Fővárosi Törvényszék
A határozat száma: 105.K.704.076/2022/4.
A felperes: Digi Távközlési és Szolgáltató Kft. (1134 Budapest, Váci út 35.)

A felperes képviselője:

Az alperes: Nemzeti Adatvédelmi és Információszabadság Hatóság (1125 Budapest, Szilágyi Erzsébet fasor 22/C.)

Az alperes képviselője:

A per tárgya: adatvédelmi ügyben hozott közigazgatási határozat (NAIH/2020/1160/10.) jogszerűségének vizsgálata

Í T É L E T

A bíróság az alperes NAIH/2020/1160/10. számú határozata 1.a. pontját az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontja megsértésének megállapítása tekintetében, valamint a 3. és 4. pontjait megsemmisíti, és a jogkövetkezmények körében az alperest új eljárásra kötelezi, ezt meghaladóan a keresetet elutasítja.

A felek a költségeiket maguk viselik.

Az ítélet ellen fellebbezésnek nincs helye.

I n d o k o l á s

A per alapjául szolgáló tényállás

[1] A felperes Magyarország egyik piacvezető internet- és televíziószolgáltatója.

[2] A felperes 2018 áprilisában tesztelési, hibaelhárítási célból létrehozott egy „test" elnevezésű tesztadatbázist (a továbbiakban: Tesztadatbázis), amelybe a lakossági ügyfelei körülbelül egyharmadának (297.649 fő) személyes adatait másolta át. A felperes egy másik, a digi.hu honlaphoz köthető „digihu" elnevezésű adatbázisában (a továbbiakban: „Digihu" Adatbázis) direkt marketing célú, a hírlevélre feliratkozók adatait és a honlap felületéhez való hozzáférésre lehetőséget adó rendszergazdai adatokat tárolt naprakészen, amely a lakossági

ügyfeleinek nem egészen 3 százalékát (25.269 fő), valamint 43 rendszergazda felhasználó adatait tartalmazta.

[3] A felperes 2019. szeptember 23-án arról szerzett tudomást, hogy egy etikus hacker informatikai támadás útján a www.digi.hu honlapon keresztül a nyílt forráskódú Drupal tartalomkezelő rendszer (a továbbiakban: Rendszer) sérülékenységét kihasználva hozzáfért a Tesztadatbázisban tárolt személyes adatokhoz, illetve hozzáférhetett a „Digihu" Adatbázisban tárolt személyes adatokhoz is. A támadást maga az etikus hacker jelezte e-mail üzenetben a felperesnek olyan módon, hogy a Tesztadatbázis egyik sorát bizonyítékként lekérte a hiba technikai jellegének ismertetése mellett.

[4] A felperes a jelzést követően a hibát kijavította (Rendszer sérülékenységét megszüntető nem hivatalos javítás letöltésével), a Tesztadatbázist törölte, az etikus támadóval titoktartási szerződést kötött, és jutalmat ajánlott neki. Ezen túlmenően az Informatikai Biztonsági Szabályzatában meghatározott féléves belső auditot, és a más rendszerei ellenőrzésére már korábban is használt webes sérülékenység vizsgáló szolgáltatást (Acunetix) kiterjesztette minden interneten keresztül elérhető rendszerére, így a digi.hu weboldalra is.

[5] A felperes az adatvédelmi incidenst 2019. szeptember 25-én bejelentette az alperesnek, amely alapján az alperes hatósági ellenőrzést, majd annak lezárását követően adatvédelmi hatósági eljárást indított.

Az alperes határozata

[6] Az alperes a 2020. május 18-án kelt NAIH/2020/1160/10. számú határozata rendelkező részének 1. pontjában megállapította, hogy

a.) a felperes 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 rendelete (a továbbiakban: általános adatvédelmi rendelet) 5. cikk (1) bekezdés b) és e) pontját azzal, hogy a hibaelhárítási célból létrehozott Tesztadatbázist a szükséges tesztek lefuttatása és a hiba kijavítása után nem törölte, így a Tesztadatbázisban tárolt nagy számú személyes adatot a következő közel másfél év alatt cél nélkül, azonosításra alkalmas módon tárolta, és a Tesztadatbázis törlésének hiánya közvetlenül lehetővé tette az adatvédelmi incidens bekövetkezését;

b.) a felperes megsértette az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseit azzal, hogy nem alkalmazott az adatkezelés biztonsága körében a kockázatokkal arányos megfelelő technikai és szervezési intézkedéseket, ugyanis az általa használt Rendszer 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; és az incidenssel érintett személyes adatok tekintetében nem alkalmazott titkosítást.

A határozat rendelkező részének 2. pontjában kötelezte a felperest, hogy vizsgálja felül valamennyi személyes adatokat tartalmazó adatbázisát abból a szempontból, hogy azokban indokolt-e titkosítás alkalmazása, és ennek eredményéről értesítse az alperest. A 3. pontban kötelezte a felperest 100.000.000 forint adatvédelmi bírság megfizetésére. A 4. pontban elrendelte a határozat nyilvánosságra hozatalát.

[7] Indokolásában az általános adatvédelmi rendeletnek a személyes adatok kezelésére vonatkozó alapelvek körébe tartozó „célhoz kötöttség" elve és a „korlátozott tárolhatóság" elve

tekintetében megállapította, hogy azokat felperes Tesztadatbázist érintő személyes adatkezelése megsértette. Megállapította, hogy az eredeti adatkezelés célja az előfizetői szerződések megkötése és teljesítése volt. A felperes a Tesztadatbázist egy műszaki hiba miatt, a szükséges tesztek elvégzése és a hiba kijavítása céljából hozta létre, amely cél elkülönül az adatkezelés eredeti céljától. A hibajavítási cél addig állt fenn, ameddig maga a hiba elhárításra nem került. Amint a hiba kijavítása megtörtént, az elkülönült adatkezelési cél is megszűnt, így a Tesztadatbázist törölni kellett volna. A felperes azonban a hiba elhárítását követően sem szüntette meg a Tesztadatbázist, ezért ezen cél nélküli adatkezelése az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontjába ütközött. A felperes továbbá azzal, hogy a hiba elhárítását követő közel másfél éves időszakban tovább tárolta a Tesztadatbázisban az érintettek azonosítására alkalmas módon a személyes adatokat, megsértette az általános adatvédelmi rendelet 5. cikk (1) bekezdés e) pontja szerinti „korlátozott tárolhatóság" elvét is.

[8] Az adattárolással kapcsolatos adatbiztonsági intézkedéseket tekintve elsődlegesen azt állapította meg, hogy az incidens a felperes által tartalomkezelésre használt Rendszerben fennállt régóta ismert és javítható sérülékenységre volt visszavezethető, amely hibát a felperes arra való hivatkozással nem javított, hogy az elérhető javítócsomag nem volt hivatalos. Az ügyben keletkezett NAIG/2020/1160/5. számú szakvéleményre (a továbbiakban: Szakvélemény) támaszkodva rögzítette, hogy a biztonsági rés megfelelő szoftver és rendszeres sérülékenységvizsgálat mellett kiszűrhető lett volna, a személyes adatok jogosulatlan megismerhetősége pedig titkosítás alkalmazásával elkerülhető lett volna. A felperes ezek elmulasztásával nem tett eleget az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseiben foglaltak követelményeknek.

[9] Az ügy összes körülményét mérlegelve, a feltárt jogsértések miatt a figyelmeztetést és a felszólítást önmagában nem tartotta arányos és visszatartó erejű szankciónak, ezért adatvédelmi bírságot alkalmazott az általános adatvédelmi rendelet 83. cikk (2) bekezdése, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 61. § (5) bekezdése és 75/A. §-a alapján. A mérlegelési jogkörben figyelembe vett súlyosító és enyhítő körülményeket a határozat indokolásának e) pontja alatt tételesen felsorolta.

[10] További jogkövetkezményként, az Infotv. 61. § (2) bekezdés a) és c) pontjai alapján elrendelte a határozat nyilvánosságra hozatalát is.

A kereset, a védirat

[11] A felperes a keresetében kérte elsődlegesen a határozat megsemmisítését és az alperes kötelezését a határozat honlapjáról való törlésére; másodlagosan a határozat megsemmisítését és az alperes új eljárásra kötelezést azzal, hogy állapítsa meg a döntés 1.a. pontjában foglalt jogsértés hiányát és a bírság jogellenességét, valamint kötelezze az alperest a határozat honlapjáról való törlésére; harmadlagosan a határozat megsemmisítését és az alperes új eljárásra kötelezést azzal, hogy állapítsa meg a döntés 1.b. pontjában foglalt jogsértés hiányát és a bírság jogellenességét, valamint kötelezze az alperest a határozat honlapjáról való törlésére; negyedlegesen a határozat megsemmisítését és az alperes új eljárásra kötelezést azzal, hogy állapítsa meg a bírság jogellenességét, valamint kötelezze az alperest a határozat honlapjáról való törlésére; ötödlegesen a határozat megsemmisítését és az alperes új eljárásra kötelezést azzal, hogy a döntés 4. pontjában meghatározott nyilvánosságra hozatalt mellőzze, és kötelezze az alperest a határozat honlapjáról való törlésére.

[12] Nem vitatta, hogy a hibaelhárítási célból létrehozott Tesztadatbázisban a hibaelhárításhoz szükségesnél hosszabb ideig tárolta az ügyféladatokat, de ezzel álláspontja szerint nem

sértette meg az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) és e) pontját. A „célhoz kötöttség" elvével kapcsolatban előadta, hogy az ügyféladatok gyűjtésére az általános adatvédelmi rendelet 6. cikk (1) bekezdés b) pontja alapján az előfizetői szerződések megkötése és teljesítése céljából került sor. Ezt a célt szolgálta a Tesztadatbázis létrehozása is, vagyis hibaelhárítás céljából a gyűjtött adatok más belső rendszerben történő elmentése és tárolása. Az adatkezelés célja nem változott, csak az adattárolásra egy további adatbázisban is sor került annak érdekében, hogy az adatok az eredeti adatkezelési célra továbbra is rendelkezésre álljanak. Hivatkozott arra is, hogy a kezelt személyes adatok köre nem bővült azáltal, hogy a Tesztadatbázist létrehozta, és amennyiben a Tesztadatbázis létrehozása vagy fenntartása az adatbiztonsági kockázatokat esetlegesen növelné is, ez nem alapelvi szintű jogsérelemként, legfeljebb adatbiztonsági kérdésként lehetne értékelhető.

[13] A „korlátozott tárolhatóság" elvének sérelmét állító alperesi álláspontot is vitatta, mivel érvelése szerint az ügyféladatok kezelésének célja nem a hibajavítás volt, ezért az adatok tárolhatóságának időtartama sem igazodhat a hibajavítás befejezéséhez. Mivel az ügyféladatok kezelésének célja az előfizetői szerződések teljesítése volt, ameddig erre a célra szükséges az adatok tárolása, addig az jogszerű akár több példányban, több adatbázisban is. Következésképpen amiatt, hogy a Tesztadatbázist nem törölte azonnal a hibaelhárítást követően, a korlátozott tárolhatóság követelményét sem sértette meg, hiszen a Tesztadatbázisban szereplő adatoknak az érintettek azonosítására alkalmas módon történő tárolására a hibajavítástól függetlenül is jogosult volt.

[14] Az adattárolással kapcsolatos biztonsági intézkedések vonatkozásában előadta, hogy a Rendszer sérülékenységének detektálása nem volt tőle elvárható. Meglátása szerint maga a Szakvélemény is azt állapította meg, hogy a Rendszer sérülékenységének kihasználása csak célzatosan, magas szintű információtechnológiai szakértelemmel és időigényes tevékenységgel volt végrehajtható. A sérülékenyég tehát nem olyan könnyen kihasználható, alapvető hiba, amellyel kapcsolatban a felperesnek külön biztonsági intézkedéseket kellett volna foganatosítania, és ebből az is következik, hogy a felperest nem terhelte gondatlanság a sérülékenység fel nem ismerése körében. A sérülékenység nem hivatalos javításának letöltése nem volt elvárható a felperestől, ugyanis annak megfelelőségét semmi nem biztosította. A titkosítás kötelező alkalmazását sem az általános adatvédelmi rendelet 32. cikke, sem más jogszabály nem írta elő, így annak elmaradása jogsértést nem valósíthat meg. E megoldást egyebekben célszerűtlennek is tartotta, mivel az az adatbázisok működését lassította, a hardverigényeket és a hibalehetőségeket pedig megnövelte volna. Álláspontja szerint a titkosítás helyett olyan egyéb adatbiztonsági intézkedéseket (jogosultság kezelés; hozzáférések naplózása; hálózati szeparáció és határvédelmi megoldások; stb.) alkalmazott, amelyek együttese az általános adatvédelmi rendelet 32. cikkének megfelelő védelmet nyújtott és mélységi, egymásra épülő kontrollokból álló rendszert eredményezett.

[15] A bírság jogszerűségét elsődlegesen a jogsértés hiányán keresztül támadta, de részletesen vitatta a mérlegelést is. Kifejtette, hogy az alperes egyes súlyosító körülményeket indokolatlanul vett figyelembe, míg egyes enyhítő körülményeket nem kellő súllyal vagy egyáltalán nem értékelt, továbbá megsértette a hatékony, arányos és visszatartó erejű bírságkiszabásra vonatkozó kötelezettségét, és nem vizsgálta megfelelően az enyhébb szankció (figyelmeztetés) alkalmazásának lehetőségét.

[16] A határozat nyilvánosságra hozatalának elrendelését is kifogásolta, mert álláspontja szerint a határozat nem érinti a személyek széles körét, és a jogsérelem súlya is csekélynek minősült.

[17] Az alperes fenntartva a határozatában foglaltakat, a kereset elutasítását kérte. Hangsúlyozta, hogy a Tesztadatbázisban történt, a hibaelhárítási cél teljesülését követő közel másfél évig tartó adattárolás nem volt szükséges az előfizetői szerződések teljesítéséhez. Meglátása szerint

elvárható lett volna a felperes részéről egyfelől a Rendszer sérülékenységének felismerése, másfelől annak vizsgálata, hogy ilyen sérülékenység mellett az általános adatvédelmi rendelet 32. cikkével összhangban egyáltalán használhatta-e a Rendszert; amennyiben igen, akkor viszont intézkednie kellett volna a kockázatok csökkentése iránt. Utalt arra is, hogy amennyiben a kockázatok csökkentésére a nem hivatalos javítások alkalmazását nem tartotta megfelelőnek, akkor más módon kellett volna kiküszöbölnie a sérülékenység kockázatát. Kiemelte, hogy a Szakvéleményben foglaltak szerint a titkosítás alkalmazása megfelelő intézkedés lett volna, amit a felperes kockázatelemzés hiányában alappal nem tehet vitássá. A jogkövetkezményeket illetően kifejtette, hogy a bírságkiszabásra és a mértékének megállapítására, valamint a határozat nyilvánosságra hozatalának elrendelésére is a jogszabályi rendelkezésekkel összhangban került sor.

Az előzetes döntéshozatali eljárás kezdeményezése, az Európai Unió Bíróságának döntése

[18] A bíróság 105.K.705.596/2020/11. számú végzésével az Európai Unió Bírósága (a továbbiakban: EUB) előzetes döntéshozatali eljárását kezdeményezte az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) és e) pontjainak értelmezésére. Az EUB a C-77/21. számú ítéletében (a továbbiakban: Ítélet) kimondta, hogy a „célhoz kötöttség" elvével nem ellentétes, ha az adatkezelő egy tesztek elvégzése és hibák kijavítása céljából létrehozott adatbázisban rögzíti és tárolja a korábban más adatbázisban gyűjtött és tárolt személyes adatokat, amennyiben az ilyen további adatkezelés megfelel azon konkrét céloknak, amely célokból a személyes adatokat eredetileg gyűjtötték, amit az általános adatvédelmi rendelet 6. cikk (4) bekezdésében szereplő szempontokra tekintettel kell meghatározni. Ugyanakkor a „korlátozott tárolhatóság" elvével ellentétesnek tartotta, ha az adatkezelő a korábban más célból gyűjtött személyes adatokat egy tesztek elvégzése és a hibák kijavítása céljából létrehozott adatbázisban az e tesztek elvégzéséhez és e hibák kijavításához szükségesnél hosszabb ideig tárolja.

[19] A felperes álláspontja szerint az EUB a bíróság végzésének téves értelmezése alapján abból indult ki, hogy az adatok eredeti gyűjtésének célja (előfizetői szerződések megkötése és teljesítése) és a Tesztadatbázis létrehozásának célja (tesztek elvégzése és hibák kijavítása) eltérő, és a téves kiindulópont miatt nem vette figyelembe azt sem, hogy a sérelmezett adattárolásra nem az eredeti cél megvalósítását követően, hanem azzal párhuzamosan került sor. Kiemelte, hogy az adatok gyűjtése és a hibajavítási célú Tesztadatbázisban tárolás egy adatkezelési célt szolgált: a felperes szerződéses kötelezettségeinek a teljesítését. A felperes ugyanannak a – tág értelemeben vett – adatkezelésnek a keretében hajtott végre – szűk értelemben vett – adatkezelési műveleteket az adatokon, amelynek első lépése az adatok gyűjtése volt, majd ezt követte az adatok különböző adatbázisokban történő tárolása az adatok gyűjtésével megegyező célra. Amennyiben az elkülönült adatkezelési célok megállapíthatók is lennének, akkor sem sérültek az adatkezelési alapelvek. A „célhoz kötöttség" elve azért nem sérült, mert – figyelemmel az Ítélet 44. pontjában foglaltakra is – a Tesztadatbázis létrehozásának célja összeegyeztethető az adatok eredeti gyűjtésének céljával, a „korlátozott tárolhatóság" elve pedig azért nem, mert nem egymást követő adatkezelésekre került sor, és amíg az adatkezelésnek legalább az egyik célja fennáll, addig az adatok tárolása jogszerű. Amennyiben a bíróság egyetért az Ítélettel kapcsolatban megfogalmazott aggályaival, kérte az EUB előzetes döntéshozatali eljárása ismételt kezdeményezését.

A bíróság döntése és annak jogi indokai

[20] A kereset részben alapos.

[21] A bíróság az alperes határozatának jogszerűségét a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) 2. § (4) bekezdése és 85. § (1)-(2) bekezdése alapján eltérő törvényi rendelkezés hiányában a kereseti kérelem, a felek által előterjesztett kérelmek és jognyilatkozatok keretei között, az alperes határozatának meghozatalakor fennálló tények alapján vizsgálta, figyelemmel az Ítéletében foglaltakra.

[22] A bíróságnak a jelen ügyben több kérdésben kellett döntenie. Egyfelől arról, hogy az előfizetők személyes adatainak a Tesztadatbázisban tárolása sértette-e a „célhoz kötöttség" elvét. Másfelől meg kellett vizsgálnia, hogy a „korlátozott tárolhatóság" elvébe ütközött-e, hogy a felperes a hibaelhárítást követően közel másfél évig tárolta az adatokat a Tesztadatbázisban. Harmadikként az adattárolással kapcsolatban megtett felperesi biztonsági intézkedéseket illetően kellett döntenie arról, hogy azok megfeleltek-e az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdésében foglalt követelményeknek. Végül, az előbbiek elbírálásától függően lehetett tárgya a pernek a jogkövetkezményeknek – a bírságkiszabás és a döntés nyilvánosságra hozatala jogszerűségének – az értékelése.

[23] A „célhoz kötöttség" elve az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontja alapján megköveteli, hogy a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Ezt kiegészítve az általános adatvédelmi rendelet (50) preambulumbekezdése megállapítja, hogy a személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték; ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését.

[24] A peres felek között nem volt vitatott, hogy a felperes a lakossági ügyfelei személyes adatait az előfizetői szerződések megkötése és teljesítése céljából gyűjtötte és tárolta, és ezen eredeti adatkezelési cél az általános adatvédelmi rendelet 6. cikk (1) bekezdés b) pontja alapján jogszerű volt. Emellett került sor 2018 áprilisában a szerver működését érintő és az előfizetői adatok megszűnését eredményező műszaki hiba miatt hibaelhárítás céljából a Tesztadatbázis létrehozására. Habár az eredeti adatkezelési cél az előfizetői szerződések megkötése és teljesítése volt, azonban ez önmagában nem jelentette azt, hogy e cél megvalósulásához ne kapcsolódhattak volna további ún. „rárakódó célok", amely egyben azt eredményezi, hogy a „célhoz kötöttség" elve ezen „rárakódó cél" tekintetében is érvényesül.

[25] Az EUB az Ítéletben (35. pontban) megállapította, hogy a további célból való adatkezelésnek akkor lehet helye, ha a személyes adatok további kezelése összeegyeztethető az eredeti adatgyűjtés céljával, amely megállapítása érdekében – figyelemmel az általános adatvédelmi rendelet 6. cikk (4) bekezdésére – figyelembe kell venni többek között: a személyes adatok gyűjtésének célja és a tervezett további adatkezelés célja közötti esetleges kapcsolatot, a személyes adatok gyűjtésének körülményeit, a személyes adatok jellegét, a további adatkezelésnek az érintetteket érintő lehetséges következményeit, a megfelelő garanciák meglétét. Az általános adatvédelmi rendelet 6. cikk (4) bekezdésében e kritériumok meghatározása példázódó jellegű, és azok közül akár egyetlen körülmény fennállása is elegendő lehet az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontjában foglaltaknak való megfeleléshez.

[26] Az EUB az Ítéletében (38. pontban) kimondta azt is, hogy a nemzeti bíróság feladata az említett kritériumok figyelembevételével és az adott ügyre jellemző körülmények

összességére tekintettel az eredeti adatgyűjtés céljának és a további adatkezelés céljának a meghatározása, és amennyiben a további adatkezelés célja eltér az eredeti adatkezelés céljától, annak vizsgálata, hogy a további adatkezelés összeegyeztethető-e az eredeti adatgyűjtési céllal.

[27] A bíróság az Ítéletre és a peres felek által nem vitatott tényekre tekintettel megállapította, hogy a felperes a személyes adatokat eredetileg az előfizetői szerződések megkötése, teljesítése céljából gyűjtötte és tárolta, emellett a Tesztadatbázis létrehozásának közvetlen célja egy konkrétan felmerült hibához kapcsolódóan a szükséges tesztek elvégzése és a hiba kijavítása volt. A bíróság – összhangban az Ítélet 44. pontjában foglaltakkal – megállapította továbbá, hogy bár a Tesztadatbázist hibaelhárítási célból hozta létre a felperes, ez ugyanakkor konkrétan kapcsolódott a személyes adatok eredeti adatkezelési céljához. A tesztelés és a hibák kijavítása nyilvánvalóan szükséges ahhoz, hogy a felperes hozzáférjen az előfizetői adatokhoz, és felhasználhassa azokat az előfizetői szerződések megkötéséhez, teljesítéséhez, ezáltal elősegítve az eredeti adatkezelési cél megvalósítását.

[28] Az alperes – az EUB Ítéletének ismeretében a per tárgyalásán tett nyilatkozatában – az eredeti adatkezelés célja (szerződések megkötése, teljesítése) és a további adatkezelési cél (hibaelhárítás) összeegyeztethetőségét nem vitatta, annak pedig nem volt jelentősége, hogy a vizsgálandó körülmények közül más körülmények alapján az összeegyeztethetőség nem volt megállapítható, ugyanis visszautalva a jelen ítélet [25] pontja utolsó mondatában kifejtettekre, akár egyetlen körülmény fennállása is megalapozhatja az összeegyeztethetőséget.

[29] A fentiek alapján a felperes – az általános adatvédelmi rendelet 6. cikk (4) bekezdés a) pontjára figyelemmel – az ügyfelek személyes adatait a Tesztadatbázisban jogszerűen, az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontjában foglaltaknak megfelelően, az eredeti adatkezelési céllal összeegyeztethető módon kezelte.

[30] A „korlátozott tárolhatóság" elve az általános adatvédelmi rendelet 5. cikk (1) bekezdés e) pontja alapján azt jelenti, hogy a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Az EUB az Ítéletében (54. és 57. pontokban) rámutatott, hogy idővel még az eredetileg jogszerű adatkezelés is összeegyeztethetetlenné válhat az általános adatvédelmi rendelettel, ha az adatok már nem szükségesek az adatkezelés céljainak eléréséhez, és az adatokat törölni kell, ha e célok megvalósultak.

[31] A jelen ügyben, bár a Tesztadatbázis létrehozásához kapcsolódó cél valóban szorosan kapcsolódott az eredeti adatkezelési célhoz, azonban – a jelen ítélet [27] pontjában részletezettek szerint – mégsem teljesen azonos azzal, amennyiben közvetlenül a szükséges tesztek elvégzését és a felmerült hiba kijavítását szolgálta. Ebből következően a Tesztadatbázisban történt adatkezelés tekintetében a korlátozott tárolhatóság elvének megfelelést e célhoz kötötten is kellett vizsgálni, és így azt kellett megállapítani, hogy a Tesztadatbázisban az adatok tárolására a tesztek elvégzéséhez és a hibák kijavításához szükséges ideig volt jogszerűen lehetőség. Mivel a hiba elhárítására 2018 áprilisában került sor, és a felperes a Tesztadatbázist csupán 2019 szeptemberében szüntette meg, ezért a több mint másfél éves adatkezelés a szükséges adatkezelési időtartamot indokolatlanul hosszú idővel meghaladta. E körülmény alapelveknek való megfelelését az általános adatvédelmi rendelet 5. cikk (2) bekezdésében foglaltak ellenére a felperes nem tudta igazolni; azt maga is elismerte, hogy a Tesztadatbázist figyelmetlenségből nem törölte, holott a fenntartását a hiba elhárítása már nem indokolta, majd a Tesztadatbázisról megfeledkezett a támadásról való tudomásszerzésig. Mindez egyértelműen azt jelzi, hogy a kifogásolt adatkezelésnek a felperesnél már nem volt meg a közvetlen (de a fentiek szerint az adatkezelés célhoz kötöttségét önmagában nem kizáró) célja. Azt az EUB az Ítélet 60. pontjában maga is

megállapította, hogy a felperesnek az az érvelése, miszerint a Tesztadatbázisban tárolt személyes adatokat figyelmetlenségből nem törölte a tesztek elvégzését és a hiba kijavítását követően, nem releváns abból a szempontból, hogy az adatokat a további kezelésük céljainak megvalósulásához szükségesnél hosszabb ideig tárolták-e.

[32] Tekintettel arra, hogy az EUB eljárását kezdeményező végzésben feltett mindkét kérdésben kifejezetten szerepelt a párhuzamos adatkezelésre, a személyes adatok párhuzamosan két adatbázisban tárolására utalás (például „az adatkezelő az egyébként jogszerű célhoz kötötten gyűjtött és tárolt személyes adatokat párhuzamosan egy másik adatbázisban is tárolja"), a felperes alappal nem hivatkozhat arra, hogy ezt nem vette figyelemben az EUB az álláspontja kialakításakor. Az Ítéletből mindössze az tűnik ki, hogy ennek a körülménynek az EUB nem tulajdonított meghatározó jelentőséget a jogi norma értelmezésénél.

[33] A fentiek alapján a felperes adatkezelése ellentétes az általános adatvédelmi rendelet 5. cikk (1) bekezdés e) pontjában foglalt „korlátozott tárolhatóság" elvével.

[34] Az általános adatvédelmi rendelet 32. cikk (1) bekezdés a) pontja alapján 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. Ugyanezen 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.

[35] A felperes nem vitatottan az adatvédelmi incidenssel érintett adatok tárolásával kapcsolatban kockázatelemzést nem végzett. A felperes álláspontjával ellentétben a Szakvéleményben leírtak alapján a felperestől elvárható lett volna a Rendszer sérülékenységének felismerése és kijavítása, ehhez komoly informatikusi ismeret nem volt szükséges. A Szakvélemény kifejezetten tartalmazza, hogy vannak olyan webes sérülékenységeket vizsgáló szoftverek, amelyek a szóban forgó sérülékenységet ki tudták volna szűrni automatizmussal is. Ezen szoftverek alkalmazásához nem kellett volna magas szintű informatikai tudás, kódfejtő képesség, „azok kezelését egy, a téma iránt érdeklődő, informatikai biztonsági kérdésekben közepesen jártás személy is el tudja sajátítani". Ilyen szoftvert egyébként maga a felperes is használt más rendszerei ellenőrzésére (Acunetix). A felperes – akár sérülékenységvizsgálat keretében – a sérülékenységgel érintett Rendszer hibájáról úgy is tudomást szerezhetett volna, ha a szoftver hivatalos honlapján tájékozódik, ahol a hiba és annak megoldása is ismertetésre került. Nem vitatott, hogy a Rendszer konkrét hibájára hivatalos javítócsomag nem állt rendelkezésre, ugyanakkor a szoftver hivatalos honlapján, az ottani fórumon bárki számára ingyenesen elérhető volt a nem hivatalos javítás. Ezt a felperes is alkalmazhatta volna, ahogy utóbb, az adatvédelmi incidensről való tudomásszerzést követően végül is megtette. Emellett a Szakvélemény és annak alapján az alperes megállapította, hogy megfelelő titkosítás használatával megakadályozható lett volna a személyes adatok megismerése. A felperes helytállóan mutatott rá arra, hogy az adatkezelés biztonságának elérésére a jogalkotó nem kötelező jelleggel rendeli el az érintett adatok titkossá tételét, de ezt is olyan intézkedésnek tartja, ami adott esetben alkalmas lehet az adatbiztonság megteremtésére. A jelen ügyben a felperes – különös tekintettel arra, hogy egyéb intézkedést nem foganatosított – legalább a személyes adatok titkosítását elvégezhette volna az adatok védelme érdekében.

[36] A fentiek alapján a felperes az adatvédelmi incidenssel érintett adatok tárolásával kapcsolatban az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdéseiben rögzített kötelezettségének nem tett eleget.

[37] A fentiek szerint a kereset a jogalap vitatása körében részben megalapozott volt: a felperes vizsgált adatkezelésével kapcsolatban a „célhoz kötöttség" elvének megsértését az alperes megalapozatlanul állapította meg, ugyanakkor jogszerű az alperes azon megállapítása, hogy a felperes megsértette a „korlátozott tárolhatóság" elvét és az általános adatvédelmi rendelet 32. cikk (1)-(2) bekezdését.

[38] A szankció megállapításánál – annak eldöntésekor, hogy szükség van-e közigazgatási bírság kiszabására, illetve a közigazgatási bírság összegének meghatározásakor – az általános adatvédelmi rendelet 83. cikk alapján a kiindulópontot a jogsértés meghatározása jelenti. Az alperes határozata alapján a bírság kiszabásának jogalapjaként három jogsértés szolgált: a „célhoz kötöttség" elvének megsértése, a „korlátozott tárolhatóság" elvének megsértése és az adatbiztonság követelményének megsértése, amelyek közül – a [23]-[29], [37] bekezdésében kifejtettek szerint – a felperes adatkezelése a „célhoz kötöttség" elvét nem sértette. Ez pedig szükségszerűen azt eredményezte, hogy a három jogsértés figyelembevételével kiszabott bírság sem megalapozott. Az alperes a határozatában a bírságkiszabás és a bírság összegének meghatározása során figyelembe vett körülményeket jogsértésenként nem különítette el, így a bíróság a jogszerűnek tartott jogsértések tekintetében a bírság kiszabásának jogszerűségét érdemben nem tudta vizsgálni.

[39] Az alperes további jogkövetkezményként elrendelte az Infotv. 61. § (2) bekezdés a) és c) pontja alapján a döntés nyilvánosságra hozatalát is, amely során a c) pont szerinti feltétel – „a bekövetkezett jogsérelem súlya" – megállapítása körében az általa megállapított mindhárom jogsértést mérlegelnie kellett. Erre tekintettel, mivel az alperes a „célhoz kötöttség" elvének megsértését jogszerűtlenül állapította meg, ezért – hasonlóan a bírságkiszabáshoz – a döntés nyilvánosságra hozatalának elrendelése sem lehetett jogszerű az alperes által figyelembe vett jogsértések száma és azok együttes súlya alapján.

[40] A bíróság megállapította, hogy az alperes határozata az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontja megsértésének megállapítása, valamint jogkövetkezmények (bírság kiszabása, döntés nyilvánosságra hozatala) alkalmazása tekintetében jogszabálysértő, ezért a Kp. 89. § (1) bekezdés b) pontja és 92. § (1) bekezdés b) pontja alapján az alperes határozatának 1.a. pontját az általános adatvédelmi rendelet 5. cikk (1) bekezdés b) pontja megsértésének megállapítása tekintetében, valamint a 3. és 4. pontjait megsemmisítette, és a jogkövetkezmények körében az alperest új eljárásra kötelezte, ezt meghaladóan a Kp. 88. § (1) bekezdés a) pontja alapján a keresetet elutasította. A jogsértések alperestől eltérő megállapítása miatt a jogkövetkezmények mérlegelésére vonatkozó keresetrészt a bíróság érdemben nem vizsgálta.

[41] A megismételt eljárás során az alperesnek kizárólag a jogkövetkezményekről kell újra döntenie, és azt kell mérlegelnie, hogy a „célhoz kötöttség" elve megsértésének hiánya milyen mértékben érinti a bírságkiszabást és a döntés nyilvánosságra hozatalának alkalmazhatóságát. Amennyiben az alperes a bírság kiszabása mellett foglal állást, akkor annak összege meghatározásánál szintén figyelembe kell vennie, hogy e jogsértés nem áll fenn a felperesi adatkezelések viszonyában. Erre tekintettel a kiszabásra kerülő bírság mértéke nem érheti el a 100.000.000 forintot.

[42] A felperes ismételten indítványozta az Európai Unió Bírósága előzetes döntéshozatali eljárásának kezdeményezését, amely indítványt a bíróság elutasította, mivel az EUB az Ítéletében az általános adatvédelmi rendelet ügyben releváns rendelkezéseit már értelmezte, és a bíróság nem osztotta a felperesnek az Ítélettel kapcsolatban megfogalmazott azon aggályát, amely szerint az EUB félreértette volna az előzetes döntéshozatali eljárást kezdeményező indítványt.

[43] A bíróság a felperes és az alperes pernyertessége-pervesztessége arányát azonosnak ítélete, ezért a Kp. 35. § (1) bekezdése folytán alkalmazandó, a polgári perrendtartásról szóló 2016. évi CXXX. törvény 83. § (2) bekezdése alapján akként határozott, hogy a felek a költségeiket maguk viselik.

[44] Az eljárás az illetékekről szóló 1990. évi XCIII. törvény 57.§ (1) bekezdés o) pontja alapján illetékmentes.

[45] Az ítélet elleni fellebbezést a Kp. 99. § (1) bekezdése zárja ki.

Záró rész

Budapest, 2023. március 9.

dr. Huber Gábor s. k. a tanács elnöke	dr. Borsos Krisztina s. k. előadó bíró	dr. Nagy Péter s. k. bíró