Ügyszám: NAIH-7395-6/2025
Előzmény: NAIH-6627/2024

Tárgy: jogsértés megállapítása hivatalból induló adatvédelmi hatósági eljárásban

H A T Á R O Z A T

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: **Hatóság**) a **[…]** (a továbbiakban: **Ügyfél1**) és a **[…]** (a továbbiakban: **Ügyfél2**) adatkezelésével kapcsolatban 2024. április 24-én hivatalból megindított **adatvédelmi hatósági eljárásban**

1. **megállapítja**, hogy **Ügyfél1** megsértette a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendelet (a továbbiakban: általános adatvédelmi rendelet vagy GDPR) 32. cikk (1) bekezdés b) pontját, továbbá ezen cikk (2) bekezdését.

2. A megállapított jogsértések miatt **Ügyfél1**-et a **jelen határozat véglegessé válásától számított 30 napon belül**

2.000.000 Ft, azaz kettőmillió forint

adatvédelmi bírság megfizetésére kötelezi;

3. **Ügyfél2** vonatkozásában a Hatóság az adatvédelmi hatósági eljárást **megszünteti.**

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-7395-6/2025 BÍRS. számra kell hivatkozni.

Amennyiben 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 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 keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak.[1] A tárgyalás tartása iránti kérelmet a keresetlevélben jelezni kell. A teljes személyes illetékmentességben nem részesülők számára a közigazgatási per illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

[1] A közigazgatási per kezdeményezésére a Hatóság honlapján elérhető NAIH_01 elnevezésű űrlap szolgál: https://www.naih.hu/kozig-hatarozat-birosagi-felulvizsgalata

INDOKOLÁS

I. A megállapított tényállás

(1) Ügyfél1-et Ügyfél2 a közöttük fennálló megbízási/adatfeldolgozói szerződés keretein belül megbízta, hogy Ügyfél2 nagyszámú természetes személy felhasználóinak azonosító és fizetési adatait tartalmazó adatbázisát költöztesse át az általa korábban igénybe vett szolgáltató által nyújtott szerverszolgáltatásról egy másik szolgáltató által nyújtott szerverszolgáltatásra és ennek érdekében felügyelje technikai szinten a folyamatot.

(2) Az adatbázis költöztetés Ügyfél1 általi kivitelezése 2023. október 21. napján este 22:00-kor kezdődött. Ennek során szükséges volt újraindítani a használt szervert, azonban az újraindítás után Ügyfél1 elmulasztotta ellenőrizni, hogy a tűzfal beállítások továbbra is megfelelőek-e. Ennek eredményeképpen Ügyfél1 nem vette észre, hogy a tűzfal beállítások visszaálltak az újraindítás után az alapértelmezett értékre, amelynek eredményeképpen a használt rendszer engedélyezte a hálózaton kívüli forgalmat és emiatt Ügyfél2 adatbázisához kívülről is hozzá lehetett férni. A hibás tűzfal-konfiguráció 2023. október 22. 00:07-től állt fent. Ezt a biztonsági hiányosságot kihasználva az adatbázishoz egy illetéktelen külső támadó (hacker) hozzáfért 2023. október 30-án 04:30-04:45 között és abból lekért több személyes adatot „bizonyítékként". A támadó 2023. október 30-án 17:57-kor zsaroló levelet küldött Ügyfél2-nek, aki ebből értesült az incidensről. Ügyfél2 az adatvédelmi incidenst bejelentette a Hatóságnak 2023. november 2-án, az érintetteket pedig tájékoztatta arról. Megállapítható, hogy Ügyfél1 a tűzfal biztonsági beállítások ellenőrzésének elmulasztásával nem garantálta az adatbázis-költöztetés biztonságos kivitelezését, amely így közvetlenül lehetővé tette az adatvédelmi incidens bekövetkezését.

1. Az Ügyfelek gazdasági tevékenysége

(3) Ügyfél1 a cégnyilvántartásban nyilvánosan elérhető adatok szerint […] került bejegyzésre. Fő tevékenysége […]. A 2023-as általános üzleti évet záró nyilvánosan elérhető beszámolója alapján az általa átlagosan foglalkoztatottak száma összesen […] fő. Honlapján elérhető információk szerint a cég azzal a céllal alakult, hogy […].[2]

(4) Ügyfél2 a cégnyilvántartásban nyilvánosan elérhető adatok szerint […] került bejegyzésre. Fő tevékenysége […]. A 2023-as általános üzleti évet záró nyilvánosan elérhető beszámolója alapján az általa átlagosan foglalkoztatottak száma összesen […] fő. Honlapján elérhető információk szerint […].[3]

2. A Hatósághoz érkezett adatvédelmi incidensbejelentés

(5) A Hatósághoz teljesként megjelölt incidens bejelentés érkezett 2023. november 2-án elektronikus úton […] azonosítószámon Ügyfél2-től az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján. Az incidensbejelentés szerint Ügyfél2 2023. október 30-án szerzett tudomást arról, hogy személyes adatok kezelésére is használt szervereit ezen a napon illetéktelen külső behatolás, hackertámadás érte. Erről Ügyfél2 a rosszindulatú támadást kezdeményező […] csoport egyik tagja, a […] álnevet használó személy által Ügyfél2 vezetőinek küldött e-mailből értesült aznap 17:57-kor.

[2] […]

[3] […]

(6) Az incidensbejelentés alapján az incidens előzményei a következők voltak: Ügyfél2 az […] Kft. (a továbbiakban: […]) szerver hosting[4] szolgáltatását vette igénybe személyes adatok tárolásához. Ugyanakkor Ügyfél2-nél folyamatban volt ezen szolgáltatás kapcsán egy szolgáltató-váltás, aminek keretében az […] helyett egy másik cég, a […] Kft. (a továbbiakban: […] szerver hosting szolgáltatására kívánt váltani Ügyfél2.

(7) A költöztetésre való felkészülés 2023. október 20-án vette kezdetét, amelynek keretein belül […]-től […]-hez kerültek átköltöztetésre a személyes adatok tárolásához szükséges szolgáltatások. Ennek technikai kivitelezésével Ügyfél2 Ügyfé1-et bízta meg.

(8) Ügyfél2 incidensbejelentése szerint az incidenst az eredményezte, hogy az adatbázis költöztetése során a régi kiszolgáló […] tűzfala[5] nem szűrte teljeskörűen a külső elérést az érintett API[6]-hoz.

(9) Az ügy kapcsán megtett incidensbejelentés alapján az incidenst lehetővé tevő hibás tűzfal-konfiguráció 2023. október 22. 00:07-től állt fent. A hiányosságot kihasználva az adatbázishoz való hacker általi hozzáférésre 2023. október 30-án 04:30-04:45 között kerül sor.

(10) Az incidensről Ügyfél2 2023. október 30-án 17:57-kor szerzett tudomást a hacker által írt e-mailből. A hiba kijavítására a tudomásszerzéstől számított 9 órával került sor. A külső hozzáférést lehetővé tévő adatbiztonsági hiányosság fennállásának időtartama ezek alapján kb. 9 nap (2023. október 22. – 2023. október 31.) volt. Az adatvédelmi incidenst Ügyfél2, mint adatkezelő 2023. november 2-án 14:20-kor jelentette elektronikus úton a Hatóságnak

(11) Az incidens-bejelentés alapján abban potenciálisan 900.000 felhasználó (becsült szám) személyes adatai voltak érintettek, amelyek Ügyfél2 szolgáltatásait igénybe vevő felhasználók. Ezek között az incidensbejelentés szerint személyazonossághoz kapcsolódó adatok, elérhetőségi adatok, pénzügyi adatok és helymeghatározó adatok voltak.

(12) Ügyfél2 a következő intézkedéseket tette az incidens orvoslása érdekében az incidensbejelentés szerint: azon biztonsági hibát, amelyet a támadók kihasználtak 9 órával a tudomásszerzést követően megszüntette, úgy, hogy a tűzfal szabályok módosításával az API már csak a belső hálózaton volt elérhető. Ügyfél2 a rendőrségen feljelentést tett az adatvédelmi incidenssel összefüggésben. Ezen felül az incidens-bejelentés időpontjában már tervezte, hogy arról tájékoztatja az érintetteket az általános adatvédelmi rendelet 34. cikkének megfelelően.

---

[4] A hosting jelentése webtárhely, vagy tárhely szolgáltatás. Ez biztosítja a weboldalon megjelenő tartalmak tárolását és elérhetőségét a látogatóink számára. Olyan szolgáltatás, amely lehetővé teszi a weboldalak számára, hogy a honlapon megjelenő tartalmakat tárolják, és az interneten keresztül elérhetővé tegyék azokat az emberek számára, akik az oldalt felkeresik.

[5] A tűzfal (angolul firewall) célja a számítástechnikában annak biztosítása, hogy a használt hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. A tűzfal olyan hálózati biztonsági rendszer, amely felügyeli és szabályozza a bejövő és kimenő hálózati forgalmat előre meghatározott biztonsági szabályok alapján. A tűzfal jellemzően akadályt képez egy megbízható belső hálózat és egy bizonytalan külső hálózat (pl. a nyílt internet) között.

[6] Az API az angol „application programming interface” kifejezés rövidítése, ami magyarul „alkalmazásprogramozási felületet” jelent. Az API-k a szoftverfejlesztők munkáját hivatottak megkönnyíteni azzal, hogy hozzáférést biztosítanak egy adott szoftver vagy eszköz utasításkészletéhez.

2. Hatósági ellenőrzés indítása az incidensbejelentés kapcsán

(13) A Hatóság a bejelentett adatvédelmi incidenssel kapcsolatban hatósági ellenőrzést indított 2023. december 19-én annak kivizsgálása érdekében, hogy Ügyfél2 maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek.

(14) A hatósági ellenőrzés megindításáról a Hatóság NAIH-9344-2/2023. ügyiratszámú végzésével értesítette Ügyfél2-t és a tényállás tisztázása érdekében nyilatkozattételre és adatszolgáltatásra szólította fel. Ügyfél2 2023. december 21-én és december 22-én a Hatóságnak eljuttatott kérelmében a nyilatkozattételre nyitva álló 15 napos határidő meghosszabbítását kérte, amelynek a Hatóság NAIH-265-1/2024. számú végzésével helyt adott.

(15) Ügyfél2 2024. január 18-án kelt válaszában arról nyilatkozott, hogy az incidens kivizsgálása során jelentés vagy jegyzőkönyv nem készült. Ügyfél2 több személyes és online tartott egyeztetés és e-mail váltás alkalmával tisztázta az adatvédelmi incidens releváns körülményeit.

(16) Az incidenst kiváltó okok kapcsán Ügyfél2 fenti válaszában pontosította az incidens-bejelentésben foglaltakat. E körben előadta, hogy a költöztetés során használt Debian[7] operációs rendszer alapértelmezés szerint ún. „ACCEPT" policy-t tartalmaz a tűzfal beállításoknál. Ez annyit jelent, hogy az minden IP-címről[8] enged hozzáférést. A költöztetés során a […] alkalmazásainak bind-ja 0.0.0.0. értékre volt beállítva, így tehát minden IP-címről engedett hozzáférést.

(17) Az adatbázis költöztetés technikai kivitelezésért felelős Ügyfél1 viszont azt feltételezte, hogy ún. „BLOCK" policy van beállítva alapértelmezett szabályként a tűzfal beállításoknál, amely viszont tiltja a hozzáféréseket. Összességében tehát a használt alkalmazásban lévő autentikációs szolgáltatás bekapcsolása maradt el a költözés előkészítése során, ami így lehetővé tette az adatbázist tartalmazó szerver külső elérését.

(18) Az incidens okainak vizsgálata során feltárt körülmények alapján arra jutott Ügyfél2, hogy a költözés előkészítésekor a hibás tűzfalbeállítások eredményeképpen olyan port[9] is megnyitásra került, amelyet nem kellett volna megnyitni. Ezen keresztül lehetett időlegesen elérni az érintett szervert, ez tette lehetővé a külső elérések nem megfelelő szűrését. Az, hogy a költöztetéshez kapcsolódóan milyen portok vannak nyitva, ennek ellenőrzése az Ügyfél2 vállalkozójának, Ügyfél1-nek volt a felelőssége. Összességében tehát Ügyfél2 szerint a használt alkalmazásban lévő autentikációs szolgáltatás bekapcsolása maradt el a költözés előkészítése során, ami így lehetővé tette a szerverek rosszindulatú támadó általi külső elérését.

[7] A Debian más néven Debian GNU/Linux, egy szabad és nyílt forráskódú Linux disztribúció (operációs rendszermagból és előre összeválogatott felhasználói programcsomagból álló „terjesztés"), amelyet a Debian Project fejlesztett ki. A Debian az egyik legrégebbi Linux kernelen alapuló operációs rendszer, és sok más Linux disztribúció alapja.

[8] Az IP-cím egy numerikus egyedi hálózati azonosító, amelyet az internet segítségével kommunikáló számítógépek egymás azonosítására használnak. Az IP-címek két fő funkciót látnak el: a hálózati interfész azonosítását és a helycímzést. Fő célja, hogy az internetre csatlakozott számítógépek, telefonok és egyéb eszközök megkülönböztethetők legyenek a digitális térben más eszközöktől vagy hálózatoktól.

[9] Számítógépes portnak nevezzük azt a bemeneti-kimeneti „kaput", amelyen keresztül eszközök és hálózatok adatátviteli kommunikációja történhet az adott számítógéppel.

(19) Az érintett felhasználói adatbázis kapcsán Ügyfél2 azt is közölte a Hatósággal, hogy a szolgáltatásait részben természetes személyek használják, illetve másrészt egyéni vállalkozók és egyéb vállalkozók is használják. Emellett vannak olyan „duplikációk” is, hogy például a felhasználó természetes személyként és egyéni vállalkozóként is regisztrált, lényegében ugyanazon adatokkal, egy-két adat eltéréssel. Ezek megoszlását Ügyfél2 a hatóság ezirányú kérdésére nem részletezte. Ügyfél2 mindössze annyit közölt a Hatósággal, hogy az incidensben a külső támadó összesen hány és milyen személyes adatot szerzett meg a sérülékenységen keresztül. Ezek alapján Ügyfél2 azt állapította meg, hogy a támadó összesen 61 név, 64 e-mail cím, 46 telefonszám, 44 lakcím és 17 bankszámlaszám adatot szerzett meg. Az érintettek valamennyien Ügyfél2 ügyfelei, akik regisztráltak a rendszerében (akár a honlapon keresztül, akár az applikáció letöltésével).[10]

(20) Ügyfél2 nyilatkozott továbbá, hogy az adatvédelmi incidenssel érintett felhasználókat e-mailben tájékoztatta az incidensről és megküldte annak szövegét a Hatóságnak. Ezen felül a Hatóság kérésére Ügyfél megküldte a külső támadó által küldött e-mail teljes szövegét is.

(21) Ügyfél2 2024. február 20-án külön értesítette arról a Hatóságot, hogy az adatokhoz a sérülékenységen keresztül hozzáférő külső támadót az ügyben indult büntetőeljárás során a rendőrség elfogta és a bíróság előzetes letartóztatásba helyezte 2024. február 17-én.

3. A Hatóság információbiztonsági szakvéleménye

(22) A Hatóság NAIH-265-4/2024. ügyiratszámon belső információbiztonsági szakvéleményt készített a rendelkezésre álló adatok alapján. Ebben megállapításra került, hogy Ügyfél2-nél az „iptables” tűzfalkezelő eszköz volt használatban, amely alapértelmezett módon telepítve van az Ügyfél2 által is használt Debian alapú Linux rendszereken. Az iptables lehetővé teszi a rendszergazdák számára, hogy konfigurálják a hálózati forgalmat irányító szabályokat, beleértve a bejövő és kimenő kapcsolatok szűrését és a portok átirányítását. Amikor frissen telepítik a Debian Linuxot, az alapértelmezett iptables beállítások általában úgy vannak konfigurálva, hogy minden forgalmat engedélyeznek (ez az ún. Ügyfél2 által is hivatkozott „ACCEPT” policy). Ez azt jelenti, hogy alapértelmezetten nincsenek konkrét tűzfal-szabályok konfigurálva, és a rendszer minden bejövő, kimenő és átirányított forgalmat elfogad. Összességében az alapértelmezett iptables beállítások azt a célt szolgálják, hogy maximális hozzáférést és rugalmasságot biztosítsanak, alapértelmezetten engedélyezve minden forgalmat. Ez az alapértelmezett konfiguráció nem minden környezetben megfelelő, különösen azokban, ahol szigorúbb biztonsági intézkedésekre van szükség. Az iptables beállításokat célszerű áttekinteni és módosítani a konkrét biztonsági követelmények és hálózati környezet alapján a telepítés után.

(23) Az „alkalmazás bind” kifejezést általában „alkalmazás kötése” vagy egyszerűen „kötés” fordítással használják a hálózati kontextusban. Ez utal arra, hogy az adott alkalmazás vagy szolgáltatás melyik hálózati interfészhez vagy címhez kötődik. Amikor egy alkalmazás a 0.0.0.0 címre köt, az azt jelenti, hogy az alkalmazás az összes elérhető hálózati interfészre figyel. A hálózati kapcsolatokban a 0.0.0.0 egy különleges cím, amelyet „meghatározatlan” vagy „wildcard” címként ismerünk, és gyakorlatilag azt jelenti, hogy „bármely cím”. A 0.0.0.0-ra való kötés lehetővé teszi az alkalmazás számára, hogy fogadja az érkező kapcsolatokat azon bármely IP-címről, amelyen a gép elérhető, legyen az a helyi hálózatból, egy adott külső IP-címről vagy az internetről. Ez a konfiguráció gyakran akkor

[10] Lásd Ügyfél2 a Hatóságnak 2024. 01. 18-án ePapíron küldött válaszához csatolt nyilatkozat 5. pontját, továbbá Ügyfél2 a Hatóságnak 2025. 02. 19-én ePapíron küldött válaszához csatolt nyilatkozat 1. pontját.

használatos, amikor azt szeretnék, hogy egy szolgáltatás az adott gépen elérhető legyen minden rendelkezésre álló hálózati interfészről.

(24) Összességében elmondható, hogy mivel a tűzfal beállítások alapbeállításra (default) voltak visszaállítva, vagyis minden forgalmat engedélyeztek („ACCEPT" policy) és az alkalmazás bind-ja 0.0.0.0- ra volt állítva („bármely cím"), így megtörténhetett, hogy sikeres külső támadást hajtottak végre rosszindulatú támadók. Ezen két beállítás tehát együttesen tette lehetővé az incidensben érintett adatok külső elérhetőségét a támadó számára.

4. A tényállás további tisztázása a hatósági ellenőrzés során

(25) A hatósági ellenőrzés során a Hatóság NAIH-265-5/2024. ügyiratszámú végzésével újabb nyilatkozattételre és adatszolgáltatásra szólította fel Ügyfél2-t, továbbá megküldte neki a NAIH-265-4/2024. ügyiratszámú belső információbiztonsági szakvéleményt azzal, hogy arra észrevételt, megjegyzést és indítványt tehet. Ügyfél2 […] 2024. április 2-án a Hatóságnak eljuttatott kérelmében a nyilatkozattételre nyitva álló 15 napos határidő meghosszabbítását kérte, amelynek a Hatóság NAIH-265-7/2024. számú végzésével helyt adott.

(26) Ügyfél2 – jogi képviselőjén keresztül – 2024. április 17-én kelt válaszában megküldte a Hatóság kérésére az Ügyfél1-el […] megkötött vállalkozási szerződést (a továbbiakban: Szerződés). A Szerződés alapján Ügyfél1 […] napját követően folyamatosan nyújt informatikai szolgáltatásokat Ügyfél2 részére. A Szerződés alapján Ügyfél1 az Ügyfél2 informatikai rendszereivel kapcsolatos szoftver szaktanácsadást, hibaelhárítást, javítást és egyedi fejlesztéseket végez. A gyakorlatban ez úgy valósult, meg, hogy Ügyfél2 egyedi megkeresésekkel (e-mail vagy Microsoft Teams megbeszélés) fordult Ügyfél1-hez aki az előre egyeztetett feladatokat teljesíti.

(27) A szerver hosting szolgáltatás költöztetésére egy összetettebb informatikai megkeresés keretében, az Ügyfél1-el megkötött Szerződés keretein belül került végrehajtásra. A szolgáltatás költöztetésének pontos időpontja és körülményei egy Microsoft Teams megbeszélés keretében kerültek meghatározásra.

(28) A költöztetés előkészítése kapcsán a tűzfal beállítását az előző bekezdésben hivatkozott, a Szerződés keretei közötti egyedi informatikai megkereséshez kötötten végezte Ügyfél1. Ügyfél2 nyilatkozata szerint a tűzfal beállítása Ügyfél1 által rosszul sikerült, aminek az eredménye a tűzfal szabályok alapértelmezett (default) érték szerinti működése lett. Ez tette aztán később lehetővé a külső hozzáférést az incidensben érintett adatbázishoz.

5. Hivatalbóli adatvédelmi hatósági eljárás indítása

(29) A tényállás további tisztázásán túl az ügyben az általános adatvédelmi rendeletben foglalt kötelezettségek, így különösen az 5., 25., 28. és 32. cikkek 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 adatvédelmi hatósági eljárás megindításáról döntött 2024. április 24-én.

(30) A hatósági eljárás során a Hatóság NAIH-6627-2/2024 végzésével értesítette Ügyfél2-őt. A Hatóság továbbá nyilatkozatot várt Ügyfél2-től, hogy az vajon tájékoztatta-e Ügyfél1-et a

költöztetés kivitelezése során arról, hogy a használt Debian operációs rendszer alapértelmezés szerint „ACCEPT” policy-t tartalmazza a tűzfal beállításoknál.

(31) Ügyfél2 a Hatóság fenti kérdésére azt a nyilatkozatot tette jogi képviselőjén keresztül 2024. május 6-án, hogy ő nem tájékoztatta arról Ügyfél1-et, hogy a költöztetéshez használt Debian operációs rendszer alapértelmezés szerint az „ACCEPT” policyt tartalmazza. Ügyfél2 a korábbi ellenőrzések során azt tapasztalta, hogy a port lezárások megfelelőek voltak. Ügyfél2 nyilatkozata szerint azt feltételezi, hogy az incidens kiváltó oka egy szerver újraindítás lehetett, amelyre a költöztetés során kerülhetett sor. Ezt amiatt feltételezi Ügyfél2, mivel egy ilyen újraindítás után állhatnak vissza a beállítások az alapértelmezett „ACCEPT” beállításra, ha nem kerülnek mentésre a korábbi tűzfalszabályok.

(32) A tényállás további tisztázása érdekében a Hatóság az ügyben a Szerződés alapján érintett Ügyfél1 bevonásáról döntött az adatvédelmi hatósági eljárásba. Erről a Hatóság Ügyfél1-et NAIH-6627-3/2024. ügyiratszámon értesítette és a tényállás tisztázása érdekében nyilatkozattételre hívta fel, továbbá megküldte neki az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 76. §-a alapján a NAIH-265/2024. ügyszámú hatósági ellenőrzés során keletkezett iratanyagot azzal, hogy lehetősége van azzal kapcsolatban észrevételeit, megjegyzéseit és indítványait előterjeszteni a Hatóságnál.

(33) Ügyfél1 a Hatóságnak küldött válasziratában úgy nyilatkozott, hogy a szolgáltatás költöztetését illetően nem volt saját biztonsági protokollja, így saját részről nem eszközölt a költöztetés során fizikai, logikai és adminisztratív biztonsági intézkedéseket. Ügyfél1 részt vett Ügyfél2 által szervezett Microsoft Teams megbeszéléseken. Ezeken a megbeszéléseken szóban volt egyeztetés a lehetséges kockázatokról és a következő témákat érintették: alkalmazások, szükséges fejlesztők, folyamat, hálózati beállítások, alkalmazás rendelkezésreállás és kiesés.

(34) Ügyfél1 közölte továbbá a Hatósággal válasziratában, hogy a szerver költöztetése nem egy alkalom volt, hanem több. A költöztetés eseményre vonatkozóan nem volt megállapítva külön tűzfalszabály, mert a korábbi beállításokat („BLOCK” policy) evidenciának vette. Ezeket a beállításokat még […] Kft. és […] Kft. eszközölte a költöztetés előtt.

(35) Ügyfél1 a hatósági ellenőrzés során keletkezett iratok vonatkozásában nem kívánt nyilatkozatot tenni.

(36) A Hatóság később NAIH-6627-6/2025. ügyiratszámon nyilatkoztatta arról Ügyfél1-et, hogy mi a véleménye Ügyfél2 azon korábbi, 2024. május 6-án a Hatóságnak tett nyilatkozatáról, miszerint Ügyfél2 „*nem tájékoztatta a* […]*-t, hogy a Debian operációs rendszer alapértelmezés szerint „ACCEPT” policy-t tartalmazza. A* […] *a korábbi ellenőrzései során azt tapasztalta, hogy a port lezárások megfelelőek voltak. A* […] *azt feltételezi, hogy egy szerver újraindítás után visszaállt a standard „ACCEPT” policyra, aminek feltehetően az volt az oka, hogy a korábban elmentett és alkalmazott szabályok nem kerültek mentésre ez alkalommal.”*

(37) Ügyfél1 szerint Ügyfél2 fenti nyilatkozata helytálló és joggal feltételezte, hogy a megfelelő port lezárások érvényben maradnak egy újraindítás után. A történtek kivizsgálása után azt valószínűsítette Ügyfél1, hogy elmaradt a mentés egy újraindítás alkalmával. A

beállításokat (beleértve a mentések megtörténtét) egy újraindítás során neki, tehát Ügyfél1-nek kellett volna ellenőriznie.[11]

(38) Ügyfél1 a fentieken túl még azt nyilatkozta, hogy a szolgáltatás költöztetése során a szerver bizonyosan újra lett indítva a felmerülő szolgáltatási hibák okának felderítése miatt. Ügyfél1-nek nem állnak rendelkezésére bizonyítékok (pl. naplófájl), amely alapján az „ACCEPT" policy-re való esetleges visszaállás megtörténte ellenőrizhető lenne. Ügyfél1 osztja Ügyfél2 azon álláspontját, hogy a port lezárások egy szerver újraindítás után visszaálltak az alapértelmezett „ACCEPT" policyra.[12]

(39) A Hatóság a fentiek után további nyilatkozatok beszerzése érdekében megkereste Ügyfél2-t NAIH-7395-1/2025. ügyiratszámú végzésével. Válaszában Ügyfél2 előadta, hogy az incidensben érintett személyes adatok és érintettek pontos száma tekintetében nem rendelkezik historikus adatbázissal, így nem tudja megjelölni, hogy pontosan hány felhasználó szerepelt az érintett adatbázisban. Az ismételten lefolytatott elemzés alapján úgy értékeli, hogy a felhasználók közül 30.303 B2C[13] felhasználó és 973.533 C2C[14] felhasználó lehetett az incidenskor az adatbázisban. Ügyfél2 továbbá előadta, hogy egy felhasználói adatbázissal rendelkezik és ezen felhasználói adatbázist hívják meg a […] alkalmazások amennyiben szükségesek a felhasználók adatai az adott folyamathoz. Ügyfél2 hangsúlyozta, hogy nem a teljes felhasználói adatbázishoz fért hozzá a hacker, hanem a pricing service alkalmazás használatával lehetősége volt a felhasználói adatbázisból adatokat lekérni.

(40) Ügyfél2 a Hatóság NAIH-7395-1/2025. ügyiratszámú végzésére végül úgy nyilatkozott, hogy adatbázis-költöztetés egy komplex hosszú folyamat volt, amelynek a része volt a felhasználói adatbázis költöztetése. A felhasználói adatbázis költözése 2023. október 21. napján este 22:00-kor kezdődött. A költöztetés további részfeladatai a felhasználói adatbázis költözését követően is folyamatosak voltak. Ügyfél1, mint a költöztetéssel a Szerződés keretei között megbízott fél feladatai még nem zárultak le a hacker általi külső hozzáférés, tehát az incidens bekövetkezésekor. Ennek részeként a felhasználói adatbázis költöztetés a hacker általi hozzáférés időpontjában már lezárult.

(41) Ügyfél2 nyilatkozata alapján a közte és Ügyfél1 közötti megállapodás nem határozott meg mérföldköveket az adatbázis-költöztetéssel kapcsolatosan, a felek a teljes adatbázis-költözésre, mint komplex teljes feladatra szerződtek és óradíjas elszámolást alkalmaztak. A komplex feladat részeként a felhasználói adatbázis átköltöztetését követően az alkalmazások költöztetését, mint további feladatokat továbbra is végezte Ügyfél1. Figyelembe véve, hogy a teljes adatbáziskköltöztetés még nem zárul le, így Ügyfél2 nem végzett utólagos ellenőrzést. Ennek oka, hogy az megítélése szerint idő előtti lett volna a teljes költözés lezárulta előtt.[15]

[11] Lásd Ügyfél1 a Hatóságnak 2024. 07. 08-án ePapíron küldött válaszához csatolt nyilatkozat 1. pontját

[12] Lásd Ügyfél1 a Hatóságnak 2024. 07. 08-án ePapíron küldött válaszához csatolt nyilatkozat 2. pontját

[13] B2C: business-to-customer angol kifejezés rövidítése. A vállalkozások (cégek) és a végfelhasználók (fogyasztók) közötti kapcsolatot jelenti, amelynek keretében a vállalatok termékeket vagy szolgáltatásokat kínálnak magánszemély vásárlóknak.

[14] C2C: customer-to-customer angol kifejezés rövidítése. Magánszemélyek közötti üzleti kapcsolatot jelent, ahol az egyik fogyasztó elad, a másik pedig vásárol.

[15] Lásd Ügyfél2 a Hatóságnak 2025. 02. 19-én ePapíron küldött válaszához csatolt nyilatkozat 4. pontját

(42) A Hatóság végül megküldte a hatósági eljárás teljes iratanyagát az Ákr. 76. §-a alapján NAIH-7395-3/2025. számú végzésével Ügyfél2-nek, és egyidejűleg NAIH-7395-4/2025. számú végzésével Ügyfél1-nek azzal, hogy arra nyilatkozatot, észrevételt, indítványt tehetnek. Erre Ügyfél1 részéről nem érkezett nyilatkozat a megszabott határidőn belül.

(43) Ügyfél2 a megszabott határidőn belül nyilatkozatot és indítványt jutatott el a Hatósághoz. Ebben a hivatalbóli hatósági eljárás kezdődátumával kapcsolatban tett megjegyzést, illetve különböző korábbi, az eljárás során tett nyilatkozatait emelte ki. Ezen felül Ügyfél2 tájékoztatta arról a Hatóságot, hogy az ügyben a Budapesti Rendőr-főkapitányság előtt folyamatban lévő büntetőeljárásban a 2025. február 14. napján előterjesztett iratismertetés iránti kérelmére egyelőre semmilyen választ nem kapott. Indítványozta ezért Ügyfél2 a Hatóságnál, hogy az keresse meg a Budapesti Rendőr-főkapitányságot, illetve az Országos Rendőr-főkapitányságot és kérjen hivatalos tájékoztatást a nyomozással kapcsolatban. Ügyfél2 szerint ennek azért lehet jelentősége, mivel a nyomozás eredményei is alátámasztják a korábbi – a Hatóságnak tett – nyilatkozatait az incidenssel kapcsolatban.

(44) A Hatóság Ügyfél2 indítványa alapján nem kért további tájékoztatást a nevezett rendőri szervektől. Ennek oka, hogy a Hatóság megítélése alapján a tényállás ezirányú további tisztázása nem szükséges. Az adatvédelmi incidens körülményeit, annak okait és a kezelése érdekében megtett intézkedéseket az eljárás során az Ügyfelek nyilatkozatai, a szolgáltatott dokumentumok és egyéb bizonyítékok alapján is kellőképpen sikerült feltárni a megalapozott döntés meghozatala érdekében.

II. Alkalmazott jogszabályi rendelkezések

Az általános adatvédelmi rendelet 2. cikk (1) bekezdése alapján az eljárás tárgyát képező adatkezelésre az általános adatvédelmi rendeletet kell alkalmazni.

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

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

Az általános adatvédelmi rendelet 4. cikk 7. pontja alapján „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza […].

Az általános adatvédelmi rendelet 4. cikk 8. pontja alapján „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

Az általános adatvédelmi rendelet 4. cikk 12. pontja alapján „adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy

jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az általános adatvédelmi rendelet 28. cikk (1) bekezdése alapján ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az általános adatvédelmi rendelet 32. cikk (1) bekezdése értelmében az adatkezelő és 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. A rendelet ide érti többek között a 32. cikk (1) bekezdés b) pontja alapján a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását.

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) bekezdése szerint az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az általános adatvédelmi rendelet 34. cikk (1)-(2) bekezdései szerint ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a 33. cikk (3) bekezdésének b), c) és d) pontjában említett információkat és intézkedéseket.

Az 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.

Általános adatvédelmi rendelet 83. cikk (4) bekezdés: „Az alábbi rendelkezések megsértését – a (2) bekezdéssel összhangban – legfeljebb 10 000 000 EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %- át kitevő összeggel kell sújtani, azzal, hogy a kettő közül a magasabb összeget kell kiszabni:

a) az adatkezelő és az adatfeldolgozó tekintetében a 8., a 11., a 25-39., a 42. és a 43. cikkben meghatározott kötelezettségek;”

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

Az Infotv. 38. § (3) bekezdése és 60. § (1) bekezdése alapján a Hatóság az Infotv. 38. § (2) és (2a) bekezdés szerinti feladatkörében a személyes adatok védelméhez való jog érvényesítése érdekében hivatalból adatvédelmi hatósági eljárást folytat.

Az Infotv. 61. § (1) bekezdés a) pontja szerint az adatvédelmi hatósági eljárásban hozott határozatában a Hatóság az Infotv. 2. § (2) bekezdésében meghatározott adatkezelési műveletekkel összefüggésben az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja.

Az Ákr. 99. §-a alapján a hatóság – a hatáskörének keretei között – ellenőrzi a jogszabályban foglalt rendelkezések betartását, valamint a végrehajtható döntésben foglaltak teljesítését.

Az Ákr. 101. § (1) bekezdés a) pontja alapján, ha a hatóság a hatósági ellenőrzés során jogsértést tapasztal, megindítja a hatósági eljárását.

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

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

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

III. Döntés

1. Ügyfél1, mint adatfeldolgozó és Ügyfél2, mint adatkezelő jogállása és egymáshoz való viszonya

(45) Az általános adatvédelmi rendelet 4. cikk 2. pontja alapján adatkezelésnek minősül a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így többek között azok tárolása és rendszerezése is. Ezek alapján Ügyfél2 által kezelt személyes adatok költöztetése az azok tárolására használt szerverről egy másik szerverre az Ügyfél2 által használt információs rendszerekben véghezvitt adatkezelési műveletnek minősül.

(46) Az általános adatvédelmi rendelet 4. cikk 7. pontja alapján adatkezelőnek minősül az a jogalany, amely az adatkezelés céljait vagy eszközeit meghatározza. A bejelentett adatvédelmi incidenssel érintett adatkezelés kapcsán Ügyfél2 minősül adatkezelőnek, mivel a természetes személy ügyfelei (felhasználók) adatainak az érintett információs rendszerek közötti költöztetésével ő bízta meg Ügyfél1-et a közöttük fennálló Szerződés alapján.

(47) A költöztetés, mint adatkezelési művelet kivitelezéséről Ügyfél2 szóban, a Microsoft Teams felületén keresztül egyeztetett Ügyfél1-el. Ennek során egyeztettek a költöztetéshez használt alkalmazásokról, a szükséges fejlesztőkről, magáról a költöztetés folyamatáról és a hálózati beállításokról is.[16] Az általános adatvédelmi rendelet 4. cikk 8. pontja alapján adatfeldolgozónak minősül az a jogalany, amely az adatkezelő nevében kezeli a személyes adatokat. Mivel az eredetileg Ügyfél2 által célként meghatározott adatkezelési művelet (költöztetés) kivitelezéséhez Ügyfél2 a Szerződés alapján utasítást adott Ügyfél1-nek, ezért Ügyfél1 adatfeldolgozónak minősül a művelet szempontjából.

2. Az adatkezelés biztonságával kapcsolatos megállapítások

(48) Az általános adatvédelmi rendelet 32. cikk (1) bekezdése értelmében az adatkezelő és 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. A rendelet ide érti többek között a 32. cikk (1) bekezdés b) pontja alapján a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását.

(49) 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 személyes adatok jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

(50) A Hatóság megítélése szerint a szerver költöztetése, mint Ügyfél1 által eszközölt művelet kockázatokkal járt az érintett természetes személy felhasználókra nézve. Ezeket a kockázatokat megfelelően fel kell tudni mérni és szükséges elfogadható szintre csökkenti. Tehát Ügyfél2 természetes személy ügyfelei elérhetőségi és megrendelési adatainak költöztetése csak a megfelelő szintű és arányos biztonsági intézkedések mellett kivitelezhető.

(51) Az általános adatvédelmi rendelet (75) preambulumbekezdése alapvetően kockázatosnak tekinti, ha az adatkezelés nagyszámú érintettre terjed ki. Ügyfél2 incidensbejelentése szerint a költöztetésben érintett adatbázis nagyságrendileg 900.000 érintett 3.600.000 személyes adatát tartalmazta. Ezen személyes adatok között személyazonossághoz kapcsolódó adatok, elérhetőségi adatok, gazdasági-pénzügyi adatok és helymeghatározó adatok érintettek. Ügyfél2 azt is közölte a Hatósággal, hogy a szolgáltatásait részben természetes személyek használják, illetve másrészt egyéni vállalkozók és egyéb vállalkozók is használják. Emellett vannak olyan „duplikációk” is, hogy például a felhasználó természetes személyként és egyéni vállalkozóként is regisztrált, lényegében ugyanazon adatokkal, egy-két adat eltéréssel.

(52) Később Ügyfél2 közölte a Hatóság kérdésére, hogy felhasználók közül 30.303 B2C felhasználó és 973.533 C2C felhasználó adatai lehettek letárolva az incidenskor az adatbázisban. Ez egyébként a teljes felhasználói adatbázisát jelentette az incidens bekövetkezésekor. Ügyfél2 hangsúlyozta, hogy a támadó nem töltötte le viszont a teljes adatbázist, abból összesen 61 nevet, 64 e-mail címet, 46 telefonszámot, 44 lakcímet és 17

[16] Lásd: Ügyfél1 a Hatóságnak 2024. május 10-én kelt ePapíron küldött válaszához csatolt nyilatkozat 1. és 2. pontjait

bankszámlaszámot kért le. Az illetéktelen hozzáféréssel megvalósult incidens tehát összesen ennyi személyes adatot érintett.[17]

(53) Az olyan adatok kezelését, amelyekből személyiség-lopás, vagy személyazonossággal való visszaélés fakadhat, szintén kockázatosnak tekintik a GDPR (75) preambulumbekezdésének előírásai. Ilyenek jelen ügyben az incidensben érintett természetes személy ügyfelek azonosítására szolgáló adatok, így: név, email cím, telefonszám, lakcím és bankszámlaszám. A Hatóság megjegyzi, hogy ezen adatok együttesen olyan adatkört képeznek, amelyek alapján egy természetes személy rendkívül pontosan azonosítható, így részére eredményesen küldhető célzottan rosszindulatú tartalom, adathalász üzenet/hívás, vagy más csalási/megtévesztési tevékenységgel összefüggő megkeresés/felhívás.

(54) Ekkora nagyságrendű, személyes adatokat is tartalmazó adatbázis esetén az abban kezelt adatok nagy száma miatt a költöztetés kockázatai is jelentősek. A jelentős adatvédelmi kockázatok fokozott figyelmet és megfelelő kockázatcsökkentő intézkedések alkalmazását követelik meg. A vizsgált jogviszonyban a költöztetési művelet kivitelezése Ügyfelek korábbi megegyezése és közös akarata alapján Ügyfél1 önálló feladata volt. Ennek kivitelezésére a Szerződés alapján került sor. Ügyfél2 a költöztetés technikai kivitelezésében nem vett részt, magát a folyamatot technikai szinten nem felügyelte, azt tehát teljes mértékben Ügyfél1-re bízta.

(55) Az ügy kapcsán megtett incidensbejelentés alapján az adatbiztonsági hiányosság 2023. október 22., 00:07-től állt fent, mivel ezen időponttól futott a kiszolgáló szerveren a hibás tűzfal beállítás („BLOCK” helyett „ACCEPT” policy). A hiányosságot kihasználva az adatbázishoz való hacker általi hozzáférésre 2023. október 30-án 04:30-04:45 között kerül sor. Az incidensről Ügyfél2 2023. október 30-án 17:57-kor szerzett tudomást a hacker által írt e-mailből. A hiba kijavítására a tudomásszerzéstől számított 9 órával került sor. A külső hozzáférést lehetővé tévő adatbiztonsági hiányosság fennállásának időtartama ezek alapján kb. 9 nap (2023. október 22. – 2023. október 31.) volt.

(56) Az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdései nevesítik az adatfeldolgozót, amelynek önálló felelőssége is van arra, hogy az adatkezelés jellege, körülményei, céljai és kockázatai alapján, a tudomány és technológia állása szerinti megfelelő szintű adatbiztonsági intézkedéseket hajtson végre. Ezeknek az adatbiztonsági intézkedéseknek többek között azt kell garantálniuk, hogy a kezelt személyes adatok ne kerüljenek jogosulatlanul nyilvánosságra, vagy azokhoz ne lehessen jogosulatlanul hozzáférni.

(57) Ügyfél1 tehát adatfeldolgozóként önálló felelősséggel tartozik az általa Ügyfél2 megbízásából és nevében kivitelezett adatkezelési műveletnek az egyeztetett keretek közötti megfelelő technikai lebonyolításáért. Ügyfél1-et a Szerződés keretei között a költöztetés konkrét technikai kivitelezés kapcsán felelősség terheli az általános adatvédelmi rendelet 32. cikke alapján a megfelelő konkrét technikai és szervezési intézkedések megtételéért.

(58) Ügyfél2 nyilatkozatai alapján megállapítható, hogy a korábbi ellenőrzések során azt tapasztalta, hogy az alkalmazott Debian operációs rendszerben és az iptables tűzfal kapcsán beállított port lezárások megfelelőek voltak. Ezeket a beállításokat még korábban […] és […] állította be. Ügyfél2 azt feltételezte, hogy egy szerver újraindítás után álltak

[17] Lásd Ügyfél2 a Hatóságnak 2024. 01. 18-án ePapíron küldött válaszához csatolt nyilatkozat 5. pontját, továbbá Ügyfél2 a Hatóságnak 2025. 02. 19-én ePapíron küldött válaszához csatolt nyilatkozat 1. pontját.

vissza a beállítások az alapértelmezett „ACCEPT” beállításra, amely aztán lehetővé tette az incidensben érintett adatokhoz a hacker általi jogosulatlan hozzáférést. Ennek Ügyfél2 szerint az lehetett az oka, hogy nem kerültek mentésre a korábbi hozzáférési beállítások.

(59) Ügyfél1 nyilatkozatai alapján elismerte, hogy a költöztetési eseményre vonatkozóan nem volt megállapítva külön tűzfalszabály. Ennek oka, hogy a korábbi, a külső hozzáférést tiltó beállításokat (amiket […] és […] eszközölt) evidenciának vette. Ügyfél1 azt is nyilatkozta, hogy a szolgáltatás költöztetése során a szervert bizonyosan újraindította a felmerülő szolgáltatási hibák okának felderítése miatt. A történtek kivizsgálása után azt valószínűsítette Ügyfél1, hogy a tűzfalbeállítások mentését elmulasztotta egy újraindítás alkalmával. A beállításokat (beleértve a mentések megtörténtét) egy újraindítás során Ügyfél1-nek, mint a költöztetéssel megbízott és azt technikai szinten kivitelező adatfeldolgozónak kellett volna ellenőriznie. Mivel ez az ellenőrzés elmaradt, a port lezárások az újraindítás után visszaálltak az alapértelmezett „ACCEPT” policyra, ami így lehetővé tette a hacker általi külső hozzáférést és az incidens bekövetkezését.[18]

(60) Az általános adatvédelmi rendelet 32. cikke előírja a kockázatokkal arányos adatbiztonsági intézkedések alkalmazását az adatfeldolgozó által. Az incidensben érintett adatok költöztetése kapcsán Ügyfél1-nek, mint adatfeldolgozónak a feladata a rábízott technikai környezetben, az általa az adatkezelő nevében végzett adatkezelési műveletekkel összefüggésben a megfelelő biztonsági szint garantálása a megfelelő beállítások alkalmazásával és ellenőrzésével. A költöztetés az érintett személyes adatok nagysága és érzékenysége miatt magas kockázatú adatkezelési művelet, amely kapcsán fokozott odafigyelés várható el az azt kivitelező adatfeldolgozótól. A művelet kivitelezése kapcsán kulcsfontosságú, hogy az adatok átvitele biztonságos, a bizalmasságot garantáló környezetben történjen, amihez illetéktelen harmadik fél nem férhet hozzá. A megfelelő tűzfalbeállítások Ügyfél1 általi ellenőrzésének elmulasztása miatt a bizalmasság azonban sérült, így az közvetlenül lehetővé tette az incidens bekövetkezését.

(61) A nagyszámú és érzékeny személyes adatot érintő magas kockázatú adatkezelési művelet bizalmasságának sérülése a fentiek alapján Ügyfél1 felelősségi körében merült fel, mivel a művelet kivitelezésével ő volt megbízva. Ügyfelek ugyan csak szóban, Microsoft Teams-en keresztül egyeztettek a költöztetés kivitelezéséről, az ezzel kapcsolatos nyilatkozataik azonban teljesen egybehangzóak, azok között ellentmondás nem fedezhető fel. Ügyfelek tehát az eljárás során végig egyetértettek abban, hogy Ügyfél1-nek kellett volna ellenőriznie a szerver újraindítása után, hogy a beállítások továbbra is megfelelőek-e a művelet kivitelezéséhez.

(62) További fontos körülmény, hogy Ügyfél1 költöztetési feladatai még nem zárultak le az incidens bekövetkezésekor, tehát Ügyfél2 részére még nem került átadásra a költöztetés eredménye, amely alapján az ellenőrizni tudta volna annak megfelelő kivitelezését. A jogsértés így az Ügyfél1 által elmulasztott biztonsági intézkedések hiányából fakad.

(63) A Hatóság megítélése alapján Ügyfél2, mint adatkezelő képes volt igazolni azt, hogy az adatbiztonsági hiányosságok nem az ő felelősségi körében merültek fel. Az Ügyfelek nyilatkozatai a költöztetés kivitelezési kapcsán teljesen egybehangzóak és nem mondanak egymásnak ellent azzal kapcsolatban, hogy az incidenst lehetővé tévő hibás tűzfalbeállítás Ügyfél1 adatfeldolgozói tevékenységének hiányosságaira vezethető vissza.

[18] Lásd Ügyfél1 a Hatóságnak 2024. 07. 08-án ePapíron küldött válaszához csatolt nyilatkozat 1. és 2. pontját

(64) A fentiek alapján a Hatóság megállapítja, hogy Ügyfél1 megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontját, továbbá ezen cikk (2) bekezdését azzal, hogy a rábízott adatkezelési műveleteket nem megfelelő adatbiztonsági intézkedések mellett végezte.

3. A bekövetkezett adatvédelmi incidens kezelése kapcsán megtett intézkedések

(65) Az általános adatvédelmi rendelet 4. cikk 12. pontja alapján adatvédelmi incidensnek minősül a biztonság sérülése, amely a kezelt személyes adatok jogosulatlan közlését, vagy azokhoz való jogosulatlan hozzáférést eredményezi. A fogalom szempontjából így a biztonsági eseménnyel való kapcsolat kulcselemnek tekinthető. Egy személyes adatokat érintő esemény csak abban az esetben minősül adatvédelmi incidensek, ha az valamilyen biztonsági sérüléssel hozható összefüggésbe, ez a kiváltó oka és a kettő között okozati összefüggés áll fent. A biztonság sérülése fakadhat a személyes adatok védelme érdekében alkalmazott biztonsági intézkedések hiányos, nem megfelelő, esetleg elavult voltából vagy épp azok teljes hiányából.

(66) Az adott ügyben a biztonsági sérülés abból adódott, hogy Ügyfél1 elmulasztotta a megfelelő technikai és szervezési intézkedések ellenőrzését Ügyfél2 természetes személy ügyfelei adataival kapcsolatban azok bizalmasságának megőrzése érdekében. A megfelelő biztonsági intézkedések hiányában ezért az incidenssel érintett adatbázisban kezelt személyes adatokhoz hozzá tudott férni az interneten keresztül a külső támadó.

(67) 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.

(68) Az incidensben érintett nagyszámú, továbbá szenzitív és pontos adatkört magában foglaló adatkezelés során, a biztonsági intézkedések sérülése miatt bekövetkező adatvédelmi incidens magas kockázatúnak minősül. Ennek oka, hogy az adatokhoz való hacker általi jogosulatlan hozzáférés után az adatkezelő ráhatása azok sorsára kikerül az ellenőrzése alól. Az adatok kezelésének további bizalmas jellegét nem lehetséges teljes mértékben a továbbiakban garantálni.

(69) A megfelelő adatbiztonsági intézkedések alkalmazása csökkentette volna annak a kockázatát, hogy azokat a hacker jogosulatlanul ne ismerhesse meg.

(70) A nagyszámú személyes adatot tartalmazó adatbázishoz történő hozzáférés összevetve az incidens körülményeivel a Hatóság megítélése szerint magas kockázatú adatvédelmi incidenst eredményezett.

(71) A fentiek alapján a Hatóság megítélése szerint az adatvédelmi incidens magas kockázatúnak tekinthető, ezért amennyiben egy ilyen esetről az adatkezelő tudomást szerez, úgy azt fő szabály szerint a tudomásszerzéstől számított 72 órán belül be kell jelentenie az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján a felügyeleti hatóságnak.

(72) Az ügy kapcsán megtett incidensbejelentés alapján az adatbiztonsági hiányosságot kihasználva az adatbázishoz való hacker általi hozzáférésre 2023. október 30-án 04:30-04:45 között kerül

sor. Az incidensről Ügyfél2 2023. október 30-án 17:57-kor szerzett tudomást a hacker által írt e-mailből. Az adatvédelmi incidenst Ügyfél2, mint adatkezelő 2023. november 2-án 14:20-kor jelentette elektronikus úton a Hatóságnak, így az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján fennálló 72 órán belüli bejelentési kötelezettségének eleget tett.

(73) Ezen felül az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján a magas kockázatú adatvédelmi incidensben érintett személyeket tájékoztatni is kell az adatvédelmi incidensről és az azzal összefüggésben megtett intézkedésekről. Ügyfél2 nyilatkozata szerint az incidensben érintett felhasználókat e-mailben tájékoztatta az incidensről. A tájékoztatás szövegét Ügyfél2 eljuttatta a Hatóság részére, amely a Hatóság megítélése szerint megfelel a rendelet 34. cikkében előírtaknak, mivel az tartalmazza az incidens jellegét, az érintett személyes adatokat, a további információkkal kapcsolatos elérhetőséget és az incidens orvoslására megtett intézkedéseket.[19]

(74) A Hatóság a fentiekre tekintettel megállapítja, hogy Ügyfél2 adatkezelőként eleget tett az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján fennálló incidensbejelentési, továbbá a 34. cikk (1) pontja szerinti érintetti tájékoztatási kötelezettségének, így az incidens kezelésével és az érintettek erről való tájékoztatásával kapcsolatban Ügyfél2 részéről jogsértést nem állapított meg.

4. Az alkalmazott szankcióval kapcsolatos megállapítások.

(75) A Hatóság megállapítja, hogy Ügyfél1 megsértette a GDPR 32. cikk 1) bekezdés b) pontját, továbbá ezen cikk (2) bekezdését.

(76) Ügyfél2 vonatkozásban a Hatóság az eljárást megszüntette az Ákr. 47. § (1) bekezdés c) pontja alapján, mivel jogsértést nem állapított meg adatkezelési tevékenysége kapcsán, így az eljárás vele szemben okafogyottá vált.

(77) Az Infotv. 75/A. § alapján 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.

(78) E körben a Hatóság az általános adatvédelmi rendelet 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az ügy összes körülményeit. Tekintettel az ügy körülményeire, az adatkezelés jellegére, az érintettek számára és az adatok érzékenységére a Hatóság megállapította, hogy Ügyfél1 vonatkozásában a jelen eljárás során feltárt jogsértés esetében a figyelmeztetés nem arányos és nem visszatartó erejű szankció, ezért a Hatóság bírság kiszabása mellett döntött az Infotv. 61. § (1) bekezdés a) pontjára figyelemmel a GDPR 58. cikk (2) bekezdés i) pontja alapján.

(79) A Hatóság Ügyfél1-el szemben a bírság kiszabásának szükségessége és összegének megállapítása során figyelembe vette az Európai Adatvédelmi Testület 4/2022-es számú iránymutatásában[20] (a továbbiakban: Bírság Iránymutatás) foglaltakat, amely az általános

[19] Lásd Ügyfél2 a Hatóságnak 2024. 01. 18-án ePapíron küldött válaszának szövegét és az ahhoz csatolt nyilatkozat 6. pontját.

[20] edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_hu_0.pdf

adatvédelmi rendelet szerinti közigazgatási bírságok kiszabásának számítási szempontjait tartalmazza. Erre tekintettel a bírság összegének meghatározására a következő szempontok alapján került sor:

I. Ügyfél1 egy magatartásával (biztonsági beállítások ellenőrzésének elmulasztása) egy adatkezelési művelet (adatbázis költöztetése) tekintetében valósította meg a jogsértést [GDPR 32. cikk (1) bekezdése, annak b) pontja és (2) bekezdésének sérelme]. A Bírság Iránymutatás 3.1. pontja alapján így a GDPR 83. cikk (4) bekezdése alapján a bírság teljes összege nem haladhatja meg a legsúlyosabb jogsértés esetén meghatározott összeget.

II. A bírságszámítás kiindulási összegének meghatározása:

II. 1. A jogsértések kategorizálása: Ügyfél1 által elkövetett jogsértés – az adatkezelés biztonságára vonatkozó rendelkezések megsértése – a GDPR 83. cikk (4) bekezdés a) pontja szerint az alacsonyabb összegű bírságkategóriába tartozó, enyhébb jogsértésnek minősül, amelyek esetében a bírság felső határa 10 millió euró vagy a vállalkozás éves árbevételének 2%-a, attól függően, hogy melyik a magasabb. Ügyfél1 legutóbbi nyilvánosan elérhető 2023. évi beszámolója szerint az éves nettó árbevétele […] HUF (azaz […] forint). Ezen összeg 2 %-a […] HUF (azaz […] forint), amely […] EUR-nak ([…] eurónak) felel meg, azaz nem éri el a GDPR 83. cikk (4) bekezdése által meghatározott statikus bírságmaximumot, a 10.000.000 EUR-nak megfelelő összeget, így Ügyfél1 a jelen ügyben legfeljebb 10.000.000 EUR-nak megfelelő összegű bírsággal sújtható.

II. 2. A jogsértések jellege, súlyossága és időtartama:

a) A jogsértés jellege (*nature of the infringement*) kapcsán a Hatóság figyelembe vette, hogy milyen érdek védelmét szolgálják a megsértett rendelkezések. A GDPR 32. cikke azt a célt szolgálja, hogy az érintett természetes személyek adatai biztonságos környezetben kerüljenek kezelésre az adatkezelő és/vagy adatfeldolgozó által. Az adatkezelő/adatfeldolgozó kötelezettsége, hogy folyamatosan nyomon kövesse azt, hogy az általa kezelt személyes adatok biztonságos, a tudomány és technológia mindenkori állásának megfelelő környezetben kerüljenek kezelésre és ezzel elfogadható szintre csökkentse az esetleges biztonsági eseményekből fakadó kockázatokat. Amennyiben GDPR ezen rendelkezései sérülnek és az adatok nem kellően biztonságos környezetben kerülnek kezelésre, úgy az érintettek magánszférája is sérülhet, pl. az elmulasztott biztonsági intézkedések hiányát kihasználó esetleges illetéktelen hozzáférésből fakadóan.

b) A jogsértés súlya (*gravity of the infringement*) kapcsán a Bírság Iránymutatás figyelembe vehető szempontként nevesíti a GDPR 82. cikk (2) bekezdés a) pontjában foglaltak szerint, a szóban forgó adatkezelés jellegét, körét vagy célját, továbbá azon érintettek számát, akiket a jogsértés érint, valamint az általuk elszenvedett kár mértékét.

- A megállapított jogsértés Ügyfél2 szolgáltatásait igénybe vevő felhasználókat érintette. A Hatóság figyelembe vette, hogy az adatbiztonsági hiányosságokkal érintett adatkezelés célja Ügyfél2 alaptevékenységéhez kapcsolódik, amely […] szolgáltatás. Ezen szolgáltatás nyújtásához a

felhasználók személyes adatainak […] kezelése elengedhetetlen. Ezen Ügyfél2 alaptevékenységének ellátásához szükséges adatok költöztetésével, mint adatkezelési művelet biztonságos kivitelezésével volt megbízva Ügyfél1. Az ilyen, Ügyfél2 gazdasági működéséhez elengedhetetlen adatok biztonságos kezelése fokozott figyelmet és körültekintést kíván meg Ügyfél1, mint adatfeldolgozó részéről is. A Hatóság ezt a körülményt a jogsértés súlyosságát növelő tényezőként értékelte.

- Ügyfél1 fő gazdasági tevékenységként informatikai szolgáltatások nyújtásával foglalkozik, így az általa Ügyfél2 nevében és megbízásából végzett adatbázis költöztetés ezen alaptevékenységéhez kapcsolódik, emiatt ennek megfelelő kivitelezése tőle fokozottan elvárható. A Hatóság ezt a körülményt a jogsértés súlyosságát növelő tényezőként értékelte.

- Ügyfél2 incidenssel érintett adatbázisában több, mint 900.000 felhasználó, legnagyobb részt magánszemélyek adatai érintettek, azaz a jogsértés érintettjeinek száma rendkívül jelentősnek mondható. A Hatóság ezt a körülményt a jogsértés súlyosságát növelő tényezőként értékelte.

- Ügyfél2 az adatvédelmi incidensről és az azt lehetővé tévő adatbiztonsági hiányosságról magától a jogosulatlan hozzáférést véghezvivő hackertől értesült. Ennek hiányában a jogsértő állapot nem jutott volna Ügyfél2 és így az azért felelős Ügyfél1 tudomására. A Hatóság ezt a körülményt a jogsértés súlyosságát növelő tényezőként értékelte.

c) A jogsértés időtartama (*the duration of the infringement*): Az ügy kapcsán megtett incidensbejelentés alapján az adatbiztonsági hiányosság 2023. október 22., 00:07-től állt fent, mivel ezen időponttól futott a kiszolgáló szerveren a hibás tűzfal beállítás („BLOCK” helyett „ACCEPT” policy). A hiányosságot kihasználva az adatbázishoz való hacker általi hozzáférésre 2023. október 30-án 04:30-04:45 között kerül sor. Az incidensről Ügyfél2 2023. október 30-án 17:57-kor szerzett tudomást a hacker által írt e-mailből. A hiba kijavítására a tudomásszerzéstől számított 9 órával került sor. A külső hozzáférést lehetővé tévő adatbiztonsági hiányosság fennállásának időtartama ezek alapján kb. 9 nap (2023. október 22. – 2023. október 31.). A Hatóság ezt az időtartamot közepesen súlyosnak értékelte. A jogsértés súlyát csökkentő tényezőként értékelte viszont azt a körülményt, hogy az arról való tudomásszerzést követően az adatbiztonsági sérülés rövid időn belül elhárításra került.

II. 3. A jogsértések szándékos vagy gondatlan jellege: a Hatóság álláspontja szerint Ügyfél1 gondatlanul követte el a jogsértést. Ügyfél1 tisztában van azzal, hogy az adatbázis költöztetésével Ügyfél2 megbízásából a Szerződés alapján adatkezelési műveletet végez. Ügyfél1 neki felróható és általa is elismert módon elmulasztotta ellenőrizni a tűzfal biztonsági beállításait a költöztetési művelet kivitelezése kapcsán, ezért kerülhetett sor a sérülékenységre és annak kihasználásával az illetéktelen külső hozzáférésre. Ügyfél1 által kivitelezett adatbázis költöztetés kellő gondosság tanúsítása mellett jogsértés elkerülésével is megvalósítható lett volna, ugyanakkor a jogsértő magatartás tanúsítására mulasztásos jelleggel került sor, ami a beállítások ellenőrzésének hiányából fakadt. A jogsértő állapotra való egyértelműen szándékos törekvést a Hatóság nem látta megalapozottnak, tekintettel arra is, hogy az a tudomásszerzést követően rövid időn belül elhárításra került, ezért azt gondolatlanul elkövetettnek értékelte.

II. 4. Az érintett adatok kategóriái: a jogsértések, bár nem érintik személyes adatok különleges kategóriáit [GDPR 9. cikk (1) bekezdés], azonban a Hatóság figyelembe vette, hogy azok egy-egy érintett esetében kellően részletes elérhetőségi adatokat és fizetési információkat tartalmaznak, amely így az adatbiztonsági hiányosság által az érintettekre jelentett kockázatokat jelentősen megnövelték. Az adatbiztonsági hiányosságokkal érintett adatkezelés tehát alapvetően magas kockázatokat hordoz az érintettek jogaira és szabadságaira nézve. A Hatóság ezt a körülményt a jogsértés súlyosságát növelő tényezőként értékelte.

II. 5. A jogsértés súlyának minősítése és a megfelelő kiindulási összeg meghatározása: mindezen szempontok alapján a Hatóság arra a megállapításra jutott, hogy Ügyfél1 által elkövetett jogsértés közepes súlyosságúnak minősül, így a Bírság Iránymutatás 4.2.4 pontja szerint az alkalmazandó felső határ 10-20%-ában kell meghatározni a bírságösszeg további számításához szükséges kiindulási összeget. Ez a konkrét esetben 1 és 2 millió EUR közötti összeg.

II. 6. A Bírság Iránymutatás 4.3 pontja értelmében, annak érdekében, hogy a bírság hatékony, arányos és visszatartó erejű legyen, a jogsértés súlyossága alapján számított kiindulási összeg a vállalkozás éves nettó árbevételének figyelembevételével a Hatóság mérlegelése alapján módosítható. Ügyfél1 2023. évi nettó árbevétele […] HUF (azaz […] forint), amely […] EUR-nak (azaz […] euró) felel meg.[21] Ügyfél1 ezek alapján a Bírság Iránymutatás 4.3 pontja értelmében a legfeljebb 2 millió euróig terjedő árbevételű vállalkozások kategóriájába tartozik, amelyeknél a bírságszámítás alapja a kiindulási összeg 0,2%-a és 0,4 %-a közé eső összeg. Ez jelen esetben 2.000 – 8.000 EUR, amely 814.000 – 3.256.000 HUF-nak felel meg.

III. A Hatóság által figyelembe vett további körülmények:

- A Hatóság súlyosító körülményként értékelte, hogy az adatbiztonságot garantáló megfelelő technikai és szervezési intézkedések ellenőrzésének elmulasztása alapvetően Ügyfél1, mint adatfeldolgozó felelősségi körében merült fel [GDPR 83. cikk (2) bekezdés d) pontja].

- A Hatóság enyhítő körülményként értékelte, hogy Ügyfél1-et ezt megelőzően a személyes adatok védelmére vonatkozó jogszabályi rendelkezések megsértése miatt a Hatóság még nem marasztalta [GDPR 83. cikk (2) bekezdés e) pont].

- A Hatóság enyhítő körülményként értékelte, hogy a jogsértő körülmény, az arról való tudomásszerzést követően az rövid időn belül elhárításra került [GDPR 83. cikk (2) bekezdés c) pont].

- A Hatóság semleges körülményként értékelte, hogy Ügyfél1 együttműködött a Hatósággal a tényállás tisztázása során, mivel ez jogszabályi kötelezettségein nem ment túl. [GDPR 83. cikk (2) bekezdés f) pont].

- A Hatóság a bírságkiszabás során a GDPR 83. cikk (2) bekezdés h) pontját semleges körülményként értékelte, mivel a jogsértésről Ügyfél2-től, mint adatkezelőtől szerzett tudomást a GDPR. 33. cikke szerint előírt incidens-bejelentési kötelezettség keretein belül.

[21] A határozathozatal időpontjában a Magyar Nemzeti Bank által nyilvánosságra hozott és irányadó EUR/HUF középárfolyam szerint. Lásd: https://www.mnb.hu/arfolyam-lekerdezes

- A GDPR 83. cikk (2) bekezdés i), j) és k) pontja szerinti körülményeket nem tartotta a Hatóság relevánsnak, mivel azok a konkrét ügy kapcsán nem voltak értelmezhetők.

(80) A Hatóság a jelen ügyben a bírság kiszabásánál figyelembe vette, hogy a kiszabott bírságnak hatékonynak, arányosnak és visszatartó erejűnek kell lennie. Tekintettel a jogsértés közepes súlyosságára és az ezt árnyaló súlyosító és enyhítő körülmények nagyjából azonos számára, a Hatóság a bírság összegét a rendelkezésre álló tartomány középösszegénél határozta meg. A Hatóság álláspontja szerint a kiszabott bírság hatékony, és ösztönző erővel bír arra, hogy Ügyfél1 a jövőben fokozott figyelemmel legyen adatfeldolgozási tevékenységeire, azokat a GDPR rendelkezéseivel összhangban végezze és a jövőben tartózkodjon a hasonló jogsértésektől.

(81) Mindezek alapján a Hatóság a rendelkező részben foglaltak szerint döntött.

IV. Egyéb kérdések

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

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

A közigazgatási per szabályait a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) határozza meg. A Kp. 12. § (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 polgári perrendtartásról szóló 2016. évi CXXX. törvény 604. § szerint alkalmazandó, digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (a továbbiakban: Dáptv.) 19.§ (1) bekezdés b) pontja szerint az ügyfél jogi képviselője elektronikus kapcsolattartásra kötelezett.

A keresetlevél benyújtásának idejét és helyét a Kp. 39. § (1) bekezdése határozza meg. A tárgyalás tartása iránti kérelem lehetőségéről szóló tájékoztatás a Kp. 77. § (1)-(2) bekezdésén alapul.

A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Itv.) 45/A. § (1) bekezdése határozza meg. Az illeték előzetes megfizetése alól az Itv. 59. § (1) bekezdése és 62. § (1) bekezdés h) pontja mentesíti az eljárást kezdeményező felet.

Az Ákr. 132. §-a szerint, ha a kötelezett a hatóság végleges döntésében foglalt kötelezésnek nem tett eleget, az végrehajtható. A Hatóság határozata az Ákr. 82. § (1) bekezdése szerint a közléssel véglegessé válik. Az Ákr. 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, 2025. április 8.

Dr. habil. Péterfalvi Attila
elnök, c. egyetemi tanár