Ügyszám: NAIH/2020/1160/10
Előzmény: NAIH/2019/7105
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 **Digi Távközlési és Szolgáltató Kft-t** (székhely: 1134 Budapest, Váci út 35., cégjegyzékszám: 01-09-667975) (a továbbiakban: Ügyfél vagy Adatkezelő) érintő, általa elektronikus úton 2019. szeptember 25-én […] azonosítószámon bejelentett adatvédelmi incidenssel kapcsolatban a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendelet (a továbbiakban: általános adatvédelmi rendelet) 5. és 32-34. cikkeiben foglalt kötelezettségei feltételezhető megsértése miatt hivatalból megindított **adatvédelmi hatósági eljárásban**

1. **megállapítja**, hogy

   a. az Ügyfél megsértette az általános adatvédelmi rendelet 5. cikk (1) bekezdésének b) („célhoz kötöttség”) és e) („korlátozott tárolhatóság”) pontjait, amikor az adatvédelmi incidenssel érintett, eredetileg hibaelhárítási célból létrehozott tesztadatbázist a szükséges tesztek lefuttatása és a hiba kijavítása után nem törölte, így az abban tárolt nagy számú ügyféladat a következő […] időszakban cél nélkül és azonosításra alkalmas módon került tárolásra a használt rendszerekben. Ezen intézkedés hiánya közvetlenül lehetővé tette az adatvédelmi incidens bekövetkezését és a személyes adatok hozzáférhetőségét.

   b. Az Ügyfél megsértette az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseit, így nem alkalmazott az adatkezelés biztonsága körében a kockázatokkal arányos megfelelő technikai és szervezési intézkedéseket, azzal, hogy

   - az általa használt tartalomkezelő ([…]) egy több mint 9 éve ismert, megfelelő eszközökkel egyébként detektálható és javítható sérülékenységét kihasználva lehetett hozzáférni a nyilvánosan elérhető digi.hu weboldalon keresztül az incidenssel érintett adatbázisokhoz;
   - az adatvédelmi incidenssel érintett személyes adatok tekintetében ([…]) nem alkalmazott titkosítást, amely így az incidensből fakadó kockázatokat nagy mértékben megnövelte.

   Ezen intézkedések hiánya közvetlenül lehetővé tette, hogy az adatbázisokban tárolt ügyféladatok hozzáférhetővé váltak a támadást végrehajtó etikus hacker által is feltárt sérülékenységen keresztül.

2. **kötelezi** az Ügyfelet, hogy vizsgálja felül az általa kezelt valamennyi személyes adatokat tartalmazó adatbázist abból a szempontból, hogy azokban indokolt-e titkosítás alkalmazása és ennek eredményeiről tájékoztassa a Hatóságot!

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

100.000.000,- Ft, azaz százmillió forint

adatvédelmi bírság megfizetésére kötelezi;

4. **elrendeli** a végleges határozatnak az adatkezelő azonosító adatainak közzétételével, de az üzleti titkok kitakarásával 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/2020/1160 BÍRS. számra kell hivatkozni.

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

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

Jelen határozattal szemben közigazgatási úton jogorvoslatnak nincs helye, de az a közléstől számított 30 napon belül a Fővárosi Törvényszékhez címzett keresetlevéllel közigazgatási perben megtámadható. A veszélyhelyzet nem érinti a keresetindítási határidőt. 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 bírósági felülvizsgálati eljárás illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

I N D O K O L Á S

I. Előzmények, a tényállás tisztázása

a. A Hatósághoz érkezett incidensbejelentés és a hatósági ellenőrzés során megállapítottak

1) A Hatóság az Ügyfél által 2019. szeptember 25-én elektronikus úton bejelentett adatvédelmi incidenssel kapcsolatban 2019. október 8-án hatósági ellenőrzést indított, mivel a bejelentésben közölt adatok nem voltak elegendőek annak megítéléséhez, hogy az Ügyfél maradéktalanul eleget tett-e az általános adatvédelmi rendeletben foglalt kötelezettségeinek, így különösen a 32-34. cikkében foglaltaknak.

A bejelentés szerint az Ügyfél legkésőbb 2019. szeptember 23-án szerzett arról tudomást, hogy egy támadó a www.digi.hu honlapon keresztül elérhető sérülékenységet kihasználva hozzáfért körülbelül […] érintett személyes adataihoz, akik nagyobb részt (kb. […] fő) az Ügyfél megrendelői és előfizetői, kisebb részt (kb. […] fő) pedig hírlevére feliratkozók voltak. A megrendelői, előfizetői

személyes adatok között megtalálható volt az érintettek neve, anyja neve, születési helye és ideje, lakcíme, személyi igazolványszáma (esetenként személyi száma), e-mail címe, vezetékes és mobil telefonszáma.

A Hatóság a hatósági ellenőrzés során NAIH/2019/7105/2. és NAIH/2019/7105/4. ügyiratszámú végzéseivel nyilatkozattételre és iratszolgáltatásra szólította fel az Ügyfelet. Az Ügyfél nyilatkozatai alapján a Hatóság az alábbiakat állapította meg a hatósági ellenőrzés során.

2) Az Ügyfél úgy szerzett tudomást a támadásról, hogy azt maga a támadó (etikus hacker) jelezte neki […]. A jelzésében a támadó jelezte, hogy – elmondása szerint – csak az érintett adatbázis egy sorát kérte le bizonyítékként, szándékai pedig segítő jellegűek, ezért a hiba technikai jellegét is ismertette Ügyfél előtt. Az Ügyfél ezek után a hibát kijavította, […].

Az incidenssel érintett adatok nagyobb része (kb. […] fő) egy […]-én tesztelési célból létrehozott […] megnevezésű adatbázis részét képezték. A tesztadatbázis létrehozásának okát és célját az Ügyfél naplófájlok, rendszer riasztások és levelezések megvizsgálása útján kísérelte meg rekonstruálni. Mivel a feltételezett feltöltési időpontra vonatkozó naplófájlok és riasztások már nem álltak rendelkezésre így az események egyértelmű rekonstruálására nem volt lehetősége az Ügyfélnek. Egy tesztelő kolléga […] e-mailjéből derült ki, hogy […]-én jelentkezett egy hiba, amely során a webszerverek nem érték el az adatbázis szervereket. Ennek eredményeképpen az előfizetői adatok elérhetősége megszűnt. Az Ügyfél feltételezése szerint ezen hiba ideiglenes kiküszöbölése céljából kerültek feltöltésre a tesztadatbázisba az adatok, az előfizetői adatok elérhetőségének biztosítása érdekében.

A hiba kiküszöbölése kapcsán létrehozott fenti tesztadatbázisba betöltött adatok forrását az Adatkezelő ügyfelei által korábban megadott személyes adatok képezték. Az ügyfelek különböző igénybejelentéseik során adták meg személyes adataikat online vagy egyéb értékesítési csatornán keresztül […]. A tesztadatbázisba betöltött adatokat eredményező legkésőbbi […] dátummal volt ellátva. Ebben az adatbázisban kb. […] természetes személy által megadott adat volt megtalálható.

A fenti hiba elhárítását, így az elérések helyreállítását követően a tesztadatbázisba feltöltött adatokat törölni kellett volna, ez azonban mulasztás következtében elmaradt. Ezen adatoknak a fenti sérülékenységen keresztüli elérhetőségéről a támadó bejelentéséig nem volt tudomása az Ügyfélnek. Az adatokhoz való hozzáférést a támadó részéről az Ügyfélnek nem sikerült detektálnia (pl. hálózatbiztonsági eszköz jelzése alapján), mielőtt arra maga a támadó felhívta volna a figyelmét.

A tesztadatbázison túl a felfedezett sérülékenységen keresztül a támadónak lehetősége volt hozzáférni az Ügyfél által fenntartott digi.hu honlap mögötti másik, […] adatbázishoz is, amely az oldalon hírlevélre feliratkozó érintettek személyes adatait tartalmazta. Itt kb. […] természetes személy által megadott adat (név, e-mail cím) volt megtalálható. A vizsgálatok alapján ebben az adatbázishoz tárolt konkrét személyes adatokhoz azonban nem mutatható ki jogosulatlan hozzáférés az Ügyfél szerint. A sérülékenység miatt a hozzáférés veszélye azonban ezen adatok tekintetében is fennállt.

3) A konkrét sérülékenység a […] oldalon keresztül állt fent. Itt a „rendezés mezőn” keresztül volt kihasználható a weboldal sérülékenysége. A jogosulatlan hozzáférést lehetővé tevő hiba oka, hogy

az Ügyfél által használt […][1] tartalomkezelő rendszerben megtalálható volt egy biztonsági rés, amit kihasznált a támadó. A biztonsági rés egyébként már több mint 9 éve ismert volt és rendelkezésre állt hozzá javítás is, amit azonban az Ügyfél korábban nem telepített. Ennek oka, hogy a javítás nem képezte részét a szoftverhez hivataloson kiadott javítás-csomagoknak. Az incidenst követően a javítócsomag[2] telepítése megtörtént.

Az Ügyfél további jogosulatlan hozzáférést az érintett adatokhoz a biztonsági résen keresztül nem mutatott ki. Más körülmény sem utalt arra, hogy esetleg az adatokhoz más is hozzáférhetett volna az etikus hackeren kívül.

4) Ügyfél tájékoztatta továbbá a Hatóságot, hogy a hasonló adatvédelmi incidensek megelőzése érdekében rendszeresen ellenőrzi az általa kezelt adatbázisokat, hogy konkrét cél nélkül ne kerüljenek kezelésre/tárolásra személyes adatok. Az adatbázisokat továbbá időről-időre megtisztítja, ellenőrzi azok biztonságát, azonosítja a hozzájuk kötődő alkalmazásokat és adatgazdákat. Ezen felül további külső vizsgálat eredményeképpen megfontolja, hogy magasabb szintű tűzfalat szerezzen be és üzemeltessen.

Az Ügyfél belső szabályzattal rendelkezik, amely alapján az általa használt alkalmazásokat naprakészen kell tartani, azokat rendszeresen e célból ellenőrizni szükséges. Az incidens megtörténtekor a […] rendszer (amellyel az érintett adatbázis kezelve volt) legfrissebb verzióját alkalmazta, a sérülékenységet javító nem hivatalos javítást, azonban ez nem tartalmazta. Maga a sérülékenység egyébként a […] volt benne. Ezzel kapcsolatban az Ügyfél előadta, hogy mivel a hivatalos verzióhoz rengeteg nem hivatalos javítást adnak ki, ezeket nincs lehetősége ellenőrizni.

A nyílt forráskódú tartalomkezelő használatát illetően Ügyfél […], elmondása szerint azért választotta ezt a rendszert, mivel az ingyenes, az egész világon széleskörűen használt, valamint egy folyamatosan tesztelt és támogatott szoftver.

Az Ügyfél […] rendszerességgel végzi el az általa használt rendszerek sérülékenységvizsgálatát az […] segítségével. Ez a vizsgálat azonban az adatvédelmi incidens bekövetkezésének időpontjáig nem terjedt ki a digi.hu weboldalra. Az incidens után a vizsgálatot kiterjesztette az Ügyfél erre a weboldalra is.

[…]

A sérülékenységet jelentő támadó […]. Az incidenssel érintett […] megnevezésű tesztadatbázist Ügyfél is törölte időközben.

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

1) A tényállás további tisztázásán túl az ügyben az általános adatvédelmi rendelet 5. és 32-34. cikkeiben foglalt kötelezettségek Ügyfél 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 adatvédelmi hatósági eljárás megindításáról döntött 2019. december 16. dátummal.

[1] […]

[2] […]

Az ügyben a hatósági ellenőrzés során megállapítottakon túl a tényállás további tisztázása vált szükségessé, ezért a Hatóság NAIH/2020/1160. és NAIH/2020/1160/3. számú végzéseivel nyilatkozattételre és iratszolgáltatásra szólította fel az Ügyfelet, amelyekre az határidőben válaszolt. Az Ügyfél nyilatkozatai alapján a Hatóság a hatósági ellenőrzésben tisztázott körülményeken túl az alábbiakat állapította meg a hatósági eljárás során.

2) Az Ügyfél bemutatta részletesen egy ábra és leírás segítségével az incidensben érintett szerverek és más hálózati elemek struktúráját és az adatbázisok helyét. Ezek alapján az incidenssel érintett adatállományok […][3] […] voltak elérhetőek, amelyek az érintett hálózaton a […] (lásd az alábbi ábrát).

[…]

Az adatbázis létrehozására és további kezelésére a […] használta az Ügyfél.

Az incidenssel érintett […] tárolt személyes adatok nem kerültek titkosításra Ügyfél nyilatkozata alapján. Ennek oka, hogy a […] vonatkozó titkosítás követelménye nem jelenik meg a belső szabályzatokban.

Az Ügyfél elmondása szerint az adatbázis […] azért sem tartotta indokoltnak, mivel a személyes adatok védelme a hozzáférések korlátozásával és megfelelő jogosultságkiosztással elvileg biztosított, továbbá az ilyen titkosítás alkalmazása az adatbázisok alkalmazhatóságában és működésében problémát okozhat. A konkrét probléma okát az Ügyfél részletesen nem indokolta.

Az Ügyfélnél egyébként az informatikai rendszerekben való titkosítás alkalmazása általánosságban megjelenik a […] megnevezésű szabályzatában. A szabályzat releváns pontjait az Ügyfél megküldte a Hatóság ezirányú kérésére.

3) A Hatóság kérésére az Ügyfél részletesen leírta, hogy a támadónak hogyan sikerült kiviteleznie a támadást és hozzáférnie az adatbázis-[…]ban tárolt személyes adatokhoz. A módszert maga a támadó ismertette az Ügyféllel. Ezek alapján a támadó egy úgynevezett […] támadást futtatott az érintett digi.hu weboldalon. Ezen támadás végrehajtása az Ügyfél véleménye szerint időigényes feladat és csak célzatosan, az illetéktelen hozzáférés szándékával hajtható végre, továbbá annak kivitelezése magas szintű technikai tudást igényel. A támadás során a támadó által végrehajtott […] oldalon sérülékenységet jeleztek, amin keresztül elérhetővé és kilistázhatóvá vált a […] tesztadatbázisban található […] összesen […] darab sora.

Az Hatóság kérésére az Ügyfél részletesen ismertette, hogy az incidenssel érintett két külön adatbázis esetében pontosan milyen adatkategóriák kerültek kezelésre, mi volt ezen adatok kezelésének célja és jogalapja, valamint, hogy pontosan hány érintett személyes adatai kerültek kezelésre.

- Előfizetői adatokat tartalmazó […] megnevezésű tesztadatbázis: érintett neve, születési neve, anyja neve, születési helye és ideje, lakcíme, személyi igazolvány száma, esetenként személyi száma, e-mail címe, vezetékes és mobil telefonszáma, bankszámlaszáma, szerződéssel kapcsolatos adatok, igénybevett szolgáltatással kapcsolatos adatok. Az adatkezelés célja ebben az esetben az előfizetői szerződés megkötése. Az adatkezelés jogalapja: az általános adatvédelmi rendelet 6. cikk (1) bekezdés b) pontja (az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél). Az

[3] […]

adatbázisban összesen […] érintett személyes adatait kezelték. Ez a szám az Adatkezelő lakossági ügyfeleinek összesen […]%-át teszi ki.

- Hírlevélre feliratkozók adatait tartalmazó élő […] nevű, a digi.hu honlaphoz köthető adatbázis: név és e-mail cím. Az adatkezelés célja ebben az esetben az érintettek üzletszerzési célú, az Ügyfél által kínált ajánlatokkal történő megkeresése (direkt marketing). Az adatkezelés jogalapja: az általános adatvédelmi rendelet 6. cikk (1) bekezdés a) pontja (az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez). Az adatbázisban összesen […] érintett személyes adatait kezelték. Ez a szám az Adatkezelő lakossági ügyfeleinek összesen […]%-át teszi ki.

Az Ügyfél továbbította a Hatóság részére az incidenssel érintett adatállományok kezelésével kapcsolatos adatkezelési szabályzatait és belső adatvédelmi incidenskezelési eljárásrendjét.

4) Az Ügyfél ismertette a Hatósággal a digi.hu weboldalon fennállt sérülékenység technikai leírását, amelyet a támadó is közölt vele üzenetében.

Az etikus hacker által küldött, a sérülékenységet leíró e-mail üzenetből kiderül, hogy a […] megnevezésű ([…] adatsort tartalmazó) adatbázis mellett az incidensben érintett […] megnevezésű adatbázis a digi.hu honlapon a hírlevélre feliratkozó érintettek személyes adatai mellett a digi.hu honlap felületéhez tartalmaz hozzáférési adatokat. Ebben a […] megnevezésű adatbázisban a […] megnevezésű […] részleges / teljes jogú rendszergazda felhasználó adatai is kiolvashatóak az etikus hacker levele szerint. Ezen adatok között szerepel a […]. Ezen adatok az üzenet szerint hozzáférést engedhetnek a digi.hu honlap adminisztrációs felületéhez.

A fentiek alapján az etikus hacker e-mail üzenete szerint az incidensben érintett adatbázisokat és személyes adatokat az alábbi táblázat szemlélteti:

Adatbázis neve	Érintettek száma	Adatok típusa
[…]	[…] előfizető	Név, születési név, születési hely és idő, anyja neve, e-mail cím, jelszó, mobiltelefonszám, bankszámlaszám, igazolványszám, tulajdonosi jogkör (tulajdonos vagy bérlő), fizetési mód, fizetési hajlandósággal kapcsolatos adatok (pl. inkasszó), szerződéssel kapcsolatos adatok, igénybevett szolgáltatás típusa, szolgáltatás kezdetének/végének dátuma.
[…]	[…] hírlevélre feliratkozó […] részleges / teljes jogú rendszergazda	Hírlevélre feliratkozók: név, e-mail cím Rendszergazdák: […]

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

II. Alkalmazott jogszabályi rendelkezések

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

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

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

Az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontja szerint a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; […] („célhoz kötöttség”).

Az általános adatvédelmi rendelet 5. cikk (1) bekezdés e) pontja szerint a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; […] („korlátozott tárolhatóság”).

Az általános adatvédelmi rendelet 5. cikk (2) bekezdése alapján az adatkezelő felelős a 5. cikk (1) bekezdésében foglalt alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

Az általános adatvédelmi rendelet 17. cikk (1) bekezdés a) pontja alapján az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha […] a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték.

Az általános adatvédelmi rendelet 32. cikk (1) bekezdés a) pontja szerint az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja ideértve, többek között, adott esetben a személyes adatok álnevesítését és titkosítását.

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

Az általános adatvédelmi rendelet 33. cikk (1)-(2) és (4)-(5) bekezdései szerint az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával

azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek. Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők. Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

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

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

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 61. § (1) bekezdés a) pontja alapján a Hatóság a 2. § (2) és (4) bekezdésében meghatározott adatkezelési műveletekkel összefüggésben az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja.

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

A közigazgatási bírság kiszabására vonatkozó feltételeket az általános adatvédelmi rendelet 83. cikke tartalmazza. Az Infotv. 75/A. § - a szerint a Hatóság az általános adatvédelmi rendelet 83. cikk (2)-(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi rendelet 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik.

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

III. Döntés

a. Az általános adatvédelmi rendelet alkalmazhatósága

Az általános adatvédelmi rendelet 99. cikk (2) bekezdése alapján a rendeletet 2018. május 25-től kell alkalmazni. Az adatvédelmi incidenssel érintett […] megnevezésű tesztadatbázis az Ügyfél nyilatkozata alapján […] került létrehozásra tesztelési, hibaelhárítása célokból.

A digi.hu honlaphoz köthető adatokat tartalmazó […] megnevezésű adatbázis direkt marketing célú, hírlevélre feliratkozók adatait és a honlap felületéhez való hozzáférésre lehetőséget adó rendszergazdai adatokat tartalmazott, amelyek nem teszt-, hanem élő, naprakész adatok voltak.

Az Ügyfél arról, hogy a két fenti adatbázishoz a digi.hu honlap egyik sérülékenységét kihasználva hozzá lehet kívülről jogosulatlanul férni legkorábban 2019. szeptember 23-án értesült a biztonsági hibát feltáró etikus hackertől. Az incidenssel érintett adatkezelés, nevezetesen az ügyféladatok tárolása az incidenssel érintett adatbázisokban, az általános adatvédelmi rendelet alkalmazandóvá válása után is fennállt. Az adatkezelésre ezért mind a 99. cikk (2) bekezdésében foglaltak, mind a tárgyi hatályra vonatkozó, a 2. cikk (1) bekezdésében foglalt előírások alapján alkalmazni kell a rendelet előírásait.

A fentieken túl megjegyzendő, hogy az általános adatvédelmi rendelet adatvédelmi incidensek kezelésére vonatkozó rendelkezései alkalmazása szempontjából az incidensről való tudomásszerzés a releváns időpont, hiszen az előírt jogkövetkezményeket a rendelet ehhez az időponthoz köti. Ebből a szempontból azon tény, hogy az incidenssel érintett és az elégtelen adatbiztonsági intézkedések alkalmazásával kezelt tesztadatbázis létrehozására mikor került sor és abban az érintettektől mikor gyűjtött adatok szerepelnek nem releváns tényező. Mind az incidens bekövetkezésével, mind az adatbiztonság nem megfelelő szintjével kapcsolatosan az érintettek jogaira és szabadságaira jelentett kockázatok a rendelet alkalmazandóvá válása után is fennálltak.

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

A Hatóság a feltárt tényállás alapján megállapította, hogy a bekövetkezett adatvédelmi incidensről az Ügyfél saját elmondása szerint legkorábban akkor szerzett tudomást, amikor azt az érintett digi.hu honlapon sérülékenységi vizsgálatot lefolytató etikus hacker e-mailben jelezte a részére […]. Korábban a sérülékenység fennállásáról az Ügyfélnek nem volt tudomása. A támadó által elvégzett sérülékenység vizsgálatot, az érintett adatbázisokban lévő adatkategóriák kilistázását és a tesztadatbázisban tárolt adatokhoz való hozzáférést az Ügyfélnek nem sikerült magától detektálnia, így az incidensről és azt lehetővé tévő sérülékenységről pusztán az azt elkövető etikus hacker 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. Az Ügyfél incidensbejelentése és a tényállás tisztázása kapcsán megállapítható, hogy a személyes adatokat tartalmazó tesztelési és hibaelhárítási célból létrehozott tesztadatbázishoz a támadónak az Ügyfél által fenntartott digi.hu honlapon keresztül elérhető sérülékenység kihasználásával sikerült hozzáfernie. A személyes adatok jogosulatlan megismerésére tehát egy informatikai biztonsági hiányosság kihasználásával kerülhetett sor, amely így adatvédelmi incidenst eredményezett.

Az általános adatvédelmi rendelet 33. cikk (1) bekezdése szerint fő szabályként az adatvédelmi incidenst be kell jelenteni a felügyeleti hatóságnak. A rendelet ezen bekezdése és a (85) preambulumbekezdése is kimondja, hogy a bejelentéstől az adatkezelő csak abban az esetben tekinthet el, ha az elszámoltathatóság elvével[4] összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Mivel a főszabály az incidens hatóságoknak való bejelentése, az ez alóli kivétel is szűken értendő.

Az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak szerint, ha az adatkezelésből – így jelen ügyben a lakossági ügyfelek és rendszergazdák adatainak tárolásából – személyazonosság-lopás vagy személyazonossággal való visszaélés fakadhat, úgy az alapvetően kockázatosnak minősül.

Az Ügyfél által tesztelési és hibajavítási célból létrehozott adatbázisban tárolt adatok (érintett neve, születési neve, anyja neve, születési helye és ideje, lakcíme, személyi igazolvány száma, esetenként személyi száma, e-mail címe, vezetékes és mobil telefonszáma, fizetési és banki adatok, igényelt szolgáltatással kapcsolatos adatok) ismeretében pedig elkövethető személyazonosság-lopás, vagy személyazonossággal visszaélés.

A biztonsági sérülésen keresztül elérhető másik, a digi.hu honlaphoz köthető, […] megnevezésű adatbázisban tárolt adatokhoz (hírlevélküldési célú és rendszergazdai adatok) tekintetében az etikus hacker szintén jelezte ezen adatok sérülékenységét, habár konkrét adatokat nem kért le, csak az elérhető adatok típusait listázta ki a rendszergazdák tekintetében ([…]). Ettől függetlenül a biztonsági intézkedések hiányosságai, így a jogosulatlan hozzáféréstől való védelem nem megfelelő szintje ezen adatok tekintetében is fennállt.

A fentiek alapján a Hatóság megítélése szerint az adatvédelmi incidens kockázatosnak tekinthető, ezért amennyiben egy ilyen esetről az adatkezelő tudomást szerez, úgy azt be kell jelentenie az általános adatvédelmi rendelet 33. cikk (1) bekezdése alapján a felügyeleti hatóságnak. A bejelentést az Adatkezelő 2019. szeptember 25-én tette meg a Hatóság felé, így ez irányú kötelezettségét az incidens tudomására jutásától számított 72 órán belül teljesítette. A Hatóság a bejelentési kötelezettség teljesítésével kapcsolatos jogsértést ezért nem állapított meg.

Az incidens kapcsán az Adatkezelő ismertette az abból eredő esetleges hátrányos következmények enyhítését célzó intézkedéseit. Ezek alapján a cél nélkül kezelt tesztadatbázist törölte, valamint telepítette azt a javítást, amely a használt […] rendszerben fennálló sérülékenységet megszüntette. Az Ügyfél már az incidens bekövetkezése előtt is alkalmazott olyan szervezési intézkedéseket, amelyekkel igyekezett kiszűrni a feleslegesen, cél nélkül kezelt adatokat, adatbázisokat, azonban ennek kapcsán az érintett tesztadatbázis nem került korábban detektálásra. Az Ügyfél ezen felül úgy nyilatkozott, hogy megfontolja magasabb szintű tűzfalak beszerzését a védelem szintjének növelése érdekében, továbbá az egyébként is végzett rendszeres sérülékenységi vizsgálatokat és […] a digi.hu weboldalra is kiterjeszti a jövőben.

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

c. Az incidenssel érintett adatok tárolásával kapcsolatos adatbiztonsági intézkedések

Az adatkezelés biztonságával kapcsolatban a rendelet 32. cikk (1) bekezdése kimondja, hogy többek között a tudomány és technológia állása és a felmerülő kockázatok figyelembevételével az adatkezelő feladata, hogy az adatok biztonságát megfelelő technikai és szervezési intézkedésekkel garantálja. Ezen cikk (1) bekezdés a) pontja ide érti adott esetben a személyes adatok álnevesítését és titkosítását.

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

1) Az incidensbejelentésben közölt információk és a hatósági ellenőrzés majd eljárás során megállapított tényállás alapján az adatvédelmi incidens bekövetkezése arra vezethető vissza, hogy az Ügyfél által tartalomkezelésre használt […] rendszerben – amellyel az incidenssel érintett adatbázisok is kezelve voltak – fennállt egy az incidens bekövetkezésekor már régóta ismert és javítható sérülékenység. Az Ügyfél ezen sérülékenységet elmondása szerint nem javította ki az incidens bekövetkezéséig, mivel az arra szolgáló javítócsomag nem képezi részét a szoftver hivatalosan kiadott változatának. Az Ügyfél a […] elérhető nem hivatalos javításokat nem követi, nem monitorozza, mivel – a szoftverhez készülő nem hivatalos javítások számossága miatt – arra elmondása miatt nincs lehetősége, kapacitása. Az Ügyfél rendszeres sérülékenységvizsgálatot végez az általa kezelt rendszerekben, azonban ez az incidens bekövetkezéséig a digi.hu weboldalra nem terjedt ki.

Az Ügyfél Informatikai Biztonsági Szabályzatának […] értelmében […].

Az incidenssel érintett ügyféladatok kezelése – a határozat III./b. pontjában foglaltak alapján is – az adatkategóriák tartalma alapján kockázatosnak tekinthető. A kockázatokat jelentősen növelő tényező, hogy az Ügyfél által kezelt adatbázisban nagyszámú érintett személyes adatai voltak megtalálhatóak:

- […] nevű tesztadatbázis: […] érintett előfizető, az Adatkezelő lakossági ügyfeleinek összesen […]%-a,
- […] nevű adatbázis: […] érintett feliratkozó, az Adatkezelő lakossági ügyfeleinek összesen […]%-a, ezen felül […] részleges / teljes jogú rendszergazda a digi.hu honlaphoz köthető hozzáférési adatai.

Ezek tehát olyan, összesen […], az Adatkezelő lakossági ügyfeleinek több mint […], a magyarországi lakosság arányában is jelentős számú érintettet érintő érzékeny adatkezelések, amelyek – az általános adatvédelmi rendelet (75) preaumbulumbekezdése alapján – az érintettek jogaira és szabadságaira jelentős kockázatokkal járnak. A rendelet 32. cikkében foglaltak alapján az adatkezelő kötelezettsége, hogy a kockázatokkal arányos adatbiztonsági intézkedéseket alkalmazzon.

Az Ügyfél által végzett tesztelési, hibajavítási tevékenység a […] megnevezésű ügyféladatbázis kapcsán egyébként nem jelentene problémát, ha egyidejűleg az ilyen adatkezeléssel jelentett kockázatokkal arányos biztonsági intézkedések is alkalmazásra kerülnek. Az Ügyfél belső információbiztonsági szabályzatai is tartalmaznak azzal kapcsolatos előírásokat, hogy a használt rendszerek kapcsán fel kell mérni előzetesen a kockázatokat, ennek során feltérképezni a korábbi

biztonsági réseket és a rendelkezésre álló javításokat, továbbá megfelelő titkosítást kell alkalmazni. Ezen felül a rendszereket rendszeresen vizsgálni kell az esetleges sérülékenységek feltárása érdekében.

2) Az Ügyfél megküldte a Hatóságnak a digi.hu weboldalon fennállt sérülékenység technikai leírását, amelyet a támadó közölt vele üzenetében. A Hatóság IT biztonsági szakértője megvizsgálta a sérülékenység támadó általi leírását és az Ügyfél által azzal kapcsolatban közölt információkat. Ennek leírását a NAIH/2020/1160/5. ügyiratszámú információbiztonsági szakértői vélemény tartalmazza, amely az Ügyféllel az Ákr. 76. §-a alapján a NAIH/2020/1160/7. számú végzéssel került ismertetésre.

A szakvéleményben foglaltak szerint megállapítható, hogy a támadó által elvégzett sérülékenységvizsgálat alapján […] sérülékenységről van szó. A hiba ezen fajtájára az jellemző, hogy […]. Léteznek azonban olyan webes sérülékenységeket vizsgáló applikációk, amelyek ki tudják szűrni az […] sérülékenységeket automatizmussal is. Ilyen pl. az Ügyfél által is hivatkozott és használt […] is széles körben használatosak ebből a célból. Ezen […] szoftverek használata egyébként különösen „magas szintű informatikai tudást”, illetve kódfejtő képességét nem igényel, azok kezelését egy a téma iránt érdeklődő, informatikai biztonsági kérdésekben közepesen jártas személy is el tudja némi gyakorlás, időráfordítás után sajátítani.

A támadó által leírt sérülékenységi vizsgálat paraméterei azt mutatják, hogy a sérülékenység a […] keresztül volt megtalálható. Ezen a linken a […] volt sérülékeny, vagyis a […] volt kihasználható […] sérülékenység. A szakértői vizsgálat szerint sikeresen kinyerhető a releváns adatbázisokon ([…] megnevezésű adatbázisok) belül található adatbázis […]. Ezeken belül további adatokat lehet megismerni, amennyiben […], így megismerhetők […] (a konkrét személyes adatok).

Az érzékeny adatoknak az adatbázisban szabad szöveges („plain text”) formában történő tárolása magas szintű biztonsági probléma a szakértői vélemény szerint, amelyet megfelelő titkosítás használatával lehet kiküszöbölni. Az Ügyfél által is említett […] használatával megakadályozható lett volna az érintett […] adatbázis konkrét tartalmának megismerése.

Az etikus hacker által küldött, a sérülékenységet leíró e-mail üzenetből derült ki az is, hogy a […] megnevezésű adatbázisból […] részleges / teljes jogú rendszergazda felhasználó adatai is kiolvashatóak. Ezen adatok között szerepel […]. Az ilyen érzékeny, rendszergazdai szintű adatokhoz való hozzáférés lehetősége szintén nagymértékben növeli az incidens kockázatait, mivel ezen adatok birtokában könnyen elkövethető személyiséglopás, illetve további akár további adatokhoz való illetéktelen hozzáférés is.

3) Az Ügyfél a fenti IT biztonsági szakvéleménnyel kapcsolatban eljuttatta észrevételeit és megjegyzéseit a Hatóságnak, miután az vele a Hatóság által az Ákr. 76. §-a alapján a NAIH/2020/1160/7. számú végzéssel ismertetésre került.

Ezek alapján az Ügyfél ismét hangsúlyozta, hogy az etikus hacker csak a […] adatbázis egyik sorát kérte le bizonyítékként és ismertette levelében, további illetéktelen hozzáférésre pedig nincs bizonyíték. A Hatóság ezen tényt jelen határozatával nem vitatja. A határozat jelen pontjában (III. fejezet / c. pont) értékelt adatbiztonsági hiányosságok ettől a körülménytől függetlenül valamennyi, az érintett adatbázisokban kezelt személyes adattal kapcsolatban fennálltak és ezért az érintettekre jelentett kockázatok az összes kezelt személyes adattal kapcsolatba hozhatók.

Az Ügyfél kiemelte továbbá, hogy a sérülékenység detektálásához szükséges magas szintű informatikai tudás mellett szól annak időigényes és bonyolult volta. A Hatóság ezzel kapcsolatban megjegyzi, hogy a sérülékenységek feltárására alkalmas említett szoftverek automatikusan képesek detektálni a biztonsági réseket, bárki számára könnyen (adott esetben ingyenesen) hozzáférhetőek, a konkrét felhasználó részéről ezért konkrét kódfejtő tudást nem igényel a használatuk.

Az Ügyfél nyilatkozatában ismét kiemelte, hogy mivel az adatbázishoz való hozzáférés-kontroll elméletileg jogosultságkiosztással biztosított, ezért nem tartotta indokoltnak a titkosítás alkalmazását. A […] adatbázis tábla […] titkosítása továbbá az Ügyfél szerint értelmezhetetlennek tűnik, mivel az érintett személyes adatok közül voltak olyanok is (pl. nevek, címek, telefonszámok), amelyek titkosítása jelen esetben problémát okozott volna az adatbázis alkalmazhatóságában és működésében. Ennek indokait az Ügyfél a továbbiakban nem részletezte. A Hatóság ezzel kapcsolatos megállapításait lásd jelen határozat III. fejezet c. pont 5) alpontjában.

Az Ügyfél végül felhívta a Hatóság figyelmét arra, hogy a […] munkavállaló (rendszergazdák, adminisztrátorok, felhasználók) […]. A Hatóság nem vitatja a fentieket, megjegyzi azonban, hogy ettől függetlenül a […] adathoz való hozzáférés lehetősége önmagában is súlyos biztonsági kockázatnövelő tényezőnek tekinthető.

4) Az Ügyfél által használt, a sérülékenységgel érintett tartalomkezelő rendszer ([…]) hibája 9 éve közismert volt az azt kijavító megoldási módszerrel együtt. Az ezzel kapcsolatos bejegyzések a szoftver hivatalos honlapján, az ottani fórumon kerültek nyilvánosan ismertetésre.[5] A hibára javítócsomagot hivatalosan nem készítettek, nem hivatalos javítás azonban rendelkezésre állt, az nyilvánosan és ingyenesen elérhető volt bárki számára.

A biztonsági rés a digi.hu weboldal etikus hacker általi sérülékenység-vizsgálata kapcsán került detektálásra. Ennek vizsgálatára az Ügyfél által is más rendszerek ellenőrzésére használt […] szoftver is alkalmas. Ezen vizsgálatokat korábban a weboldal kapcsán az Ügyfél azonban mellőzte, így a sérülékenységet sem detektálhatta. A nyilvánosan elérhető, ügyfelek által látogatott weboldal kapcsán a biztonsági vizsgálatok mellőzése így lehetővé tette, hogy a sérülékenységre ne derüljön fény egészen a konkrét incidens bekövetkezéséig. A rendszeres sérülékenységvizsgálattal a hiba kiszűrhető lett volna, ezt az etikus hacker vizsgálata is bizonyítja. Ebből a szempontból a fennálló sérülékenység javítására alkalmas szoftverkomponens „nem hivatalos” volta irreleváns tényező, mivel annak a hiba fennállása és detektálhatósága kapcsán nincs jelentősége. A fokozott figyelmet és intézkedéseket a használt rendszerek biztonsági réseit illetően az Ügyfél belső szabályzatai is előírják.

Az interneten nyilvánosan elérhető és (adott esetben nagyszámú) ügyfelek által is látogatható weboldalak kapcsán az esetleges sérülékenységekre való felkészültség fokozottan elvárható a fenntartók részéről. Ez a tudomány és technológia állása és a megvalósítás költségei szempontjából nem okozhatna az Ügyfélnek sem jelen esetben különösebb gondot, figyelemmel a piacon elfoglalt pozíciójára is. A weboldal és minden más interneten elérhető rendszer rendszeres sérülékenységvizsgálatának előírásáról az Ügyfél is intézkedett az incidens után, elismerve ennek szükségességét.

Az incidensben érintett adatbázisok kezelésének biztonsági szintje ezért nem felelt meg az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseiben foglalt előírásoknak, mivel a régóta

[5] […]

ismert, egyébként kiszűrhető és javítható biztonsági hiba, továbbá a digi.hu oldal sérülékenységi vizsgálatainak elmaradása lehetővé tette a személyes adatokhoz való jogosulatlan hozzáférést.

5) Az Ügyfél arról is tájékoztatta a Hatóságot, hogy az érintett adatbázisokban nem került sor titkosítás alkalmazására a személyes adatokon ([…]). Ezt az etikus hacker által küldött üzenet is megerősíti, mivel az abban foglaltak alapján az adatbázisból lekérhetővé váltak a konkrét személyes adatok, olvasható formában. Ennek bizonyítására az etikus hacker lekérte az érintett […] adatbázis egy sorát, amelyet az Ügyféllel is közölt.

Az Ügyfél Informatikai Biztonsági Szabályzatának […].

Az adatbázisokat az Ügyfél a […] szoftvert használva hozta létre, amelyben lehetőség van az adatok […] titkosítására. Az alkalmazott technológia kapcsán a kezelt személyes adatokon a titkosítás használatára megvolt tehát a lehetőség, alkalmazása többletköltséget sem jelenthet. Az Ügyfél nyilatkozata alapján ennek ellenére eltekint az általa kezelt […] adatbázisokban a titkosítás alkalmazásától, így az incidenssel érintett adatbázisoknál sem alkalmazta ezt a lehetőséget. Ennek okaként az Ügyfél azt jelölte meg, hogy a személyes adatok védelme a hozzáférések korlátozásával és megfelelő jogosultságkiosztással elvileg biztosított, továbbá az ilyen titkosítás alkalmazása az adatbázisok alkalmazhatóságában és működésében problémát okozhat. A lehetséges problémákat az Ügyfél nem részletezte.

A titkosítás használatának hiányában azonban jelen esetben az incidenssel érintett adatbázisokban tárolt személyes adatok túlnyomó része kiolvashatóvá, jogosulatlanul megismerhetővé vált. Ezen tény az bekövetkezett adatvédelmi incidens kapcsán pedig az érintettekre jelentett kockázatokat jelentősen megnövelte.

A személyes adatok titkosítását általánosságban az általános adatvédelmi rendelet 32. cikk (1) bekezdés a) pontja is említi, mint megfelelő biztonsági intézkedést.

Az Ügyfél ugyan nem részletezte, hogy az adatbázis […] titkosítását miért tartja ezzel a konkrét adatkezeléssel kapcsolatban problémásnak, azonban ennek hiányában is törekednie kell az érzékeny és nagy számban kezelt személyes adatok kiszivárgása elleni védelemre. A titkosítás elmaradásának pontos okait pedig az általános adatvédelmi rendelet 5. cikk (2) bekezdése alapján igazolnia kell tudni.

Mivel a titkosítás elmaradása a bekövetkezett incidens, továbbá az alkalmazott biztonsági intézkedéseknek az érintettekre jelentett kockázatait jelentősen megnövelte, ezért az általános adatvédelmi rendelet 32. cikk (1) bekezdés a) pontjának, továbbá ezzel kapcsolatos saját belső szabályzatának való megfelelés érdekében a Hatóság felszólította jelen határozattal az Ügyfelet, hogy a kockázatok csökkentése céljából vizsgálja felül az általa kezelt valamennyi személyes adatokat tartalmazó adatbázist abból a szempontból, hogy azokban indokolt-e titkosítás alkalmazása és ennek eredményeiről – az elszámoltathatóság elvéből is következően – tájékoztassa a Hatóságot.

6) A Hatóság a fentiekre tekintettel ezért megállapította, hogy az Ügyfél nem tett eleget az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseiben foglalt, az adatbiztonsággal kapcsolatos jogszabályi előírásoknak.

d. Az incidenssel érintett tesztadatbázis kezelésének megfelelése egyes alapelveknek

1) Az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontjában nevesített „célhoz kötöttség” elve megköveteli, hogy a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon.

A 29-es Adatvédelmi Munkacsoport kapcsolódó véleménye (WP203) szerint a célhoz kötöttség lényege, hogy megakadályozza az adatok olyan célú felhasználását, amelyre az érintettek nem számíthatnak előre, tiltakoznának ellene, vagy egyébként sem alkalmasak az adatok az ilyen célok elérésre. Az alapelv két további részelvből tevődik össze, nevezetesen először a cél meghatározásának kötelezettségéből és másodszor pedig az ezzel összefüggő felhasználás kötelezettségéből.

Az Ügyfél az incidenssel érintett tesztadatbázis létrehozásának célját abban jelölte meg, hogy […]-én jelentkezett egy hiba, amely miatt az előfizetői adatok elérhetősége megszűnt. Ezen hiba kijavítása céljából lett létrehozva a mintegy […] érintett, az Adatkezelő lakossági ügyfeleinek összesen […]%-ának különböző, az előfizetői szerződések megkötése során megadott adatait tartalmazó tesztadatbázis. Ezen adatbázis létrehozásának célja (hibajavítás) tehát elkülönül a személyes adatok eredeti kezelésének céljától (szerződés teljesítése). A hibajavítás, mint önálló adatkezelési cél legitim lehet, azonban ezen elkülönült adatkezelésnek is meg kell felelnie az általános adatvédelmi rendelet előírásainak, így többek között a célhoz kötött adatkezelés alapelvének is.

A hibajavítási cél a tesztadatbázis létrehozása kapcsán addig áll fent, ameddig maga a hiba elhárításra nem került az Adatkezelő által. Amint a hiba kijavítása megtörtént az elkülönült adatkezelési cél is megszűnik, így az általános adatvédelmi rendelet 17. cikk (1) bekezdés a) pontjában foglaltakra is figyelemmel a személyes adatokat tartalmazó tesztadatbázist törölni kellett volna. Az adatbázis a hiba elhárítása utáni tárolása már nélkülözött bármilyen adatkezelési célt, amelyre maga az Ügyfél is utalt a Hatóságnak küldött válaszaiban (lásd: az Ügyfél a Hatóság NAIH/2019/7105/4. számú tényállás tisztázó végzésére adott 2019. november 28-án kelt nyilatkozatának 4. pontját).

A nagyszámú érzékeny ügyféladatot tartalmazó adatbázis cél nélküli tárolása ezért majd […], a hiba elhárításától egészen az incidens bekövetkezéséig fennállt. Az Ügyfél ezen adatkezelési tevékenysége ezért megsértette az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontjában nevesített „célhoz kötöttség” alapelvét.

2) Az általános adatvédelmi rendelet 5. cikk (1) bekezdés e) pontjában nevesített „korlátozott tárolhatóság” elve megköveteli, hogy a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

A célhoz kötöttség alapelvével szorosan összefüggő ezen alapelv az elavult, már semmilyen célból nem használható személyes adatok tárolásának tilalmát fogalmazza meg. Az alapelv azonban a tárolási idő behatárolását az érintettek azonosítására alkalmas módon való adattárolás szempontjából korlátozza. Az anonimizált adatok tárolására így továbbra is lehetősége van az adatkezelőnek, azonban annak olyan formában kell történnie, hogy biztosan ne lehessen belőlük az érintettre következtetést levonni, őket a továbbiakban azonosítani.

Az Ügyfél által hibaelhárítási célból létrehozott adatbázisban kezelt személyes adatok a cél megvalósulása után változatlan, így az érintettek azonosításra alkalmas módon kerültek tárolásra. Az adatok azonosításra alkalmas voltát az etikus hacker által az Ügyfélnek megküldött sérülékenységet feltáró üzenet is megerősítette. Az adatok olvashatóságát, így az érintettek adataihoz való hozzáférést és azonosításukat egyébként az adatokat érintő titkosítás alkalmazásának hiánya is megkönnyítette, ahogy az a határozat korábbi pontjaiban is megállapításra került.

Azzal tehát, hogy az Ügyfél az érintettek adatait tartalmazó, hibaelhárítási célból létrehozott tesztadatbázist a hibaelhárítás megtörténte utáni majd […] időszakban az érintettek azonosítását lehetővé tevő módon tárolta megsértette az általános adatvédelmi rendelet 5. cikk (1) bekezdés e) pontjában nevesített „korlátozott tárolhatóság” alapelvét.

e. Az alkalmazott szankcióval kapcsolatos megállapítások.

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

A bírságkiszabás szükségességének megállapítása során a Hatóság mérlegelte a jogsértések súlyosító és enyhítő körülményeit az alábbiak szerint:

Súlyosító körülmények:

- Az Ügyfélnél bekövetkezett adatvédelmi incidens egy olyan adatbiztonsági hiányosságra vezethető vissza, amelyre a piacon régóta elérhető volt az ingyenes javítás, a sérülékenység pedig akár harmadik személy által is könnyen detektálható volt, így az adatokhoz való jogosulatlan hozzáférésnek való kitettség elhárítására az Ügyfélnek a kockázatok megfelelő felmérése esetén nagyon régóta lehetősége lett volna.

- Az Ügyfél által az ügy kapcsán érintett adatok nagy száma, azok érzékenysége által jelentett kockázatok, továbbá az Ügyfél piaci pozíciója, amelyek alapján fokozottan elvárható tőle a megfelelő adatbiztonsági intézkedések alkalmazása.

- Ahogy az saját belső szabályzataiban is megjelenik, az Ügyfél által használt (nyílt forráskódú) tartalomkezelő rendszer használatából adódó kockázatokat, illetve azok felmérését az Ügyfélnek kell viselnie és azokkal kapcsolatban helyt állnia. Az Ügyfél ezen intézkedések hiányával saját belső szabályzatai előírásainak sem tett megfelelően eleget.

- Az érintett személyes adatokra alkalmazott titkosítás és ezzel kapcsolatos kockázatok felmérésének hiánya is megnövelte az incidensnek való kitettség kockázatait. Ezen intézkedés alkalmazása szintén megjelenik az Ügyfél vonatkozó belső szabályzataiban, amelynek szintén nem, illetve hiányosan tett eleget.

- A digi.hu honlap tekintetében az adminisztrátori (rendszergazdai) jogosultsággal rendelkező felhasználók érintettségét a Hatóság a biztonsági kockázatokat súlyosan növelő tényezőként vette figyelembe.

- A Hatóság a megállapított adatbiztonsági hiányosságokat olyan rendszerszintű problémának tekinti, amely alapján a jogsértő helyzet már az incidens bekövetkezése előtt is régóta fennállt az adatkezelő Ügyfélnél az érintett adatbázisok tekintetében.

- Az adatbiztonsági hiányosságokon túl az incidens bekövetkezése közvetlenül visszavezethető a hibaelhárítási célból létrehozott tesztadatbázis alapelvi szinten jogsértő cél nélküli és az érintettek azonosítására alkalmas módon való hosszú ideig […] történő tárolására. Amennyiben a tesztadatbázis az alapelveknek megfelelően törlésre került volna a hibajavítási cél megvalósulása után, úgy az incidens által az érintettekre jelentett kockázatok is sokkal enyhébbek lettek volna, mivel az érintett adatalanyok száma ezen tesztadatbázisban szereplők számával ([…] érintett) csökkenthető lett volna. Az adatbiztonsági hiányosságok a tesztadatbázis időben való törlése esetén csupán a direkt-marketing adatbázisban kezelt személyes adatok ([…] érintett) és a digi.hu honlap rendszergazdai adatai ([…] érintett) esetén álltak volna fent.

- A cél nélkül kezelt adatok beazonosítását, az adatok megtisztítását, aktualizálását és szükség szerint törlését az Ügyfél belső előírásai is tartalmazzák, amely szintén ellentétben áll az incidensben érintett tesztadatbázis kezelésének körülményeivel.

- Az adatbiztonsági hiányosságok és az alapelvi szinten jogsértő adatkezelés nagy számú (összesen […] fő) érintett személyes adatait érintette, amely tartalmazza az Ügyfél lakossági ügyfeleinek […]. Ez az ország lakosságának arányához viszonyítva is jelentős szám (a magyarországi lakosság […]).

- A Hatóság a bírság összegének meghatározása során figyelembe vette, hogy az Ügyfél által elkövetett alapelvi jogsértések az általános adatvédelmi rendelet 83. cikk (5) bekezdése szerint a magasabb maximális összegű bírságkategóriába tartozó jogsértésnek minősülnek.

Enyhítő körülmények:

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

- Az Ügyfél nyilatkozatában is elismerte, hogy az incidensben érintett tesztadatbázist már korábban törölnie kellett volna.

Egyéb, figyelembe vett körülmények:

- A bekövetkezett adatvédelmi incidensről való értesülése után az Ügyfél az incidens kezelésével kapcsolatos szinte valamennyi, az általános adatvédelmi rendelet 33. cikke által előírt intézkedést azonnal megtette, így az incidenst kivizsgálta, azt a Hatóság részére a tudomásszerzéstől számított 72 órán belül bejelentette, a sérülékenységet megszüntető javítást telepítette, a jogszerűtlen kezelt adatbázist pedig törölte, belső szabályzatait a sérülékenységvizsgálatok elvégzése kapcsán módosította. A Hatóság így az Ügyfél 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 az Ügyfél 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 bírság összegének megállapítása során figyelembe vette a Hatóság, hogy az Ügyfélnek a 2018. január 1. – 2018. december 31. közötti általános üzleti évet záró nyilvánosan elérhető beszámolója alapján ebben az évben összesen 47.299.383.000 HUF (négyvenhétmilliárd-kétszázkilencvenkilencmillió-háromszáznyolcvanháromezer forint) nettó árbevétele volt. A Hatóság továbbá figyelembe vette, hogy az Ügyfélnek a 2019. január 1. – 2019. december 31. közötti üzleti évben a Hatóságnak NAIH/2020/1160/6. számú tényállás tisztázó végzésére küldött válasza szerint 51.890.528.182 HUF (ötvenegymilliárd-nyolcszázkilencvenmillió-ötszázhuszonnyolcezer-száznyolcvankettő forint) nettó árbevétele volt. A bírság megállapítása során a jogsértés fennállásának időszakára tekintettel vette figyelembe a Hatóság a 2018 és 2019-es üzleti éveket. A fentiek alapján a kiszabott bírság összege a jogsértés súlyával arányban áll.

A Hatóság az Infotv. 61. § (2) bekezdés a) és c) pontjai alapján a határozatnak az Ügyfél azonosító adataival (az üzleti titkok kitakarásával) 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. § (2) bekezdés a) pontja alapján a Hatóság döntésével szembeni közigazgatási per törvényszéki hatáskörbe tartozik, a perre a Kp. 13. § (11) bekezdése alapján a Fővárosi Törvényszék kizárólagosan illetékes. A polgári perrendtartásról szóló 2016. évi CXXX. törvénynek (a továbbiakban: Pp.) – a Kp. 26. § (1) bekezdése alapján alkalmazandó – 72. §-a alapján a törvényszék hatáskörébe tartozó perben a jogi képviselet kötelező. Kp. 39. § (6) bekezdése szerint – ha törvény eltérően nem rendelkezik – a keresetlevél benyújtásának a közigazgatási cselekmény hatályosulására halasztó hatálya nincs.

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

A keresetlevél benyújtásának idejét és helyét a Kp. 39. § (1) bekezdése határozza meg. A tárgyalás tartása iránti kérelem lehetőségéről szóló tájékoztatás a Kp. 77. § (1)-(2) bekezdésén alapul. A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Itv.) 44/A. § (1) bekezdése határozza meg. Az illeték előzetes megfizetése alól az Itv. 59. § (1) bekezdése és 62. § (1) bekezdés h) pontja mentesíti az eljárást kezdeményező felet.

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. május 18.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár