Ügyszám: NAIH/2020/66/21

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) a **„ROBINSON-TOURS" Idegenforgalmi és Szolgáltató Kft. „f.a."** (székhely: 8230 Balatonfüred, Gombás köz 5., cégjegyzékszám: 19-09-501812) (a továbbiakban: Ügyfél 1. vagy adatkezelő) (képviseli: ECONO-GROUP Pénzügyi és Gazdasági Szakértő Kft., […] felszámoló, cím: 8200 Veszprém, Házgyári út 22/B.) adatkezelését és a **Next Time Media Ügynökség Kft.** (székhely: 1202 Budapest, Fiume u. 17., cégjegyzékszám: 01-09-294227) (a továbbiakban: Ügyfél 2. vagy adatfeldolgozó) adatfeldolgozását érintő adatvédelmi incidenssel kapcsolatban 2020. január 30. napján megindított hatósági ellenőrzés során feltárt körülmények miatt 2020. április 2. napján hivatalból megindított **adatvédelmi hatósági eljárásban**

I. Ügyfél 1. mint adatkezelő tekintetében

1) megállapítja, hogy

a) Ügyfél 1. 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) 25. cikk (1)-(2) bekezdéseiben foglalt beépített és alapértelmezett adatvédelem elvének, mivel a weboldala kialakításával nem megfelelően kiválasztott adatfeldolgozót bízott meg, ami súlyos, alapelvi szinten jogsértő és nem biztonságos adatkezelési tervezési hiányosságokhoz vezetett. A tervezési, kialakítási hiányosságok közvetlenül lehetővé tették azt, hogy az adatkezelés bizalmas jellegének sérülésével magas kockázatú adatvédelmi incidens következett be.

b) Ügyfél 1. nem tett eleget az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontjában foglalt kötelezettségének, amikor az általa kínált utazási szolgáltatásokkal összefüggésben kezelt személyes adatokat tároló rendszerét és honlapját úgy használta és üzemeltette, hogy ahhoz bárki hozzáférhetett az interneten keresztül egy sérülékenység fennállása miatt. Ezen hiányosság miatt az adatok kezelésének bizalmas jellege súlyosan sérült, ami közvetlenül lehetővé tette a magas kockázatú adatvédelmi incidens bekövetkezését.

c) Ügyfél 1. nem tett eleget az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján fennálló tájékoztatási kötelezettségének a bekövetkezett adatvédelmi incidenssel kapcsolatban, amikor nem tájékoztatta a magas kockázatú adatvédelmi incidensről az érintetteket.

2) utasítja Ügyfél 1-et, hogy a jelen határozat véglegessé válásától számított 15 napon belül tájékoztassa az érintetteket a bekövetkezett incidens tényéről és körülményeiről, az érintett személyes adatok köréről és az elhárítás érdekében megtett intézkedésekről,

3) a fenti jogsértés miatt Ügyfél 1-et a **jelen határozat véglegessé válásától számított 30 napon belül**

20.000.000 Ft, azaz húszmillió forint

adatvédelmi bírság megfizetésére kötelezi;

II. Ügyfél 2. mint adatfeldolgozó tekintetében

1) megállapítja, hogy Ügyfél 2. nem tett eleget az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontjában foglalt kötelezettségének, amikor az incidenssel érintett adatbázishoz bárki hozzáférhetett az interneten keresztül egy sérülékenység fennállása miatt, így az adatok feldolgozásának bizalmas jellege súlyosan sérült. Ennek oka, hogy Ügyfél 2. a weboldal üzemeltetése során az érintett teszt- és éles adatbázisok közötti kapcsolatot nem szüntette meg, továbbá a weboldalt nem vetette alá megfelelő biztonsági ellenőrzéseknek, sérülékenységi teszteknek. A mulasztás közvetlenül lehetővé tette a személyes adatok elérhetőségét és így az adatvédelmi incidens bekövetkezését.

2) a fenti jogsértés miatt Ügyfél 2-őt a **jelen határozat véglegessé válásától számított 30 napon belül**

500.000 Ft, ötszázezer forint

adatvédelmi bírság megfizetésére kötelezi;

III. elrendeli a végleges határozatnak Ügyfél 1. és Ügyfél 2. azonosító adatainak közzétételével történő **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/2020/66 BÍRS. számra kell hivatkozni.

Az I./2) pontban előírt intézkedések megtételét Ügyfél 1-nek az intézkedés megtételétől számított 15 napon belül kell írásban – az azt alátámasztó bizonyítékok előterjesztésével együtt – igazolnia a Hatóság felé.

Amennyiben Ügyfél 1. és Ügyfél 2. 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 I./2) pont szerinti kötelezés nem teljesítése, illetve a bírság és a késedelmi pótlék meg nem fizetése esetén a Hatóság elrendeli a határozat, a bírság és a késedelmi pótlék végrehajtását.

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

megtámadható. A veszélyhelyzet a keresetindítási határidőt nem érinti. A keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak. A tárgyalás tartása iránti kérelmet a keresetlevélben jelezni kell. A veszélyhelyzet ideje alatt a bíróság tárgyaláson kívül jár el. A teljes személyes illetékmentességben nem részesülők számára a közigazgatási per illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

INDOKOLÁS

I. Előzmények és a tényállás tisztázása

1) A Hatósághoz 2019. december 29-én közérdekű bejelentés érkezett, amely arra hívta fel a figyelmet, hogy a https://www.lastminute.robinsontours.hu/partnerkapu_foglalasaim weboldalon keresztül bárki számára elérhetőek Ügyfél 1. természetes személy ügyfeleinek személyes adatai, így többek között utasok neve, elérhetőségei, lakcímadatok, személyi igazolvány és útlevélszámok, foglalással és utazással, úticéllal, szállással valamint a szerződéskötéssel kapcsolatos adatok. Az adatok https://www.robinsontours.hu/partnerkapu_foglalasaim linken keresztül is elérhetőek voltak. A bejelentés szerint erre a bejelentő úgy jött rá, hogy internetes böngészés közben édesapja nevét írta be a Google keresőjébe, majd az egyik találaton keresztül, bármilyen jogosultság ellenőrzés nélkül sikerült megnyitnia egy adatbázist.

A Hatóság ellenőrizte a fenti linkeket és NAIH/2020/66/2., NAIH/2020/66/3. és NAIH/2020/66/5. ügyiratszámú feljegyzéseiben megállapította, hogy a linkek birtokában, azt a webböngészőbe beírva, bármilyen jogosultságellenőrzés, vagy más informatikai biztonsági intézkedés közbeiktatása nélkül a weboldalon – a bejelentő által állítottaknak megfelelően – elérhető egy adatbázis, amely különböző természetes személy ügyfelek személyes adatait tartalmazza. Az adatbázisban található adatok alapján valószínűsíthető, hogy a legtöbben az utazási irodaként működő Ügyfél 1. utazási szolgáltatásait igénybe vevő ügyfelek. A Hatóság arról is meggyőződött, hogy az adatbázisban tárolt adatokhoz a Google keresőben rákeresve (pl. egy utas nevére való keresés) is el lehet jutni. A tartalmakat tehát a Google keresőmotorja is felderítette, és abban ezeket kulcsszavas kereséssel elérhetővé tette.

Az elérhető személyes adatok a következőek:

- „vezérutas” neve,
- útitársak száma és neve,
- indulás és érkezés dátuma, foglalás dátuma,
- foglalás státusza (végleges/törölt/lekérés alatt),
- foglalási szám,
- lakcímadatok (ország, irányítószám, település, utca, házszám, emelet, ajtó pontossággal),
- személyi igazolvány száma kiállítási és lejárati dátummal együtt,
- útlevél száma kiállítási és lejárati dátummal együtt,
- e-mail cím, telefonszám,
- utazási szerződés készítésének dátuma.

A honlapon a személyeket úticél és dátum alapján is lehetséges volt szűrni. Az adatbázisban ezen felül az egyes ügyfelekhez lehetősége van bárkinek útlevél fotót feltölteni, illetve megjegyzést írni az egyes foglalások mellé. Az útlevél fotó feltöltés lehetőségét választva nem csak képeket, hanem gyakorlatilag bármilyen formátumú fájlt ki lehetett választani feltöltésre.

A linkeken keresztül megtekinthető táblázat összesen 375 rekordot tartalmazott. Ezek között voltak valószínűsíthetően fiktív személyek is (pl.: „TESZT TESZT”, „TESZT IVÁN” stb.), azonban többségük létező természetes személy ügyfeleket takart. Az útitársak száma és neve alapján ennél azonban sokkal több, ezer feletti személy adatai is elérhetőek voltak a honlapon keresztül.

A linkeken keresztül elérhető adatbázisból lehetőség volt arra is, hogy az egyes ügyfelekkel kötött utazási szerződéseket bárki szabadon letölthesse pdf formátumban. Az egyes szerződések közül a Hatóság eljáró ügyintézője bizonyítékul letöltött öt darabot, valamint egy e-mail-es foglalási igazolást is. A letölthető szerződések részletesen tartalmazták valamennyi szerződő utas személyes adatait, az úticélt, az utazás dátumát, a lefoglalt szállás adatait és a szolgáltatás bruttó árát személyekre bontva.

A Hatóság a fentiekre tekintettel hatósági ellenőrzést indított 2020. január 30-án, mivel a rendelkezésre álló adatok nem voltak elegendőek annak megítéléséhez, hogy Ügyfél 1. maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak.

2) A későbbi napokon (2020. február 3.) történő, NAIH/2020/66/7. számú feljegyzéssel dokumentált újraellenőrzés szerint a nyilvánosan elérhető adatbázishoz folyamatosan újabb rekordok, benne személyes adatokkal és kapcsolódó szerződésekkel kerültek hozzáfűzésre, feltöltésre. Az ügyféladatbázis frissülése tehát ily módon élőben követhető volt a honlapon keresztül. Az adatbázis 2020. február 4-én már nem volt viszont ily módon elérhető.

A Hatóság NAIH/2020/66/4. számú végzésével nyilatkozattételre és iratszolgáltatásra szólította fel Ügyfél 1-et, amelyet az a visszaérkezett tértivevény tanúsága szerint 2020. február 4-én vett át.

Az Ügyfél 1. a fenti végzésre határidőben megküldött nyilatkozatához csatoltan egyben megküldte a Hatóság honlapjáról letöltött minta alapján kitöltött adatvédelmi incidens-bejelentését.

Az incidensbejelentés és a végzésre adott válaszok alapján Ügyfél 1. úgy nyilatkozott, hogy az említett linkeken keresztül valóban utazási irodai szolgáltatásait igénybe vevő ügyfelei adatai voltak elérhetőek. A valódi természetes személyek mellett az adatbázisban szerepeltek tesztelésre létrehozott, fiktív személyek is. Ügyfél 1. az adatok rögzítésének célját az egyes utazásokat lefoglaló, valamint a ténylegesen utazó érintettek azonosításában jelölte meg, amelyre azért van szüksége, hogy az érintett és Ügyfél 1. között létrejövő megállapodásokat vissza tudja keresni és a teljesítés kapcsán fel tudja venni az érintettekkel a kapcsolatot. Az adatbázishoz kizárólag olyan Ügyfél 1-gyel szerződött partnerek képviselői léphettek be, akikkel Ügyfél 1-nek érvényes szerződése volt.

Az adatbázisban található adatokat Ügyfél 1. dedikált szerveren, strukturáltan, SQL formátumban tárolta. Ügyfél 1. Ügyfél 2-őt, mint adatfeldolgozót bízta meg a tárhelyszolgáltatói, programozói, rendszergazdai, informatikai szolgáltatói feladatokkal. Az adatok Ügyfél 2. szerverein tárolódtak, amelynek pontos helye a 1143 Budapest, Ilka u. 31. alatti Invitech szerverteremben található. Az adatok biztonsága érdekben Ügyfél 2. adatfeldolgozóként az alábbi intézkedéseket foganatosította: tűzfal, vírusirtó, többszintű azonosítási és hozzáférési jogosultság ellenőrzés, erős jelszavak használata és kikényszerített cseréje, napi szintű biztonsági mentés az adatbázisról, naplózás az adatokkal történt műveletekről.

Ügyfél 1. közölte, hogy nem rendelkezett a Hatóság NAIH/2020/66/4. számú végzésének kézhezvétele előtt tudomással az adatvédelmi incidensről, mivel azt nem jelezték neki sem üzleti

partnerei, sem adatfeldolgozója vagy bármely más érintett, továbbá saját működése során sem észlelte azt. Az incidensről való tudomásszerzés után az azonban azonnal kivizsgálásra és bejelentésre került a Hatóság részére az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján, mivel Ügyfél 1. az incidens kivizsgálása után úgy ítélte meg, hogy az kockázatos az érintettek jogaira és szabadságaira nézve. Ügyfél 1. az adatvédelmi incidenst az az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján nyilvántartásba is vette.

Az incidens kiváltó okát Ügyfél 1. abban jelölte meg, hogy Ügyfél 2. által végzett weboldal fejlesztés közben létrejött egy tesztkörnyezet, amely a végső verzióból nem került eltávolításra. Ennek folyományaként a valós, éles adatok a tesztelésre használt adatállományba is bekerültek. Ez a valós adatokkal is folyamatosan frissülő tesztkörnyezet nem került levédésre. Ügyfél 1-nek nem volt tudomása ezen tesztkörnyezetről, azt ő nem is használta. Mivel Ügyfél 1. honlapján közvetlenül nem volt olyan hivatkozás található, amely a tesztkörnyezetre mutat, ezért azt csak a konkrét URL meghívásával lehetett elérni. Ennek alapján Ügyfél 1. valószínűsíti, hogy csak kevesen férhettek hozzá jogosulatlanul az adatokhoz.

Ügyfél 1. incidensbejelentése alapján a sérülékenység 2019. november 13-tól 2020. február 4-ig állt fent a honlapon keresztül. A sérülékenység összesen 781 érintett, összesen kb. 2506 darab személyes adatát érintette, amelyek: név, cím, születési dátum, útlevél száma és lejárati dátuma, személyi igazolvány száma és lejárati dátuma, e-mail cím, telefonszám, indulás és érkezés dátuma, valamint az egyes utazási szerződések pdf formátumban és az abban található adatok (pl. szerződéses érték). Az incidenssel érintett adatbázisban kiskorúak adatai is szerepeltek. Az érintettek személyi köre Ügyfél 1-nél 2019. november 13. és 2020. február 4. közötti időszakban utazásokat foglaló magyar nemzetiségű utasokat és idegenvezetőket ölelt fel.

A Hatóság végzésének kézhezvétele után Ügyfél 1. azonnal jelezte telefonon Ügyfél 2-nek a sérülékenységet, aki haladéktalanul intézkedett arról, hogy URL-eken keresztül ne lehessen a továbbiakban elérni az éles adatokkal frissülő tesztkörnyezetet. Ügyfél 1. megítélése szerint az adatvédelmi incidenst kiváltó sérülékenység összességében Ügyfél 2. nem körültekintő, gondos eljárásából fakadt. Ügyfél 1. továbbá közölte a Hatósággal, hogy az incidens miatt szabályozási anyagát felülvizsgáltatja. Ügyfél 1. azt is közölte, hogy az érintettek tájékoztatását tervezi a hatósági eljárás eredményéről, annak lezárását követően.

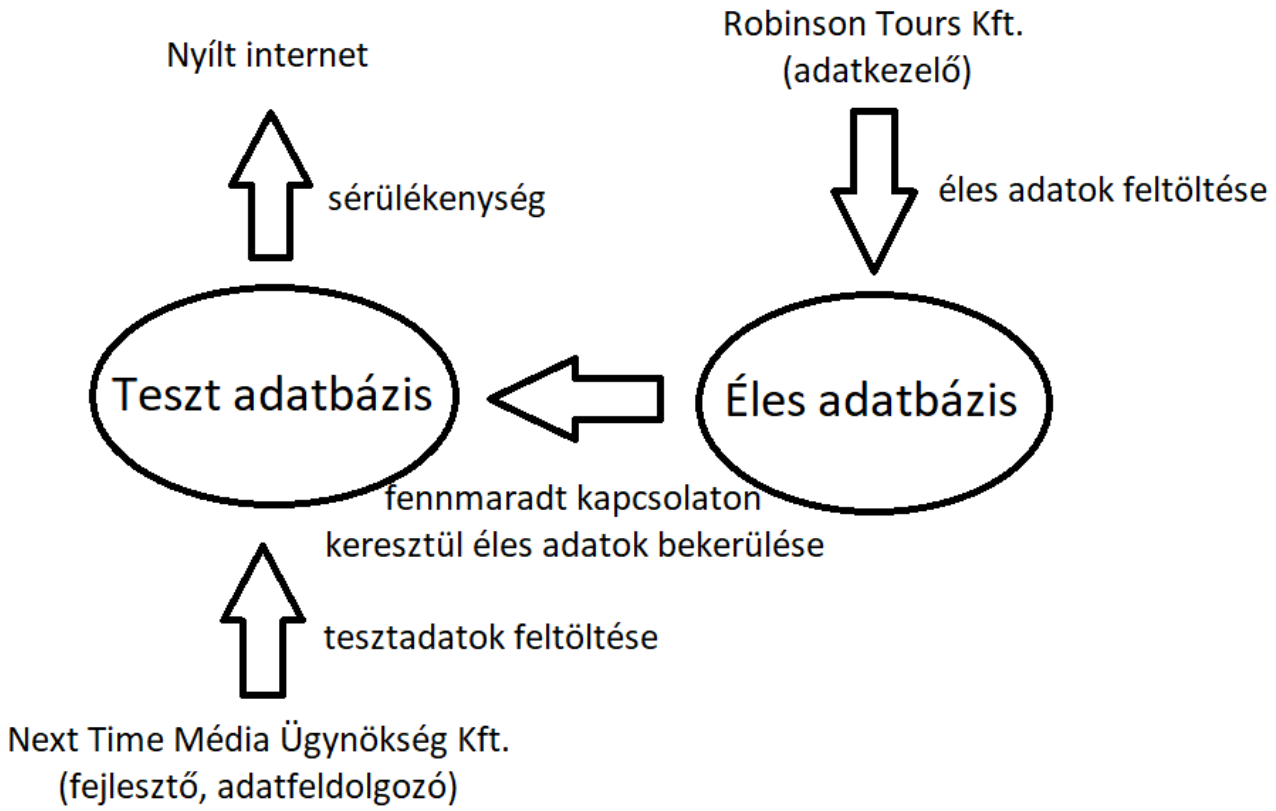
3) A Hatóság NAIH/2020/66/10. számú végzésével újabb nyilatkozattételre és iratszolgáltatásra szólította fel Ügyfél 1-et, amelynek az határidőben eleget tett.

Válaszai szerint az incidenssel érintett adatbázishoz hozzáférő szerződéses partnerek utazásközvetítői szerződést aláíró utazásközvetítők voltak. A velük kötött szerződés mintáját Ügyfél 1. csatolta válaszához. Az adatbázishoz összesen 307 utazásközvetítő férhetett hozzá, akik ott azonban adatot bevinni, módosítani nem tudtak. Minden utazásközvetítő csak a saját foglalásaihoz fért hozzá. Az adatbázisba kizárólag Ügyfél 1. volt jogosult adatokat felvinni.

Ügyfél 1. tájékoztatta a Hatóságot, hogy az incidenssel érintett adatbázishoz nem volt jogosultságellenőrzési rendszer kiépítve, ebből fakadt az adatvédelmi incidens bekövetkezése. Ügyfél 1. azonban azóta felhasználónév és jelszó alkalmazását rendelte el a rendszerben, a továbbiakban ezzel hozzáférhető csak az arra felhatalmazott munkatársak részére az adatbázis. Jelszókezelési szabályzatát Ügyfél 1. ismertette válaszában.

Ügyfél 1. ismertette, hogy a sérülékenység fennállásának időszakában (2019. november 13. – 2020. február 4.) összesen két IP címről[1] történt külső, jogosulatlan hozzáférés 28 darab foglalás összesen 30 db dokumentumához, négy alkalommal (2020. január 30. és 31., továbbá február 1. és 3. napjain). Kimutatható adatvédelmi incidens így ténylegesen ezen alkalmakkal kapcsolatban valósult meg.

Ügyfél 1. kifejtette, hogy a fejlesztés során létrejött tesztkörnyezet és ahhoz tartozó tesztadatbázis – tekintve, hogy a tesztelés nem éles adatokkal történt – nem került levédésre. A tesztelés végén az adatállomány azonban nem került törlésre és kapcsolatban maradt a különálló, immár éles rendszerrel és adatbázissal is. Az éles rendszerbe Ügyfél 1. által bevitt személyes adatok a tesztadatbázisba is átkerültek, mivel a két rendszer között fennmaradt egy adatkapcsolat. A sérülékenységen keresztül az éles adatokkal is folyamatosan frissülő tesztadatbázis volt elérhető (lásd az alábbi ábrát).



A sérülékenységen keresztül elérhető adatbázisban összesen 309 darab utazási szerződéshez lehetett hozzáférni. Ezek a korábbiakban ismertetett szerint összesen 781 érintett, összesen kb. 2506 darab személyes adatát tartalmazták. Az érintettek közül összesen 46 volt gyermekkorú (18 éven aluli).

[1] Ügyfél 1. által kimutatott […] számú IP címről a Hatóság eljáró ügyintézője megállapította, hogy az a Hatóság internet-előfizetésének IP címe. Az ezen IP címhez kapcsolható adatbázis hozzáférések ezért a hatósági ellenőrzés keretei között végrehajtott, hivatalos feljegyzésekben dokumentált lekérdezésekhez köthetőek nagy valószínűséggel (lásd: NAIH/2020/66/13. sz. feljegyzés).

Ügyfél 1. arról is nyilatkozott, hogy az elérhető felületen keresztül az „útlevél másolat feltöltés” lehetőségen keresztül nem lehetett kívülről adatot feltölteni, mivel azt kizárólag az éles rendszerbe tudtak feltölteni Ügyfél 1. munkatársai pdf vagy jpeg formátumban. Az éles rendszer vírusvédelemmel rendelkezett.

Ügyfél 1. a Hatóság felhívására csatolta válaszához Ügyfél 2-vel kötött adatfeldolgozói szerződését („adatfeldolgozási megállapodás”, […]). A szerződést 2019. április 10-én kötötte meg egymással Ügyfél 1. és Ügyfél 2. A szerződés 4. pontja szerint az adatfeldolgozás biztonságának garantálása és a kockázatokkal arányos intézkedések megtétele, valamint ezekben az adatkezelő támogatása az adatfeldolgozó (Ügyfél 2.) feladata és kötelessége. Az adatfeldolgozó feladata a személyes adatok véletlen vagy jogellenes megsemmisülésének, módosításának, engedély nélküli hozzáférhetővé tételének, vagy azokhoz való engedély nélküli hozzáférésnek a megakadályozása. Ennek érdekében köteles a kockázatokkal arányos szervezési és technikai intézkedéseket megtenni. Az adatfeldolgozó az adatokhoz történő illetéktelen személyek általi hozzáférést köteles megakadályozni, ezen kötelezettség szándékos vagy gondatlan megsértéséből eredő kárért felelősséggel tartozik. Adatfeldolgozó köteles folyamatosan figyelemmel kísérni az általa alkalmazott intézkedéseket az adatvédelmi jogi megfelelés érdekében.

4) A Hatóság NAIH/2020/66/12. számú végzésével újabb nyilatkozattételre és iratszolgáltatásra szólította fel Ügyfél 1-et, amelynek az határidőben eleget tett.

Válaszához csatolva Ügyfél 1. megküldte a jogosulatlan hozzáféréseket részletesen kimutató táblázatot, amely alapján megállapítható, hogy az összes dokumentum-hozzáférés közül 26 esetben a Hatóság IP címéről, a hatósági ellenőrzés keretein belül töltöttek le dokumentumokat (2020. január 30. és 31., továbbá február 1. és 3. napjain). A maradék négy dokumentum-hozzáférés nem a Hatóság IP címéhez köthető.

Ügyfél 1. a fentieken túl megküldte az Ügyfél 2-vel megkötött „Komplex informatikai rendszer fejlesztése” tárgyú 2019. április 10-én kelt szerződést másolatban, amelyhez kapcsolódóan kötötte meg szintén ezen dátummal a már hivatkozott „adatfeldolgozási megállapodást”. A szerződés alapján ennek keretei között fejlesztette ki Ügyfél 2. az utazásfoglalások nyilvántartására és adminisztrációjára az incidensben érintett rendszert és adatbázist. A fejlesztett rendszer és annak keretében az adatbázis célja az volt, hogy abban az Ügyfél 1-el szerződött partnerek által közvetített utazási szolgáltatásokat igénybe vevő érintettek személyes adatai (azonosító adatok, elérhetőségek, úticéllal és utazással kapcsolatos adatok, szerződések, okmányadatok stb.) kerüljenek tárolásra és kezelésre.

5) A tényállás további tisztázásán túl az ügyben az általános adatvédelmi rendeletben foglalt kötelezettségek Ügyfél 1. általi feltételezhető megsértésének további szükséges vizsgálata miatt az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 60. § (1) bekezdésére tekintettel, a Hatóság a rendelkező részben foglaltak szerint adatvédelmi hatósági eljárás megindításáról döntött. Erről a Hatóság 2020. április 2-án kelt NAIH/2020/66/14. ügyiratszámú értesítésével értesítette az Ügyfél 1-et, amelyet az 2020. április 6-án vett át.

6) A Hatóság NAIH/2020/66/16. számú, 2020. május 11-én kelt végzésével értesítette Ügyfél 2-őt arról, hogy ügyfélként bevonja az adatvédelmi hatósági eljárásba az általános adatvédelmi rendeletben foglalt kötelezettségek feltételezhető megsértésének vizsgálata miatt, egyben felhívta nyilatkozattételre és iratszolgáltatásra. Ügyfél 2. a végzésre határidőben válaszolt.

Ügyfél 2. nyilatkozata alapján az incidenssel érintett tesztadatbázis – amelyen keresztül a személyes adatok elérhetővé váltak az interneten keresztül – időközben törlésre került. Az érintett rendszert ezen felül Ügyfél 2. átköltöztette egy zártabb, biztonságosabb rendszerbe. Ez a művelet a válaszadáskor még folyamatban volt.

Ügyfél 2. nyilatkozata alapján korábban a rendszer biztonságát érintő, „autentikációs ellenőrzések" csak a belépési pont körül történtek meg. A Hatóság azirányú kérdésére, hogy az érintett rendszer biztonsági célú felülvizsgálata milyen időközönként történik meg, Ügyfél 2. csupán annyit közölt, hogy az incidenssel érintett weboldal védelme fix, egyébként a „webes világból érkező hírek és napi történések" alapján tájékozódik arról, hogy a védelmi intézkedéseket frissíteni kell-e.

A Hatóság azon kérdésére, hogy weboldal mögötti foglalási adatbázis teszt verziója miért nem került korábban törlésre, Ügyfél 2. azt válaszolta, hogy véleménye szerint a törlésnek nincs értelme, mivel bármikor előfordulhat, hogy „valamit fejleszteni kell", „meg kell oldani valamit" így „soha sincs vége a tesztelésnek". A teszt és az éles adatbázis közötti kapcsolódási pont megszüntetésével kapcsolatban Ügyfél 2. azt nyilatkozta, hogy véleménye szerint az nem lényeges kérdés, mivel a jogosultság ellenőrzés (hiánya) képezte a hiba forrását.

7) A Hatóság NAIH/2020/66/19. számú végzésével újból felhívta nyilatkozattételre és iratszolgáltatásra Ügyfél 2-őt, amely a végzésre határidőben válaszolt.

Ügyfél 2. nyilatkozata alapján jelenleg nem rendelkezik Informatikai Biztonsági Szabályzattal és Adatvédelmi Szabályzattal.

Ügyfél 2. az incidenssel érintett rendszer (a weboldal), általa hivatkozott „autentikációs ellenőrzéseiről" nem rendelkezik jegyzőkönyvvel, azokat nem dokumentálta.

Ügyfél 2. továbbá nyilatkozott arról, hogy az incidenssel érintett adatbázishoz való jogosulatlan hozzáféréseket naplózó logadatok 30 napos időintervallumban íródnak felül. Mire Ügyfél 2. megkapta a megkeresést (Ügyfél 1-től), hogy ezekre szükség van, már csak a 2020. január 24. – 2020. február 10. közötti hozzáférések naplóját tudta lementeni. Ezt megküldte Ügyfél 1-nek, amelyet az pedig továbbított a Hatóságnak a NAIH/2020/66/12. számú korábbi végzésre adott válaszához mellékelve. Ennek eredményeképpen tájékoztatta Ügyfél 1. arról a Hatóságot, hogy csupán 2020. január 30. és 31., továbbá február 1. és 3. napjain történtek külső hozzáférések az adatbázishoz.

8) A Hatóság NAIH/2020/66/18. számú végzésével nyilatkozattételre hívta fel Ügyfél 1-et, amelyben többek között kérte, hogy nyilatkozzon arról, hogy 2019. évi üzleti évben mekkora összeg volt az értékesítése nettó árbevétele.

Ügyfél 1. bejegyzett székhelyéről a fenti végzés két alkalommal való ismételt postázás után is „nem kereste" jelzéssel érkezett vissza a Hatósághoz. A Hatóság időközben a cégnyilvántartásban szereplő adatokból értesült arról, hogy Ügyfél 1. 2020. június 16-tól kezdve felszámolás alatt áll. Ügyfél 1. 2019 és 2020 évi gazdálkodására vonatkozó adatok pedig időközben közzétételre kerültek az Elektronikus Beszámoló Portálon.

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 az adatvédelmi incidenssel érintett adatkezelésre az általános adatvédelmi rendeletet kell alkalmazni.

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

Az általános adatvédelmi rendelet 5. cikk (1) bekezdés f) pontja szerint a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

Az általános adatvédelmi rendelet 25. cikk (1) bekezdése szerint az adatkezelő 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 mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Az általános adatvédelmi rendelet 25. cikk (2) bekezdése szerint az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

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

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

Az általános adatvédelmi rendelet 33. cikk (1) 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 adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

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

Az általános adatvédelmi rendelet 34. cikk (4) bekezdése alapján, ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a (3) bekezdésben említett feltételek valamelyikének teljesülését.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2. § (2) bekezdése szerint az általános adatvédelmi rendeletet az ott megjelölt rendelkezésekben foglalt kiegészítésekkel kell alkalmazni.

Az Ákr. 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 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 általános adatvédelmi rendelet 5. cikkének megsértése esetén a kiszabható bíróság felső határa az általános adatvédelmi rendelet 83. cikk (5) bekezdés a) pontja alapján a 20 000 000 eurónak (EUR), illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeg.

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

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

III. Döntés

1. Az adatvédelmi incidens kezelése, magas kockázati besorolása és bejelentése

Az adatvédelmi incidenst kiváltó sérülékenységről Ügyfél 1. saját elmondása szerint először a Hatóság NAIH/2020/66/4. ügyiratszámú tényállástisztázó végzéséből 2020. február 4-én szerzett tudomást. Korábban a sérülékenységről és az adatvédelmi incidensről nem volt tudomása. Ügyfél 1. utazási szolgáltatásait igénybe vevő érintettek adatait is tartalmazó adatbázishoz való hozzáférést Ügyfél 1-nek nem sikerült magától detektálnia, így az incidensről és azt lehetővé tévő sérülékenységről pusztán a Hatóság jelzése alapján értesült.

Az általános adatvédelmi rendelet 4. cikk 12. pontja alapján adatvédelmi incidensnek minősül a biztonság sérülése, amely a kezelt személyes adatokhoz való jogosulatlan hozzáférést eredményezi. A fogalom szempontjából így a biztonsági eseménnyel való kapcsolat kulcselemnek tekinthető. A Hatóság a közérdekű bejelentő által nyújtott információk alapján több hozzáférést is eszközölt az adatbázishoz a sérülékenységen keresztül, továbbá később Ügyfél 1. incidensbejelentésben is elismerte a sérülékenységet. Ügyfél 1. által fenntartott honlapon keresztül elérhető sérülékenység kihasználásával volt tehát lehetőség az érintetti adatokhoz való hozzáféréshez. A személyes adatok jogosulatlan megismerésére tehát egy informatikai biztonsági hiányosság kihasználásával kerülhetett sor, amely így több esetben is adatvédelmi incidenst eredményezett. Ezek közül az illetéktelen hozzáférések közül a Hatóság is több esetet dokumentált hivatkozott feljegyzéseiben.

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

Az általános adatvédelmi rendelet (75) preamubulumbekezdése az olyan adatok kezelését, amelyekből személyiség-lopás, vagy személyazonossággal való visszaélés fakadhat, továbbá kiemelten a gyermekek adatainak kezelését az érintett személyek jogaira és szabadságaira nézve alapvetően kockázatos adatkezelésnek tekinti. A Hatóság azt is kiemeli, hogy az utazási szerződésekben található adatokból, így az utazás idejéből, céljából, továbbá a szerződés

értékéből további következtetések vonhatóak le az adott utas anyagi körülményeire nézve is. Ezen felül a szintén elérhető lakcímadatokkal összevetve az érintett otthontartózkodására is következtetést lehet levonni. Ezen adatok együttes kezelése összevetve az incidens körülményeivel a Hatóság megítélése szerint magas kockázatú adatvédelmi incidenst eredményezett.

Az érintett természetes személyek magánszférájára jelentett magas kockázat szempontjából további fontos körülmény, hogy Ügyfél 2. (adatfeldolgozó) nyilatkozata alapján az érintett adatbázishoz való külső, jogellenes hozzáféréseknek csak a 2020. január 24. – 2020. február 10. közötti naplóját tudta lementeni. A sérülékenység teljes fennállási ideje (2019. november 13. – 2020. február 4.) alatti illetéktelen hozzáférések pontos száma így nem ismert, azonban a 2019. december 29-i a Hatóságnak küldött közérdekű bejelentés tartalma alapján ilyenre korábban is sor került már, legalább a közérdekű bejelentő által. A sérülékenység fenti hosszabb ideig tartó fennállása is növelte a kockázatokat.

A Hatóság a fentiekre tekintettel szintén a magas kockázatot megalapozó körülményként értékeli, hogy az adatbázishoz mind a közérdekű bejelentő, mind a Hatóság hozzáfért, viszont az illetéktelen hozzáférések teljes száma és a hozzáférők személye a sérülékenység idejére vonatkozó teljes naplóállomány hiányában nem mérhető pontosan fel. A hozzáférők személyét és számát Ügyfél 1. utólag már nem tudja felmérni és azonosítani, amely az incidensben érintett személyes adatok további sorsával kapcsolatban nagyfokú bizonytalanságra, aggodalomra ad okot. Az adatkezelő az általa felmérhetetlen fokú és mértékű, de bizonyítottan megtörtént adatszivárgásnál csak az érintettek tájékoztatásával próbálhatja meg csökkenti jelen esetben az egyébként is magas kockázatokat.

A Hatóság megítélése szerint a magas kockázatot megalapozó további körülmények, hogy az adatbázisban kezelt személyes adatokat a Google is indexálta, azok ezen keresőmotoron keresztül is elérhetőek voltak, így azokra sokkal könnyebben rá lehetett akár egyszerű internetes böngészés, névre történő találomra való rákeresés során is bukkanni.

A fentiek alapján a Hatóság megítélése szerint az adatvédelmi incidens magas kockázatúnak tekinthető, ezért amennyiben egy ilyen esetről az adatkezelő tudomást szerez, úgy azt be kell jelentenie az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján a felügyeleti hatóságnak. A bejelentést az Adatkezelő 2020. február 6-án e-mailben tette meg a Hatóság felé, miután arról a Hatóság tényállás tisztázó végzéséből tudomást szerzett annak 2020. február 4-i kézhezvételét követően. Az adatkezelő így bejelentési kötelezettségét az incidens tudomására jutásától számított 72 órán belül teljesítette. A Hatóság a bejelentési kötelezettség teljesítésével kapcsolatos jogsértést ezért nem állapított meg.

2. Az érintettek tájékoztatása az adatvédelmi incidensről

Ügyfél 1. incidensbejelentésében úgy nyilatkozott, hogy az érintettek tájékoztatását tervezi a hatósági eljárás eredményéről, annak lezárását követően. Ezen nyilatkozat, illetve a hatósági eljárás során a Hatóságnak küldött további nyilatkozatok alapján Ügyfél 1. jelen határozat meghozataláig nem tájékoztatta az érintetteket az adatvédelmi incidensről az általános adatvédelmi rendelet 34. cikke alapján.

Az általános adatvédelmi rendelet 34. cikk (1) bekezdése szerint az adatkezelő feladata, hogy indokolatlan késedelem nélkül tájékoztassa az érintetteket az adatvédelmi incidensről, ha az magas kockázatú incidensnek minősül.

A Hatóság megítélése szerint az incidens olyan magas kockázatúnak minősül, amely indokolja, hogy az általános adatvédelmi rendelet 34. cikk (1) bekezdése szerint arról az érintetteket is tájékoztassák, hiszen az olyan tovagyűrűző következményekkel járhat az érintettek magánéletére nézve, amelyre az adatkezelőnek már nincs ráhatása az általa elvégezhető incidenskezelés során (lásd a kockázati besorolásról jelen határozat előző, III./1. pontjában foglaltakat).

Az incidens kockázatai – az általános adatvédelmi rendelet (85)-(86) preambulumbekezdéseiben foglaltaknak megfelelően – csak úgy mérsékelhetők eredményesen, ha az érintettek erről tudomással bírnak, és megtehetik az általuk szükségesnek tartott további intézkedéseket.

Ügyfél 1. adatkezelőként felelősséggel tartozik azért, hogy a bekövetkezett adatvédelmi incidens kockázatait fel tudja mérni. Ennek oka, hogy elsősorban az adatkezelő van tisztában azzal, hogy milyen személyes adatokat, milyen célokból és adatkezelési módszereket alkalmazva kezel. Az adatvédelmi incidens esetleges magas kockázati besorolása és ezért arról az érintetti tájékoztatás szükségességének megítélése Ügyfél 1. fő feladata, ezen kérdés megítélését nem háríthatja át a „hatósági eljárás eredményeinek függvényeire” hivatkozva a felügyeleti hatóságra. Az adatkezelőnek az érintetteket indokolatlan késedelem nélkül kell tájékoztatnia az incidensről, amint a tudomására jutott az általános adatvédelmi rendelet 34. cikke alapján, nem várhat a hatósági eljárás lezárulásáig.

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

A fentiek alapján a Hatóság megállapítja, hogy Ügyfél 1. a tájékoztatás hiányával, elodázásával nem tett eleget az általános adatvédelmi rendelet 34. cikk (1) bekezdésében foglaltaknak, ezért a 34. cikk (4) bekezdésére tekintettel felszólította Ügyfél 1-et arra, hogy az érintetteket tájékoztassa a magas kockázatú adatvédelmi incidensről.

3. Az adatkezelés biztonságával kapcsolatos megállapítások

A Hatóság megvizsgálta azt is, hogy Ügyfél 1. mint adatkezelő és Ügyfél 2. mint adatfeldolgozó mennyiben tettek eleget az incidens bekövetkezésével közvetlenül összefüggő adatbiztonsági követelményeknek a már működő rendszer tekintetében.

Az általános adatvédelmi rendelet 32. cikk (1) bekezdésében foglaltak alapján az adatkezelőnek és az adatfeldolgozónak a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében a tudomány és technológia állásának megfelelő technikai és szervezési intézkedéseket kell végrehajtania, ide értve a rendelet a 32. cikk (1) bekezdés b) pontja alapján a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét.

Ezt az általános adatvédelmi rendelet 32. cikk (2) bekezdése is megerősíti, amikor kimondja, hogy 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 adatvédelmi incidenssel érintett rendszerben fennálló sérülékenység abból adódóan valósulhatott meg, hogy a személyes adatok kezelése során nem megfelelő biztonsági beállításokat alkalmaztak az érintett rendszerben az alábbiak szerint.

Ügyfél 2. a weboldal üzemeltetése során az érintett teszt- és éles adatbázis közötti kapcsolatot nem szüntette meg, továbbá a weboldalt nem vetette alá megfelelő biztonsági, sérülékenységi teszteknek. A tesztadatbázis és már valós adatokkal Ügyfél 1. által feltöltött és használt éles adatbázis között így fennmaradt egy kapcsolódási csatorna, amelyen keresztül az éles adatok folyamatosan, valós időben továbbításra kerültek a tesztadatbázisba. Ezt a valós idejű kapcsolatot Ügyfél 1. és Ügyfél 2. nyilatkozatai mellett a Hatóság által dokumentált próbaletöltések és hozzáférések is megerősítik.

A sérülékeny, éles adatokat tartalmazó tesztadatbázis azért volt elérhető a biztonsági résen keresztül, mivel annak biztonságával Ügyfél 2. a fejlesztés befejezése után már nem foglalkozott. Az incidens nem következett volna be, ha a tesztadatbázist Ügyfél 2. törli, vagy azt biztonságos környezetbe áthelyezi, vagy kapcsolatát az éles adatbázissal megszünteti. Ezek a mulasztások tehát közvetlenül lehetővé tették a személyes adatok elérhetőségét.

A tesztadatbázis a fentiek értelmében gyakorlatilag az éles adatbázis sérülékeny másolataként funkcionált, melynek mérete az idő előrehaladtával folyamatosan nőtt. Ez az ügyféladatok duplikálását eredményezte majd három hónapon keresztül. A személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt Ügyfél 1. vagy Ügyfél 2. észlelte volna.

Ügyfél 1. az általa kínált utazási szolgáltatásokkal összefüggésben kezelt személyes adatokat tároló rendszerét és honlapját a fentiek miatt úgy használta és üzemeltette, hogy ahhoz bárki hozzáférhetett az interneten keresztül egy sérülékenység fennállása miatt. Ezen biztonsági hiányosság miatt az adatok kezelésének bizalmas jellege súlyosan sérült, ami közvetlenül lehetővé tette a magas kockázatú adatvédelmi incidens bekövetkezését.

Ügyfél 1. is hivatkozott arra, hogy adatfeldolgozóként Ügyfél 2. nem járt el a rendszer kiépítése során elég körültekintően és gondosan, továbbá a rendszerhez nem volt jogosultságellenőrzési rendszer kiépítve.

A fentiekre tekintettel a Hatóság megállapítja, hogy

- Ügyfél 1. az adatok rendszerbe való betöltése és ottani kezelése, tulajdonképpen a rendszer használata,
- Ügyfél 2. a rendszer hanyag üzemeltetése és nem megfelelő biztonsági ellenőrzése és tesztelése révén,

megsértették az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját, mivel a szolgáltatás futása során annak bizalmas jellegét sem az adatkezelés, sem az adatfeldolgozás során nem tudták garantálni.

4. A beépített és alapértelmezett adatvédelem elvével kapcsolatos megállapítások

Az általános adatvédelmi rendelet 25. cikk (1)-(2) bekezdései tartalmazzák a beépített és alapértelmezett adatvédelem elvét, amely szerint az adatkezelés kockázatainak figyelembevételével olyan megfelelő technikai és szervezési intézkedéseket kell az adatkezelőnek végrehajtania az adatkezelés módjának meghatározásakor, amelyek célja az adatvédelmi elvek hatékony megvalósítása. Ezen felül szintén az adatkezelő feladata olyan megfelelő technikai és

szervezési intézkedések végrehajtása, amellyel biztosítja a kizárólag a konkrét cél szempontjából szükséges adatok kezelését. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

Az incidensben érintett, eredetileg tesztelési célból létrehozott adatbázishoz (amely később az éles adatokkal is folyamatosan frissült), a Google keresőjén keresztül és egyszerű internetes linkek birtokában bárki hozzáférhetett a 2019. november 13. – 2020. február 4. közötti időszakban.

Az adatbázisban tárolt adatok kezelése az előző pontokban kifejtetteknek megfelelően önmagában is magas kockázatú adatkezelést eredményezett, különös tekintettel a gyermekek és szerződéses adatok érintettségére. Az ilyen adatok kezelése során ezért az adatkezelők részéről fokozottan elvárható, hogy a magas kockázattal arányos technikai és szervezési intézkedéseket tegyenek már az adatkezelés tervezési időszakában az adatkezelés alapelveinek garantálása érdekében.

Az adatkezelés bizalmasságának garantálása az általános adatvédelmi rendelet 5. cikk (1) bekezdés f) pontjában is megjelenik. E szerint a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, bizalmassága például a jogellenes adatkezelés megelőzése érdekében.

A 25. cikk (1)-(2) bekezdései alapján így az adatkezelőknek az adatkezelés tervezése, módjának meghatározása során úgy kell eljárniuk, hogy a majdani adatkezelés megkezdésekor az az alapelveknek – pl. az integritás és bizalmas jelleg alapelvének is – megfelelő legyen.

Ügyfél 2. az incidenssel érintett adatkezelés bizalmasságának garantálása kapcsán kifejtette, hogy az általa fejlesztett rendszer (ami gyakorlatilag Ügyfél 1. weboldala) egészét a fejlesztés során nem tesztelte, nem vizsgálta biztonsági szempontból, csupán „a belépési pont körül” végzett ellenőrzéseket, az incidenshez vezető hibát így korábban nem észlelhette. Ügyfél 2. továbbá a lefolytatott ellenőrzésekről sem rendelkezik jegyzőkönyvekkel, amelyekkel megtörténtüket bizonyítani tudná. Ügyfél 1. megbízása keretei között Ügyfél 2. tehát elmulasztotta elvégezni a weboldal és a rendszer megtervezése és kifejlesztése során azon biztonsági teszteket, illetve más intézkedéseket, amelyekkel a sérülékenységhez vezető okok kiszűrhetőek vagy megszüntethetőek lettek volna (pl. weboldal sérülékenység vizsgálata, a teszt- és éles adatbázis fennmaradó kapcsolatának megszüntetése, a tesztkörnyezet nyílt elérhetőségének megszüntetése).

A fenti tervezési intézkedések hiánya lehetővé tette, hogy mind az oldalra mutató link ismeretében, mind a Google keresőjén keresztül bárki, bármilyen előzetes jogosultságellenőrzés nélkül hozzáférjen az online felületen tárolt személyes adatokhoz és dokumentumokhoz.

Az Európai Adatvédelmi Testület 4/2019 számú, a beépített és alapértelmezett adatvédelem elvéről szóló iránymutatása kimondja, hogy az adatkezelőknek már az új adatkezelés megtervezése során figyelemmel kell lenniük ezen elv érvényesülésére és annak megvalósulását később is ellenőrizniük, monitorozniuk kell. Az iránymutatásban foglaltak kiemelik, hogy az adatkezelő felelősséggel tartozik a beépített és alapértelmezett adatvédelem elvével kapcsolatos kötelezettségek érvényesüléséért az adatfeldolgozó(k) által végzett adatkezelési műveletek

viszonylatában is. Ezt az adatkezelőnek figyelembe kell vennie, amikor szerződést köt az adatfeldolgozóval.[2]

Az adatkezelés meghatározásakor, így jelen esetben a weboldal és kapcsolódó informatikai infrastruktúra megtervezése és kifejlesztésekor alkalmazott intézkedések nem voltak elegendőek ahhoz, hogy az általános adatvédelmi rendelet 25. cikkének megfelelően az adatkezelés bizalmas jellegét biztosítsák. Ennek köszönhetően később, a weboldalon keresztül a személyes adatok hozzáférhetővé váltak meghatározatlan számú személy számára.

Adatkezelőként Ügyfél 1. felelősséggel tartozik az általa megbízott adatfeldolgozó (Ügyfél 2.) tevékenységéért, így az adatfeldolgozói szerződés megkötése során kellő gondossággal kell eljárnia a megfelelő adatfeldolgozó kiválasztásakor. Az adatfeldolgozói szerződés keretei között Ügyfél 2. hanyagul tervezte meg és fejlesztette ki a rendszert, amelyre csak az adatvédelmi incidens bekövetkezéskor derült fény, arról korábban sem Ügyfél 1., sem Ügyfél 2. nem szerzett tudomást.

Az alapelvi szinten jogsértő, nem biztonságos és súlyos incidenshez vezető adatkezelés így gyakorlatilag determinálva volt már a rendszer tervezési és kialakítási fázisában, amikor még a konkrét adatkezelés el sem kezdődött. A későbbi jogsértések bekövetkezése egyenes következménye a hanyag tervezésnek és a nem megfelelő adatfeldolgozó megbízásának.

A magas kockázatú adatvédelmi incidenshez vezető súlyos tervezési hiányosságok és a nem megfelelő adatfeldolgozó megbízása miatt Ügyfél 1. megsértette ezért az általános adatvédelmi rendelet 25. cikk (1)-(2) bekezdéseit.

5. Az alkalmazott szankció és indoklása

1) A Hatóság a tényállás tisztázása során megállapította **Ügyfél 1. vonatkozásában**, hogy az adatkezelése során

- megsértette az általános adatvédelmi rendelet 25. cikk (1)-(2) bekezdéseit,
- megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját,
- megsértette az általános adatvédelmi rendelet 34. cikk (1) bekezdését.

Erre tekintettel a rendelkező részben foglaltak szerint a Hatóság utasította az Ügyfelet, hogy tegye meg a szükséges intézkedéseket annak érdekében, hogy az érintettek adatvédelmi incidensről való tájékoztatása az általános adatvédelmi rendelet 34. cikkében foglaltak szerint megvalósuljon.

A Hatóság megvizsgálta, hogy indokolt-e az Ügyfél 1-el szemben adatvédelmi bírság kiszabása. E körben a Hatóság a GDPR 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az ügy összes körülményét.

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

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

[2]https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

A Hatóság súlyosbító körülményként vette figyelembe a következőket:

- Az incidenssel érintett személyes adatok kezelése az adatok jellegéből fakadóan magas kockázattal jár, ezért az adatkezelőknek fokozott elővigyázatossággal kell eljárniuk a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. Ügyfél 1. ennek ellenére nagyszámú személyes adat (összesen 781 érintett, összesen kb. 2506 darab személyes adata, köztük gyermekkorúak adatai és szerződéses összegekre vonatkozó adatok) kezelésére használt rendszere folyamatos bizalmas jellegének biztosítása érdekében nem hozott megfelelő intézkedéseket.

- A Hatóság megállapította, hogy egy alapvetően magas kockázatú adatkezelés tekintetében Ügyfél 1. a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott, amikor a személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt Ügyfél 1. észlelte volna. Az ilyen adatok kezelésére való biztonsági felkészültség profit alapú vállalkozásoktól fokozottan elvárható.

- A Hatóság az adatvédelmi incidensről közérdekű bejelentés alapján szerzett tudomást, Ügyfél 1. által az adatvédelmi incidens észlelésére nem került sor.

- A Hatóság a megállapított adatbiztonsági hiányosságokat olyan rendszerszintű problémának tekinti, amely alapján a jogsértő helyzet már a bizonyítható jogosulatlan hozzáférések bekövetkezése előtt is hónapokkal fennállt az adatkezelőnél az érintett tesztadatbázis tekintetében.

- Az adatkezelés bizalmasságának sérülése gyakorlatilag determinálva volt már a rendszer hanyag megtervezésekor, amikor még a konkrét adatkezelés el sem kezdődött. A későbbi jogsértő adatkezelés egyenes következménye a hanyag tervezésnek és a nem megfelelő adatfeldolgozó megbízásának.

- Ügyfél 1. adatkezelőként felelősséggel tartozik azért, hogy a bekövetkezett adatvédelmi incidens kockázatait fel tudja mérni. Ennek oka, hogy az adatkezelő van tisztában azzal, hogy milyen személyes adatokat, milyen célokból és adatkezelési módszereket alkalmazva kezel. Az adatvédelmi incidens esetleges magas kockázati besorolása és ezért arról az érintetti tájékoztatás szükségességének megítélése Ügyfél 1. fő feladata, ezen kérdés megítélését nem háríthatja át a „hatósági eljárás eredményeinek függvényeire” hivatkozva a felügyeleti hatóságra. Az adatkezelőnek az érintetteket indokolatlan késedelem nélkül kell tájékoztatnia az incidensről, amint a tudomására jutott az általános adatvédelmi rendelet 34. cikke alapján, nem várhat a hatósági eljárás lezárulásáig.

A Hatóság enyhítő körülményként vette figyelembe a következőket:

- Az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán kár érte volna.

- A feltárt tényállásból arra lehet következtetni, hogy a jogsértés nem volt szándékos, azt Ügyfél 1. gondatlansága okozta. Erre utal az is, hogy az Ügyfél az incidensről való tudomásszerzést követően azonnal intézkedéseket tett a feltárt sérülékenység megszüntetése érdekében.

- A Hatóság figyelembe vette, hogy az Ügyféllel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést.

Egyéb, figyelembe vett körülmények:

- A bekövetkezett adatvédelmi incidensről való értesülése után Ügyfél 1. az incidens kezelésével kapcsolatos szinte valamennyi, az általános adatvédelmi rendelet 33. cikkei által előírt intézkedést azonnal megtette, így az incidenst kivizsgálta, azt a Hatóság részére a tudomásszerzéstől számított 72 órán belül bejelentette, a sérülékenységet Ügyfél 2. közreműködésével megszüntette, a jogszerűtlen kezelt adatbázist pedig törölte. A Hatóság így az Ügyfél 1. konkrét adatvédelmi incidenskezelési gyakorlatában problémát nem tárt fel. A Hatóság e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – kifejezetten enyhítő körülményként nem értékelte.

- A Hatóság figyelemmel volt arra is, hogy Ügyfél 1. mindenben együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást sem – mivel a jogszabályi kötelezettségek betartásán szintén nem ment túl – értékelte kifejezetten enyhítő körülményként.

A fentiekre tekintettel a Hatóság szükségesnek tartja a bírság kiszabását, csupán az Infotv. 75/A. §-a szerinti figyelmeztetés alkalmazását nem tartotta megfelelőnek.

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

Ügyfél 1. által elkövetett jogsértések az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja szerint az alacsonyabb összegű bírságkategóriába tartozó jogsértésnek minősülnek.

A bírság kiszabása során a Hatóság végül figyelembe vette Ügyfél 1. gazdasági súlyát. E körben figyelembe vette, hogy

- 2019. évi beszámolója szerint 5.344.545.000 HUF (ötmilliárd-háromszáznegyvennégymillió-ötszáznegyvenötezer forint) nettó árbevétele volt.
- 2020. évi felszámolás miatti tevékenységet záró éves beszámolója szerint a 2020. január 1. és 2020. június 15. közötti időszakban 551.404.000 HUF (ötszázötvenegymillió-négyszáznégyezer forint) nettó árbevétele volt.
- 2020. június 16-tól kezdve felszámolás alatt áll.

A Hatóság a jogsértés fennállásának időszakára (2019. november 13. – 2020. február 4.) tekintettel vette figyelembe a 2019 és 2020 évekre vonatkozó gazdasági adatokat. A jogsértés súlyára és Ügyfél 1. fenti gazdálkodási adataira tekintettel a kiszabott bírság mértéke ezért a Hatóság megítélése szerint a jogsértés súlyával arányosnak tekinthető.

2) A Hatóság a tényállás tisztázása során megállapította **Ügyfél 2. vonatkozásában**, hogy az adatfeldolgozása során megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját.

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

Erre tekintettel a Hatóság az Infotv. 61. § (1) bekezdés a) pontja alapján a rendelkező részben foglaltak szerint döntött, és jelen határozatban az Ügyfél 2-őt adatvédelmi bírság megfizetésére is kötelezte.

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

A Hatóság súlyosbító körülményként vette figyelembe a következőket:

- Az incidenssel érintett személyes adatok kezelése az adatok jellegéből fakadóan magasabb kockázattal jár, ezért az adatfeldolgozóknak fokozott elővigyázatossággal kell eljárniuk a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. Ügyfél 2. ennek ellenére nagyszámú személyes adat (összesen 781 érintett, összesen kb. 2506 darab személyes adata, köztük gyermekkorúak adatai és szerződéses összegekre vonatkozó adatok) kezelésére használt, általa Ügyfél 1. részére fejlesztett és üzemeltetett rendszer folyamatos bizalmas jellegének biztosítása érdekében nem hozott megfelelő intézkedéseket.

- A Hatóság megállapította, hogy egy alapvetően magas kockázatú adatkezelés tekintetében Ügyfél 2. a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott, amikor a személyes adatokhoz rendkívül könnyen hozzá lehetett kívülről férni, anélkül, hogy ezt Ügyfél 2. észlelte volna. Az ilyen adatok kezelésére való biztonsági felkészültség profit alapú vállalkozásoktól fokozottan elvárható.

- A Hatóság az adatvédelmi incidensről közérdekű bejelentés alapján szerzett tudomást, Ügyfél 2. által az adatvédelmi incidens észlelésére nem került sor.

- A Hatóság a megállapított adatbiztonsági hiányosságokat olyan rendszerszintű problémának tekinti, amely alapján a jogsértő helyzet már a bizonyítható jogosulatlan hozzáférések bekövetkezése előtt is hónapokkal fennállt az érintett tesztadatbázis tekintetében.

- Ügyfél 2. elmulasztotta elvégezni a weboldal és a rendszer fejlesztése során azon biztonsági teszteket, illetve más biztonsági intézkedéseket amelyekkel a sérülékenység kiszűrhető vagy megszüntethető lett volna (pl. weboldal sérülékenység vizsgálata, a teszt- és éles adatbázis fennmaradó kapcsolatának megszüntetése). Ezek a mulasztások Ügyfél 2-nek magas szinten felróhatóak, mivel fő tevékenységként informatikai szolgáltatásokat nyújtó vállalkozásként működik.

A Hatóság enyhítő körülményként vette figyelembe a következőket:

- Az eljárás során a Hatóságnak nem jutott tudomására olyan információ, amely arra utalna, hogy az érintetteket a jogsértés nyomán kár érte volna.

- A Hatóság figyelembe vette, hogy az Ügyfél 2-vel szemben korábban nem állapított meg a személyes adatok kezelésével kapcsolatos jogsértést.

Egyéb, figyelembe vett körülmények:

- A Hatóság figyelemmel volt arra is, hogy Ügyfél 2. mindenben együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást – mivel a jogszabályi

kötelezettségek betartásán szintén nem ment túl – nem értékelte kifejezetten enyhítő körülményként.

A fentiekre tekintettel a Hatóság szükségesnek tartja a bírság kiszabását, csupán az Infotv. 75/A. §-a szerinti figyelmeztetés alkalmazását nem tartotta megfelelőnek.

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

Ügyfél 2. által elkövetett jogsértések az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja szerint az alacsonyabb összegű bírságkategóriába tartozó jogsértésnek minősülnek.

A bírság kiszabása során a Hatóság végül figyelembe vette Ügyfél 2. gazdasági súlyát. E körben figyelembe vette, hogy

- 2019. évi beszámolója szerint 47.155.000 HUF (negyvenhétmillió-százötvenötezer forint) nettó árbevétele volt.
- 2020. évi adónem áttérés miatti üzleti évet záró éves beszámolója szerint a 2020. január 1. és 2020. március 31. közötti időszakban 1.772.000 HUF (egymillió-hétszázhetvenkétezer forint) nettó árbevétele volt.

A Hatóság a jogsértés fennállásának időszakára (2019. november 13. – 2020. február 4.) tekintettel vette figyelembe a 2019 és 2020 évekre vonatkozó gazdasági adatokat. A jogsértés súlyára és Ügyfél 2. fenti gazdálkodási adataira tekintettel a kiszabott bírság mértéke ezért a Hatóság megítélése szerint a jogsértés súlyával arányosnak tekinthető.

3) A Hatóság az Infotv. 61. § (2) bekezdés a) és c) pontjai alapján a határozatnak Ügyfél 1. és Ügyfél 2. azonosító adataival történő nyilvánosságra hozatalát is elrendelte, mivel a jogsértés súlyos és személyek széles körét érinti.

IV. Egyéb kérdések

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

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

A közigazgatási per szabályait a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) határozza meg. A Kp. 12. § (1) bekezdése alapján a Hatóság döntésével szembeni közigazgatási per törvényszéki hatáskörbe tartozik, a perre a Kp. 13. § (3) bekezdés a) pont aa) alpontja alapján a Fővárosi Törvényszék kizárólagosan illetékes. A Kp. 27. § (1) bekezdés b) pontja alapján a törvényszék hatáskörébe tartozó perben a jogi képviselet kötelező. A Kp. 39. § (6) bekezdése szerint a keresetlevél benyújtásának a közigazgatási cselekmény hatályosulására halasztó hatálya nincs.

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

A keresetlevél benyújtásának idejét és helyét a Kp. 39. § (1) bekezdése határozza meg. A tárgyalás tartása iránti kérelem lehetőségéről szóló tájékoztatás a Kp. 77. § (1)-(2) bekezdésén alapul. A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Itv.) 45/A. § (1) bekezdése határozza meg. Az illeték előzetes megfizetése alól az Itv. 59. § (1) bekezdése és 62. § (1) bekezdés h) pontja mentesíti az eljárást kezdeményező felet.

A veszélyhelyzet ideje alatt érvényesülő egyes eljárásjogi intézkedésekről szóló 74/2020. (III. 31.) Korm. rendelet (a továbbiakban: Korm. rendelet) 35. §-a szerint ha e rendelet eltérően nem rendelkezik, a veszélyhelyzet a határidők folyását nem érinti.

A Korm. rendelet 41. § (1) bekezdése szerint a veszélyhelyzet ideje alatt a bíróság tárgyaláson kívül jár el. Ha a perben a veszélyhelyzet idején kívül tárgyalást kellene tartani, a felperes akkor kérheti, hogy a bíróság tárgyaláson kívüli elbírálás helyett a tárgyalást a veszélyhelyzet megszűnését követő időpontra halassza el, ha
a) a bíróság a közigazgatás cselekmény halasztó hatályát legalább részben nem rendelte el,
b) a keresetindításnak halasztó hatálya van, és a bíróság halasztó hatály feloldását nem rendelte el,
c) ideiglenes intézkedést nem rendeltek el.

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

Budapest, 2020. december 9.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár