intézkedések megtételéről határozatott, az érintetteket tájékoztatta és az incidenst nyilvántartásba vette. Az adatvédelmi incidensek bejelentésével kapcsolatos szabályozás hiányosságain túl a Hatóság így az Ügyfél konkrét adatvédelmi incidenskezelési gyakorlatában további problémát nem tárt fel. Az incidenskezelési szabályzat hiányát azonban rendszerszintű problémaként értékelte a Hatóság.

Súlyosító körülményként értékelte a Hatóság, hogy a megállapított adatbiztonsági hiányosságok egy magas kockázatú adatvédelmi incidens bekövetkezéséhez vezettek, amelynek eredményeképpen körülbelül 100 természetes személy személyes adatai (köztük személyazonossággal való visszaélésre alkalmas adatok) kerültek nyilvánosságra. A hiányosság így az érintettek jogai és szabadságaira jelentett kockázatok szempontjából magas besorolású incidenst eredményezett, amelyről az Ügyfél is csak a Hatóság eljárása kapcsán értesült.

A Hatóság azt is figyelembe vette, hogy az Ügyfél az incidensről való tudomásszerzés után viszont azonnal további adatbiztonsági intézkedések megtételét indítványozta.

A Hatóság figyelemmel volt arra is, hogy az Ügyfél mindenben együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – kifejezetten enyhítő körülményként nem értékelte.

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, 2020. január 24.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár