Ügyszám: NAIH-559-26/2013/H.

Tárgy: személyes adatok kezelése nyereményjáték során

H A T Á R O Z A T

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 61. § (1) bekezdés c) és f) pontja alapján

a **Fővárosi Ásványvíz- és Üdítőipari Zrt.-t** (1239 Budapest, Helsinki út 121-123., a továbbiakban: FÁÜ Zrt.)

1.500.000 Ft, azaz egymillió-ötszázezer forint adatvédelmi bírság

megfizetésére kötelezem az általa végzett jogellenes adatkezelés miatt.

Az Infotv. 61. § (2) bekezdése alapján elrendelem a határozat azonosító adatokkal való nyilvánosságra hozatalát.

A bírságot a határozat jogerőre emelkedését követő **15 napon** belül ***a Nemzeti Adatvédelmi és Információszabadság Hatóság központosított bevételek beszedése célelszámolási forintszámlája (10032000-00319425-30006009)*** javára kell megfizetni. **Az összeg átutalásakor** kérem, **hivatkozzon a NAIH-559/2013. BÍRS. számra**.

A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.) 132. § (1) bekezdés a) pontjára tekintettel amennyiben a kötelezett pénzfizetési kötelezettségének határidőben nem tesz eleget, késedelmi pótlékot köteles fizetni. A késedelmi pótlék mértéke a Ket. 132. § (2) bekezdése alapján minden naptári nap után a felszámítás időpontjában érvényes jegybanki alapkamat kétszeresének 365-öd része. Késedelmi pótlékot a teljesítési határidő utolsó napját követő naptól kell felszámítani. A bírság és a késedelmi pótlék meg nem fizetése esetén a Hatóság elrendeli a határozat végrehajtását, a bírság és a késedelmi pótlék adók módjára történő behajtását.

A hatósági eljárás kapcsán eljárási költség nem merült fel, ezért annak megállapításáról és viseléséről nem rendelkeztem.

E döntés ellen közigazgatási úton jogorvoslatnak helye nincs, de a közléstől számított 30 napon belül a Fővárosi Közigazgatási és Munkaügyi Bírósághoz címzett, azonban a Hatósághoz benyújtandó keresettel lehet kérni annak bírósági felülvizsgálatát. A tárgyalás tartása iránti kérelmet a keresetben jelezni kell. A teljes személyes illetékmentességben nem részesülők számára a bírósági felülvizsgálati eljárás illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jogos.

I N D O K O L Á S

I. Előzmények

Több bejelentés érkezett a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban: Hatóság), melyben a bejelentők azt kifogásolták, hogy a FÁÜ Zrt. hozzájárulásuk nélkül a születési dátumot, az email címet, valamint a telefonszámot harmadik személynek továbbította és azokat bárki számára hozzáférhetővé tették az interneten.

2012. október 13-án nyilvánossá vált, hogy egy török hackercsoport feltörte a FÁÜ Zrt. által üzemeltetett http://3d.pepsi.hu/ promóciós internetoldalt, és több mint ötvenezer felhasználó személyes adatát (név, e-mail cím, telefonszám, születési dátum, a település neve, és a belépéshez használt jelszó) lopták el. Az adatokat nyilvánosságra hozták az interneten, a http://leaks-db.hacktalk.net/node/20 címen az incidenst követően több mint 9 hónapig elérhetőek voltak a bejelentők által kifogásolt személyes adatok. A személyes adatok más oldalakon (pastebin.com; bindrand.com; pastemine.com) keresztül is elérhetőek voltak, azonban ezek törlése iránti intézkedés hatékony volt, a Hatóság eljárásának megindításakor már nem voltak elérhetőek az adatok ezeken a honlapokon. A Hatóság 2012. október 15-én közleményt bocsátott ki, amelyben felhívta a figyelmet az adatbiztonsági követelmények fontosságára.

Az ügyben a Hatóság az Infotv. 38. § (3) bekezdés a) pontja értelmében 2013. február 5-én vizsgálati eljárást indított. Ennek keretében a FÁÜ Zrt. jogtanácsosa arról tájékoztatott, hogy a „Pepsi – Lásd a világot 3D-ben” c. nyereményjátékot tartalmazó fogyasztói promóciót megbízási szerződés alapján a Createam Promotion Kft. igénybevételével szervezte meg. Az adatlopási incidenst követően a FÁÜ Zrt. megkereste az adatokat megjelentető oldalak adminisztrátorait az illegálisan megszerzett adatok azonnali levétele iránt. A hacktalk.net honlap számos megkeresés után sem vette le az adatokat, ezért a FÁÜ Zrt. hivatalos levélben fordult az adott honlap internetes adatbázisban számukra elérhető regisztrálójához, a WhoisGuardhoz a szükséges intézkedések megtétele iránt. A FÁÜ Zrt. továbbá arról tájékoztatta a Hatóságot, hogy amennyiben a megkeresésük nem vezet eredményre, úgy az ICANN egységes domain jogvita-kezelési szabályzatára hivatkozva panasszal fordulnak az illetékes USA-beli WIPO szervezethez.

Mivel a fenti hackertámadás óta több hónap eltelt, az adatok még mindig elérhetőek voltak a http://leaks-db.hacktalk.net/node/20 oldalon, és számos körülmény tisztázásra várt még, ezért a Hatóság vizsgálati eljárás során feltárt tények, körülmények alapján az Infotv. 55. § (1) bekezdés a) pontjának megfelelően a vizsgálati eljárást lezárta és adatvédelmi hatósági eljárást indított annak vizsgálatára, hogy a két cég megtett-e mindent az adatbiztonság, illetve az érintettek jogainak érvényesülése érdekében.

II. Az eljárás menete

1. A Hatóság a tényállás tisztázása érdekében több végzésben megkereste a FÁÜ Zrt.-t és a Createam Kft.-t is. A Hatóság kérdéseire minden esetben teljes körűen, valamint határidőben válaszoltak.

2. A Hatóság vizsgálatának tárgya volt egyrészt az általánosan alkalmazott adatkezelési gyakorlat, valamint a „Pepsi – Lásd a világot 3D-ben” c. nyereményjátékkal kapcsolatos adatlopási incidens kivizsgálása, az adatbiztonsági követelményeknek való megfelelőség ellenőrzése.

3. A Createam Promotion Kft. nevet változtatott az eljárás ideje alatt, amelyről a Hatóságot tájékoztatta. Emiatt az ügyben a továbbiakban mint Createam Reklámügynökség Kft., rövidítve Createam Kft. szerepel.

A Hatóság a NAIH-559-10/2013/H. iktatószámú végzésében a Createam Kft. kérésére, az általa megjelölt adatvédelmi, informatikai és ügyviteli szabályzatok zártan kezeléséről rendelkezett.

4. A FÁÜ Zrt. a Hatóság megkeresésére arról tájékoztatott, hogy a „Pepsi – Lásd a világot 3D-ben” c. nyereményjátékot megbízási szerződés alapján a Createam Kft. igénybevételével szervezte meg. A 2011. március 1-jén megkötött megbízási szerződés 1.1.7. pontja úgy rendelkezett, hogy a *„[…] a Megbízott feladata a promóció teljes körű megtervezése, megvalósítása és lebonyolítása”*, amely kiterjedt az adatkezelési és adatfeldolgozási feladatok ellátására is. A Createam Kft. az adatkezelői minőségét nem ismeri el. A FÁÜ Zrt. értelmezése szerint a 95/46/EK irányelv alapján nem a szerződéses definíciók az irányadóak, hanem a személyes adatokkal kapcsolatos tényleges szerep a meghatározó. A FÁÜ Zrt.-nek - válasza alapján - hozzáférése nem volt az adatokhoz, az adatokat a Createam Kft. gyűjtötte, rendszerezte, tárolta, csak a nyereményjáték nyerteseinek adatait adta át részére. A fentiek, továbbá azon körülmények alapján, hogy a Createam Kft. alvállalkozót vett igénybe, illetve a fogyasztói megkereséseket a Createam Kft. postai és elektronikus levélcímére lehetett megküldeni, a FÁÜ Zrt. álláspontja szerint a Createam Kft. volt az adatkezelő a nyereményjáték lebonyolítása során. A FÁÜ Zrt. a nyereményjáték témakoncepcióját (márka, marketingkommunikáció) határozta meg. Utasításai kiterjedtek a játék vizuális elemeinek, menetének jóváhagyására, azonban az adatkezelés körében hozott döntésekre, így az adatbiztonság technikai feltételeire nem. A FÁÜ Zrt. álláspontja szerint a Createam Kft. nem vitatja azt a tényt, hogy az adatbiztonsági feladatokat a Createam Kft. látta el.

A Createam Kft. ezzel szemben előadta, hogy feladatát a FÁÜ Zrt. utasításai alapján látta el. Ezt támasztja alá az a tény és piaci gyakorlat, hogy a nyereményjátékot az adott termékeket forgalmazó vállalat, így a FÁÜ Zrt. marketing és értékesítési céljainak elérése érdekében, az általuk meghatározott döntések, és keretek között, az általuk napi szinten adott utasítások alapján szervezték meg. Ezzel ellentétben a FÁÜ Zrt. leszögezte, hogy egyetlen célja a projekt külsős lebonyolítása és a nyeremények kiosztása volt, de a fogyasztók konkrét személyei és adatai kívül estek a FÁÜ Zrt. érdekkörén.

A Createam Kft. állítása szerint nem vett igénybe további adatfeldolgozót. A Shirokuma Kft.-vel kötött webhosting megállapodás tárgya a szükséges tárhely és a tárhelyen lévő fájlok interneten való elérhetőségének biztosítása volt csupán.

5. A *„Pepsi – Lásd a világot 3D-ben” fogyasztói promóció részvételi szabályai”* című dokumentáció alapján a személyes adatok kezelésének jogalapja az érintett hozzájárulása. Az adatkezelés célja a nyereményjátékban történő részvétel érdekében való adatkezelés, azonban az érintett nyilatkozhatott úgy, hogy a FÁÜ Zrt. vagy annak megbízásából eljáró harmadik személy további marketing célú tevékenysége érdekében tovább kezelje a személyes adatait. A szabályzat tájékoztatja az adatalanyokat az érintetti jogosultságaikról, és felhívja a figyelmüket a jogorvoslati lehetőségekre. A szabályzat 20. pontja leírja, hogy az adatok feldolgozását a FÁÜ Zrt. megbízásából a Createam Kft. végzi. A FÁÜ Zrt. állítása szerint ezt a szabályzatot a Createam Kft. szövegezte meg, amelyet ők nem hagytak jóvá. A Createam Kft. tájékoztatása szerint a szabályzat a promóció honlapján mindenki számára elérhető volt.

A Createam Kft. válasza szerint a nyereményjátékot követően az adatok leválogatása megtörtént az alapján, hogy az érintett hozzájárulását adta-e a további adatkezeléshez. Ahol a hozzájárulás nem terjedt ki a további kereskedelmi célú adatkezelésre, azokat a személyes adatokat a Createam Kft. törölte a rendszeréből. Az adatok további felhasználására azonban nem került sor, mivel a FÁÜ Zrt. ilyen utasítást nem adott.

6. A FÁÜ Zrt. állítása szerint, az adatbiztonsági incidenst követően a FÁÜ Zrt. és a Createam Kft. a kárelhárító intézkedéseket közösen hajtotta végre, szorosan együttműködtek a károk csökkentése érdekében. Két feladatot tűztek ki célul, egyrészt az érintettek megfelelő tájékoztatását, másrészt az illegálisan közzétett adatok törlését. Körülbelül 50.000 személy volt érintett, ebből 695 fő esetében az email postafiók jelszava is kikerült a rendszerből. Az utóbbi érintetti kör volt a veszélyeztetettebb, mivel harmadik személyek a közzétett jelszóval visszaélve email postafiókba vagy akár azonos jelszóval védett egyéb személyes felületükre is beléphettek. Ennek a személyi körnek kétkörös email üzenetet, valamint SMS üzenetet küldött ki a Createam Kft., egyúttal felhívták a fogyasztók figyelmét a jelszó megváltoztatására a visszaélések elkerülése érdekében. A FÁÜ Zrt. válságkezelési intézkedései keretében válságkezelő csoport felállításáról gondoskodott, a fogyasztók megkeresése érdekében telefonos ügyfélszolgálatokat állítottak fel, rendőrségi feljelentést tettek a BRFK Gazdaságvédelmi Főosztályán, továbbá az érintett hatóságokkal felvették a kapcsolatot. A nyomozás a Hatóság vizsgálatának idején még folyamatban volt. Az ellopott és illegálisan közzétett személyes adatok törlése érdekében a FÁÜ Zrt. és a Createam Kft. felvették a kapcsolatot azoknak a honlapoknak (pastebin.com; bindrand.com; pastemine.com; hacktalk.com) az adminisztrátoraival, ahol az adatok közzétételre kerültek. A hacktalk.net kivételével az adatokat eltávolították a honlapokról.

A Createam Kft. állítása szerint a károk elhárítása és enyhítése során sem járhatott el önállóan, annak irányítását is FÁÜ Zrt. végezte. A Createam Kft. saját nevében is tett rendőrségi feljelentést.

7. A Createam Kft. a tájékoztatása alapján 2011. június 1. és 2011. augusztus 31. között bonyolította le a fent nevezett nyereményjátékot a FÁÜ Zrt. felkérése és iránymutatásai alapján. Állítása szerint az adatlopási incidenst a FÁÜ Zrt. alvállalkozója, a Soda Team Kft. által üzemeltetett http://3d.pepsi.hu webcímen keresztül követték el. A Createam Kft. állítása szerint az interneten felejtett aldomain és ennek a Shirokuma Kft. szerverére történő indokolatlan átirányítása tette lehetővé, hogy a FÁÜ Zrt.-t, vagyis a Pepsi-t támadó hackerek rátalálhattak arra a szerverre, ahol a bűncselekmény útján eltulajdonított adatokat a Createam Kft. a FÁÜ Zrt. kérésére előírásszerűen tárolta.

A Createam Kft.-nek nem volt tudomása arról, hogy a http://3d.pepsi.hu aldomaint átirányították a Shirokuma Kft. szerverére. Ezért nem a Createam Kft. felelt, az aldomain létrehozása, megszüntetése és átirányítása a FÁÜ Zrt. feladata volt. A Createam Kft. véleménye szerint a FÁÜ Zrt. alvállalkozója felelős és hibás azért, hogy a tettesek eljuthattak az adatokhoz.

Az ismeretlen tettesek globalizáció- és USA-ellenes üzenete alapján arra lehet következtetni, hogy a támadás célpontjai multinacionális, amerikai cégek voltak, mint a PEPSI, amelynek a FÁÜ Zrt. is egyik vállalata. A Createam Kft. véleménye alapján az elkövetés módja, indoka, célja és következménye azt bizonyítja, hogy a FÁÜ Zrt. által tulajdonolt és a Soda Team Kft. által egy éve, indokolatlanul az interneten felejtett link vezette el a hacker csoportot az adatokat tartalmazó szerverhez. A szerver a Createam Kft. alvállalkozójának, a Shirokuma Kft. üzemeltetésében állt. A Createam Kft. az erről szóló, a Shirokuma Kft.-vel kötött webhosting szerződés másolati példányát a Hatóság rendelkezésére bocsátotta.

8. A Createam Kft. által becsatolt levelezés alapján a PepsiCo egyesült királysági központja a www.pepsi.hu oldal biztonsági ellenőrzéséről intézkedett a promóció ideje alatt. A biztonsági ellenőrzés célja, hogy a Pepsi-fogyasztók adatainak megfelelő szintű védelmét biztosítsák. A levelezésből az derült ki, hogy az ellenőrzést 2011 októberében zárták le és egy jelentést bocsátottak a FÁÜ Zrt. és a Createam Kft. rendelkezésére, amiben egyes sebezhető pontokra hívták fel a figyelmet.

A tényállás pontos tisztázása érdekében a Hatóság a biztonsági ellenőrzésről szóló dokumentációt mindkét féltől bekérte. A FÁÜ Zrt. egy dokumentációt bocsátott a Hatóság rendelkezésére, míg a Createam Kft. a FÁÜ Zrt. által csatolttal egyező jelentés mellé még két jelentést mellékelt. Tekintettel arra, hogy a másik két dokumentum eredete, készítésének célja, az ügyhöz való kapcsolódása nem tisztázott, és a Createam Kft. sem adott erre vonatkozó tájékoztatást, így ezek vizsgálatát a Hatóság mellőzi.

A mindkét fél által azonos formában megküldött biztonsági ellenőrzésről szóló jelentés (a továbbiakban: jelentés) az egyes sebezhetőségi pontokat veszi sorra, és mindegyik esetben leírja a fenyegetettséget, annak hatásait, illetve a megoldási lehetőséget. A sebezhetőségi pontokat 1-5-ig tartó skálán értékelte, ahol az 1-es besorolás minimális sebezhetőséget mutat. A jelentésben négy esetben 3-as szintű, „súlyos” (serious) sebezhetőségi pont található. A „súlyos” besorolás a jelentés alapján az alábbiaknak felel meg: a rendszert támadó fél specifikus információkhoz nyer hozzáférést, mint például a biztonsági beállítások, amely visszaélésekhez vezethet. Ez azt jelenti, hogy a támadó a fájlok tartalmához részben hozzáférhet, azok tartalmát nyilvánosságra hozhatja, könyvtárakat böngészhet, nyilvánosságra hozhatja a szűrési szabályokat, valamint a biztonsági szerkezetet. Továbbá eredményezheti a szolgáltatások megtámadását, a szolgáltatás illetéktelen használatát, mint például elektronikus levelek továbbítását.

Súlyos sebezhetőségi besorolást kapott az interneten keresztüli kommunikáció biztonsági védelme, amelyet a jelentés több aspektusból vizsgált. Azonos besorolást kapott a távoli hozzáférés, amely sérülékenységet egy támadó könnyen kihasználhatna. Ezenkívül tizenhárom pont esetében állapítottak meg a jelentésben 2-es, azaz közepes fokú sebezhetőséget.

9. A FÁÜ Zrt. jogi képviselője iratbetekintési jogával élt 2013. július 30-án, amiről a Hatóság NAIH-559-16/2013/H. ügyiratszámon jegyzőkönyvet vett fel. Az iratbetekintési jog gyakorlása nem terjedt ki azon dokumentumokra, amelyek zártan kezeléséről döntött a Hatóság.

10. Az adatbiztonsági követelményeknek való megfelelés tisztázása érdekében a Hatóság további kérdések feltételét tartotta szükségesnek.

10.1. A FÁÜ Zrt. előadta, hogy műszaki utasításokkal nem látta el a Createam Kft.-t, továbbá ismételten hangsúlyozta, hogy a Createam Kft. a projekt teljes körű lebonyolítására és adatkezelési feladataira kapott felhatalmazást. A Createam Kft. az incidenst követően nem működött együtt a FÁÜ Zrt.-vel az adatokat tartalmazó szerver adatbiztonsági vizsgálatának elvégzése érdekében.

A FÁÜ Zrt. állítása szerint a 3d.pepsi.hu domaint a rendelkezésükre álló bizonyítékok alapján a Createam Kft. üzemeltette és véleményük szerint a honlap szerverre való „rámutatásának” megszüntetése a projekt után is a Createam Kft. feladata lett volna. Ennek alátámasztásául szolgál a megbízási szerződés 1.1.4. pontja, miszerint a megbízás kiterjed az SMS és WEB rendszer felállítására és üzemeltetésére. A 3d.pepsi.hu forráskódjával a Createam Kft. rendelkezett, illetve a domain műszaki jellemzői is arra engednek következtetni, hogy azt a Createam Kft. kezelhette. A Soda Team Kft. Microsoft alapú szerverrel dolgozott, a 3d.pepsi.hu weboldal azonban PHP és MySQL technológiákkal lett fejlesztve, így a Soda Team Kft. a technológiai korlátok miatt sem

üzemeltethette a domaint. A Soda Team Kft. szerepével kapcsolatban a FÁÜ Zrt. továbbá azt jelezte, hogy a promóciós tevékenységben nem vett részt. Sem a promóció szerveréhez, sem a 3d.pepsi.hu szerveréhez nem volt technikai vagy jogi hozzáférése a Soda Team Kft.-nek. A Soda Team Kft. a www.pepsi.hu oldalt üzemeltette, az ezzel kapcsolatos hosting tevékenysége 2012. év végén megszűnt. A FÁÜ Zrt. a Soda Team Kft.-vel kötött keretszerződés másolati példányát a Hatóság rendelkezésére bocsátotta.

A keretszerződés alapján a Soda Team Kft. a weboldalak kifejlesztését, elkészítését, meglévő oldalak továbbfejlesztését; weboldalak folyamatos üzemeltetését, működtetését és karbantartását vállalta. A keretszerződés a weboldalakkal kapcsolatos további teendőkre is kiterjedt, továbbá tartalmazta a szoftverfejlesztési és karbantartási, szoftver és hardver beszerzési tevékenységet is.

A FÁÜ Zrt. véleménye szerint az incidens és az aldomain fennmaradása között nincs ok-okozati összefüggés. Az incidens oka a Createam Kft. kezelésében lévő szerver nem megfelelő technikai vagy műszaki védelme lehetett, illetve egyéb ok-okozati összefüggés lehetett a személyes adatok nem megfelelő helyen történő tárolása miatt, ami – a FÁÜ Zrt. szerint – a Createam Kft. érdekkörébe eső kérdés. A FÁÜ Zrt. válasza szerint az adatfeltörés nyilvánvalóan nem következett volna be az aldomain szerverre történő „rámutatása" nélkül, a link fennmaradása azonban önmagában nem teremthet okot egy megfelelő védelmi rendszerrel ellátott szerver feltörésére, továbbá az incidens a promóció idején is bekövetkezhetett volna, amikor a rámutatás indokolt volt.

A FÁÜ Zrt. állítása szerint a kommunikáció irányítását a márka goodwill sérelmével, és reklámozói minőségében vele szemben várható potenciális fogyasztói kárigényekkel kapcsolatos szempontok miatt vette át, de nem mint adatkezelő intézkedett.

A FÁÜ Zrt. az adatok jövőbeni felhasználására vonatkozóan további utasításokat nem adott, a Createam Kft.-nek a szerződésben foglaltak szerint kellett eljárnia. A FÁÜ Zrt. a cég- és márkatulajdonos PepsiCo belső utasítása szerint legfeljebb 3 évig tárolhatja az adatokat, azonban a bekövetkezett incidensre tekintettel már nem születhet döntés a további felhasználásról.

10.2. A Createam Kft. az újabb végzésben megfogalmazott kérdésekkel kapcsolatban arról tájékoztatta a Hatóságot, hogy a promóció lezárását követően nem kapott további utasításokat a FÁÜ Zrt.-től az adatok kezelésével kapcsolatban.

A 3d.pepsi.hu és az adatokat tároló szerver között fennálló internetes kapcsolatról a Createam Kft.-nek állítása szerint nem volt tudomása, a kapcsolat felett nem cégük rendelkezett és ez nem volt a FÁÜ Zrt.-vel kötött szerződésük része. Elmondásuk szerint a domain a FÁÜ Zrt. tulajdonában van, annak kezelését a FÁÜ Zrt.-vel kötött szerződés alapján a Soda Team Kft. végezte.

A Createam Kft. elmondása szerint a biztonsági ellenőrzés eredménye alapján a FÁÜ Zrt. a Createam Kft.-től semmilyen módosítást, intézkedést nem kért. Ebből a Createam Kft. arra következetett, hogy a felállított oldal adatbiztonsági technológiája, architektúrája, működése megfelelt a FÁÜ Zrt.-nek. A Createam továbbá azt állítja, hogy 2011. október 18-án úgy tudta, hogy a promóciós aldomain 2011. október 31-ig lesz elérhető, amit azután a www.pepsi.hu-t üzemeltető Soda Team Kft. visszaállít a promóciót megelőző állapotba. Ez utóbbi intézkedésre nem került sor.

Az alkalmazott informatikai technológiákról a Createam Kft. tájékoztatta a Hatóságot. Előadta, hogy mind szerver oldali, mind pedig szoftver oldali logolást alkalmaztak az esetleges hibák vagy visszaélések kiszűrése érdekében. Erre vonatkozóan a FÁÜ Zrt.-től iránymutatást nem kaptak,

azonban a fejlesztések során folyamatosan egyeztettek és az elkészült elemek a FÁÜ Zrt. jóváhagyása után kerültek beépítésre.

Az elkövetés módjával kapcsolatban a Createam Kft. arról tájékoztatott, hogy a naplófájlok vizsgálata szerint az oldal egy automatizált feltörési eljárás áldozata lett, amelynek működési elve az volt, hogy végig vizsgálja a linkeken keresztül a lehetséges sebezhető pontokat. A naplófájlok alapján megállapítható volt, hogy az adatok eltulajdonítása a http://3d.pepsi.hu oldalon keresztül történt. A Createam Kft. véleménye szerint amennyiben a Soda Team Kft. megszüntette volna az internetes kapcsolatot az aldomain és az adatokat tároló nem nyilvános szerver között, úgy az incidens nem következhetett volna be.

A Createam Kft. az adatok tárolására vonatkozóan előadta, hogy az általános gyakorlatuk szerint az adatok mennyiségét minimalizálják, és jelszóval védetten MySQL táblában tárolják. Több szintű biztonsági rendszerük eleme […].

III. Az ügyben alkalmazandó jogszabályi előírások

Az Infotv. 3. § 2. pontja szerint: *„személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés."*

Az Infotv. 3. § 9. pontja értelmében az *„adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja."*

Az Infotv. 3. § 10. pontja kimondja, hogy *„adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése."*

Az Infotv. 3. § 17. pontja alapján az *„adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik."*

Az Infotv. 3. § 18. pontja meghatározza, hogy az *„adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi."*
Az Infotv. 4. § szerint:
„(1) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.
(2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

(3) A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
(4) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani."

Az Infotv. 5. § (1) bekezdés alapján *„személyes adat akkor kezelhető, ha*
a) ahhoz az érintett hozzájárul, vagy
b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés)."

Az Infotv. 7. §-a értelmében: *„(1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.*
(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
(4) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja
a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.
(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek."

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 3. § (1) bekezdése szerint *„személyes adat akkor kezelhető, ha*
a) ahhoz az érintett hozzájárul, vagy
b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete elrendeli."

IV. Megállapítások

1. Az Infotv. 3. § 2. pontja alapján „Pepsi – Lásd a világot 3D-ben” c. nyereményjáték során gyűjtött adatok (név, telefonszám, lakcím, e-mailcím, születési dátum) személyes adatnak minősülnek.

2. A nyereményjáték lebonyolítása során, valamint az azt követően alkalmazott adatkezelési gyakorlatot is vizsgálata alá vonta a Hatóság.

A fogyasztói promóciós részvételi szabályzat, valamint a FÁÜ Zrt. és a Createam Kft. a Hatóság végzésére adott, egybehangzó válaszai alapján megállapítható volt, hogy az adatkezelés jogalapja az Avtv. 3. § (1) bekezdés a) pontjának megfelelően, az érintettek hozzájárulása volt. A szabályzat értelmében az érintettnek meg volt a lehetősége a választásra, mivel a nyereményjátéknak akkor is résztvevője lehetett, ha promóción túli adatkezeléshez nem járult hozzá. A Hatóság elfogadta a Createam Kft. válaszát, miszerint 2011. augusztus 31-et követően az adatok leválogatása megtörtént, és azon érintettek személyes adatait törölték, akik a további adatkezeléshez nem járultak hozzá. Az adatkezelés célja meghatározott volt, továbbá az érintetteket tájékoztatták törléshez való jogukról, valamint a jogorvoslati lehetőségekről.

A Hatóság az adatkezelés vizsgálata során azt állapította meg, hogy az adatkezelés megfelelő jogalapon nyugodott.

3. Az adatlopási incidenst és az adatbiztonsági követelményeket vizsgálva a FÁÜ Zrt. és a Createam Kft. egymásnak ellentmondó nyilatkozatokat tettek arra vonatkozóan, hogy ki milyen szerepet töltött be a promóció során és az incidens bekövetkeztekor. A Hatóság az adatkezelői és adatfeldolgozói minőség megállapításakor irányadónak tekintette a 95/46/EK irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport 1/2010. számú véleményét az „adatkezelő” és az „adatfeldolgozó” fogalmáról (a továbbiakban: WP29 vélemény).

3.1. A FÁÜ Zrt. álláspontja szerint a promóciót teljes mértékben kiszervezte, annak lebonyolítása a Createam Kft. feladata volt. Ezzel szemben a Createam Kft. saját szerepét adatfeldolgozóként határozta meg, feladatait a FÁÜ Zrt. utasításai alapján látta el.

A Hatóság a két fél között létrejött megbízási szerződés 1.1.7. pontjában tett megállapítást, miszerint a Createam Kft. felhatalmazást kap többek között az adatkezelői és az adatfeldolgozói feladatok ellátására, túl általános megfogalmazásként értékelte. A szerződésben a felek nem térnek ki pontosan arra, hogy kinek milyen feladata van, holott a több tízezer személyt is érintő promóciós tevékenység során ez elvárható lett volna. Ezzel összefüggésben a Hatóság méltányolja azt az álláspontot, miszerint nem önmagában a definíciók határozzák meg az adatkezelői státuszt, hanem az adatokkal végzett tényleges tevékenységek. Önmagában azonban az a tény, hogy a FÁÜ Zrt. a nyertesek adatait leszámítva személyes adatokat fizikailag nem birtokolt, szintén nem elegendő bizonyíték arra vonatkozóan, amely alapján az adatkezelői minőségét a promócióval kapcsolatban a Hatóság kizárhatná. A WP29 vélemény ezzel egybevág, ugyanis azt mondja ki, hogy *„az adatokhoz való hozzáférés nem elengedhetetlen feltétele az adatkezelői minőségnek”*.

A FÁÜ Zrt. azon érvelése, hogy a Createam Kft. további adatfeldolgozót vett igénybe és emiatt szükségszerűen adatkezelő volt, nem fogadható el. A Createam Kft. és a Shirokuma Kft. közötti webhosting szerződés áttekintése után a Hatóság azt a következtetést vonta le, hogy a közöttük lévő szerződés tárgya tárhely és a tárhely interneten keresztüli elérhetőségének biztosítása volt.

Ez a tény tehát nem alapozza meg a Createam Kft. adatkezelői minőségét, mindazonáltal nem is zárja ki, hogy Shirokuma Kft. az Infotv. előírásaival ellentétes módon adatfeldolgozóvá vált.

A Hatóság a FÁÜ Zrt.-nek azt az álláspontját, miszerint a fogyasztók személye és adatai kívül estek az érdekkörén, nem fogadja el. Az adatok érintetti hozzájáruláson alapuló továbbkezelésének a célja egyértelműen az volt, hogy a FÁÜ Zrt. további marketing céljaira felhasználhassa azokat, így nem hivatkozhat alappal arra, hogy a fogyasztók adatainak további kezelése kívül esik az érdekkörén.

A rendelkezésre álló információk, levelezések másolata alapján a FÁÜ Zrt. sok tekintetben utasította a Createam Kft.-t, továbbá az adatok a nevéhez fűződő nyereményjáték lebonyolítása során kerültek összegyűjtésre, és az adatok kezelésének célját a FÁÜ Zrt. határozta meg. Az adatok a FÁÜ Zrt. érdekében kerültek a promóció során felhasználásra, illetve a jövőbeni felhasználás céljáról is ő rendelkezhetett volna. A WP29 vélemény értelmében az a fél minden esetben adatkezelőnek minősül, aki az adatkezelés vagy adatfeldolgozás célját meghatározza, de facto ezt a döntést meghozza.

A fogyasztói promóciós részvételi szabályzat rendelkezéseit sem kifogásolta a FÁÜ Zrt. – amely szerint ő minősül adatkezelőnek –, noha az mindenki számára elérhető módon a promóció honlapján közzé volt téve. Ugyanakkor a Hatóság elfogadja azt az érvelést, hogy nem önmagában a szabályzatban vagy a szerződésben használt fogalmak alapján kell megítélni a szerepeket, hanem a tényleges tevékenység alapján. Ezt a WP29 vélemény is hasonlóan fogalmazza meg.

A FÁÜ Zrt. továbbá a Createam Kft. adatkezelői minőségének bizonyítása érdekében hivatkozott arra, hogy a promóció résztvevőivel a Createam Kft. tartotta a kapcsolatot. Ez a tényező a Createam Kft. adatkezelői minőségére enged következtetni, azonban nem minősül olyan bizonyítéknak, amely egyben kizárná a FÁÜ Zrt. adatkezelői minőségét. A WP29 vélemény alapján az adatfeldolgozói minőségnek két, konjunktív feltétele van, az egyik, hogy az adatkezelőtől elkülönült szervezet végezze az adatfeldolgozást, valamint hogy nem saját nevében, hanem az adatkezelő nevében járjon el. Ez tehát nem zárja ki a FÁÜ Zrt. adatkezelői minőségét. A 3.2. pontban kifejtettek alapján bizonyítást nyert, hogy a Createam Kft. a FÁÜ Zrt. nevében tartotta a kapcsolatot az érintettekkel, tehát eleget tett ebben a tekintetben az adatfeldolgozó fogalmi feltételeinek.

A FÁÜ Zrt. adatkezelői minőségét erősíti továbbá a WP29 vélemény azon kitétele, miszerint vizsgálandó a domináns fél a jogviszonyban, továbbá az érintettek előtti ismertség, valamint az érintetteknek erre az ismertségre alapozott ésszerű elvárásai. Vélelmezhető, hogy az érintettek a nyereményjáték szervezőjének a FÁÜ Zrt.-t, a Pepsi kötődésű vállalatot gondolták, tekintettel arra, hogy a honlapon a Pepsi márkajelzése, védjegye volt megtalálható, valamint a nyereményjátékban történő részvétel Pepsi márkájú termékek vásárlásához volt kötve. A Createam Kft.-vel az érintett, a fogyasztó legfeljebb akkor került kapcsolatba, ha valamilyen panaszával, kérésével megkereste a nyereményjáték szervezőit, mert kapcsolatként a Createam Kft. elérhetőségei voltak megadva, de címzettként akkor is a FÁÜ Zrt.-t kellett feltüntetni.

A WP29 vélemény alapján az adatkezelő fogalmát nem befolyásolhatják olyan más, gyakran ellentétes vagy átfedésben lévő, egyéb jogterületekhez tartozó fogalmak, mint amilyen a szellemi tulajdon terén a szerző vagy a jogosult fogalma. Az, hogy valaki a szellemi tulajdon jogosultja, nem zárja ki annak a lehetőségét, hogy adatkezelőnek is minősüljön, és így alanya legyen az adatvédelmi jogból eredő kötelezettségeknek. Erre tekintettel a FÁÜ Zrt. nem hivatkozhat adatkezelői minőségének kizárására azon az alapon, hogy ő csak a márkajelzést adta a promóció lebonyolításához.

3.2. A Createam Kft. szerepét vizsgálva a Hatóság azt állapította meg, hogy tevékenysége végzéséhez sok tekintetben a FÁÜ Zrt. utasítást adott, azonban minden lényeges körülményt nem határozott meg számára. Az adatfeldolgozás egyes, érdemi döntést nem igénylő technikai műveletek elvégzését jelenti, különösen ilyen az adatrögzítés és az archiválás. Az adatfeldolgozás fogalmi körén belül csak az a tevékenység fogadható el, ahol az adatkezelő érdemi döntést nem igénylő tevékenységelemeket ruházza át az adatfeldolgozóra. A WP29 vélemény alapján az adatfeldolgozó fogalmi körén addig nem terjeszkedik túl, amíg a feldolgozás módjának meghatározása az adatfeldolgozó részéről csak technikai és szervezeti kérdéseket érint. Amennyiben az adatfeldolgozás módjára való befolyás szintje azonban olyan mértékű, hogy az előbbiekben említetteken túlterjeszkedik, úgy adatkezelői minőséget kap.

A WP29 vélemény alapján az adatfeldolgozói minőségnek két, konjunktív feltétele van, ahogy ezt a 3.1. pontban már leírtuk. A Createam Kft. mindkét feltételnek eleget tett, mivel a FÁÜ Zrt.-től elkülönült szerv és a fogyasztói promóció részvételi szabályaiból az derült ki az érintett számára, hogy törlési kérelme vagy egyéb kérdése esetén a FÁÜ Zrt.-hez fordulhat, tehát a Createam Kft. a FÁÜ Zrt. nevében tett eleget feladatainak.

A Createam Kft. a promóció lebonyolítása során az adatfeldolgozó fogalmi körén nem terjeszkedett túl. A nyereményjáték lebonyolítására a FÁÜ Zrt. adatkezelői, adatfeldolgozói jogosítványokat adott a Createam Kft. részére, a megbízási szerződés 5.9. pontja szerint a *„[…] a projekt komplex és a fogyasztók védelme szempontjából jogszabályilag szigorúan szabályozott jellegénél fogva napi (illetve adott esetben napszaki) pontosságú a megbízó által adott és a megbízott által elfogadott specifikációknak megfelelő […] teljesítést igényel […].”* A fenti rendelkezések alapján a FÁÜ Zrt. adta az utasításokat, specifikációkat. A Createam Kft. köteles volt ezeknek a specifikációknak megfelelően eljárni, csak annyiban dönthetett az adatok feldolgozásának módjáról, amennyiben arra a FÁÜ Zrt.-től nem kapott utasítást. A WP29 vélemény azt is adatfeldolgozónak tekinti, aki a főként célokra vonatkozó általános iránymutatások alapján működik, de az iránymutatás a módokat illetően nem megy bele a részletekbe.

3.3. A Hatóság álláspontja és a WP29 vélemény értelmében a hatáskör/ feladat átruházása nem eredményezheti a személyes adatok védelmének csökkenését. A felelősséget úgy kell elosztani, hogy az adatvédelmi szabályok betartása a gyakorlatban megfelelően biztosított legyen. A 3.1. és a 3.2. pontban tárgyalt körülményekre tekintettel, valamint arra, hogy a FÁÜ Zrt. és Createam Kft. nem tisztázták megfelelően szerződésben a jogviszonyukat az adatok kezelése vonatkozásában, a Hatóság megállapítja a FÁÜ Zrt. adatkezelői minőségét és a Createam Kft. adatfeldolgozói minőségét.

A Hatóság fontosnak tartja kiemelni, hogy az adatkezelői, illetve adatfeldolgozói minőség az Infotv. 7. § (2) bekezdése alapján az adatbiztonsági kérdésekkel kapcsolatban nem válik el élesen, tekintettel arra, hogy az adatkezelő általános felelőssége mellett az adatfeldolgozó a tevékenységi körében a végzett műveletek során az adatok biztonságáról ugyanúgy köteles gondoskodni.

4. A Hatóság a FÁÜ Zrt. és a Createam Kft. javára értékelte, hogy az adatlopási incidenst követően együttműködve azon dolgoztak, hogy a károkat enyhítsék, illetve az esetleges további károk bekövetkezését megelőzzék. Ennek érdekében válságkezelő csapatot állítottak fel, továbbá az érintetteket a rendelkezésre álló kommunikációs csatornák mindegyikén próbálták értesíteni és felhívni a figyelmüket a további teendőkre.

Az érintettek tájékoztatásán túlmenően felvették a kapcsolatot azon honlapok adminisztrátoraival, ahol az ellopott adatokat közzétették és kérték a jogellenesen közzétett adatok törlését. Az adatok

megjelentek a pastebin.com, a binrand.com, pastemine.com és a hacktalk.net oldalakon. A hactalk.net oldal kivételével az adatokat rövid időn belül sikerült eltávolítatniuk.

A http://leaks-db.hacktalk.net/node/20 oldalon a több mint 50 ezer felhasználó adata az incidenst követően több mint 9 hónapig elérhetőek voltak. Az oldal a „Pepsi Hungary Accounts Leak 3" címet viselte, és az adatok az alábbi sorrendben kerültek feltűntetésre: név, email cím, helység név, mobil szám, születési dátum, regisztráció időpontja. A Hatóság folyamatosan ellenőrizte az adatok elérhetőségét és azt állapította meg, hogy 2013. július 16-án az adatok még elérhetőek voltak, az ezt követő (2013. augusztus 22.) ellenőrzés során már nem. Az adatok jogellenes nyilvánosság felé közvetítése tehát több mint 9 hónapon keresztül megvalósult.

5. Az Infotv. 7. § (3) bekezdés értelmében az adatokat megfelelő intézkedésekkel védeni kell, a konkrét esetre alkalmazandóan különösen a jogosulatlan hozzáféréstől, továbbítástól és a nyilvánosságra hozataltól. Az adatlopási incidens során az adatokhoz jogosulatlanul hozzáfértek, és különböző oldalakon jogosulatlanul nyilvánosságra is hozták.

5.1. Az érintett adatokat a 2011. június 1. és 2011. augusztus 31. között lezajlott *„Pepsi – Lásd a világot 3D-ben"* című promóció során gyűjtötték. Az adatlopási incidens 2012. október 13-án, több mint egy évvel a nyereményjáték lezárását követően történt.

5.2. Az Infotv. 7. § (6) bekezdése alapján mind az adatkezelőnek, mind pedig az adatfeldolgozónak kötelessége az adatok biztonságát szolgáló intézkedések megtétele, oly módon, hogy azok a technika mindenkori fejlettségére tekintettel a lehető legmagasabb szintű védelmet biztosítsák. A FÁÜ Zrt.-től és a Createam Kft.-től – tekintettel gazdasági súlyukra és arra, hogy több mint 50 ezer érintett személyes adatát kezelték – elvárható volt, hogy ennek a kikötésnek úgy tesznek eleget, hogy a rendelkezésre álló adatbiztonsági technikák közül a leghatékonyabbat alkalmazzák.

5.3. A tényállás tisztázása során az állapítható meg, hogy a 3d.pepsi.hu aldomain internetes fellelhetősége vezette el az elkövetőket a szerver adataihoz. Az aldomain üzemeltetőjére vonatkozóan eltérő álláspontra helyezkedtek a felek. A FÁÜ Zrt. szerint az oldal üzemeltetője a Createam Kft. volt, míg a Createam Kft. szerint a FÁÜ Zrt. alvállalkozója, a Soda Team Kft. felelt az érintett honlapért.

A Createam Kft. által becsatolt levelezés alapján a PepsiCo egyesült királysági központja a www.pepsi.hu oldal biztonsági ellenőrzéséről intézkedett a promóció ideje alatt. A biztonsági ellenőrzés célja az volt, hogy a PepsiCo fogyasztók adatainak megfelelő szintű védelmét biztosítsák. Erről a PepsiCo 2011. június 9-én értesítette a Soda Team Kft.-t. A Soda Team Kft. 2011. június 9-i válaszában arról tájékoztatta a PepsiCo-t, hogy ez 2011. május 16. óta nem az ő feladata, és forduljanak a FÁÜ Zrt.-hez. A biztonsági ellenőrzés lefolytatásához szükséges adatok megadásában a FÁÜ Zrt. mellett a Createam Kft. működött közre. A biztonsági ellenőrzés lezárásról 2011. október 4-én érkezett válasz a PepsiCo-tól, amelyben néhány sebezhető pontra (some vulnerabilities) hívják fel a figyelmet. A PepsiCo mind a Createam Kft., mind pedig a FÁÜ Zrt. részére megküldte a biztonsági ellenőrzés során feltárt sebezhetőségi pontokra való felhívó levelét. Ezenkívül a PepsiCo felajánlotta, hogy szervez egy találkozót a jelentésben megfogalmazottak áttekintésére, hogy azok orvoslása megfelelő legyen. Erre válaszul 2011. október 18-án a Createam Kft. jelezte, hogy az oldal üzemeltetését nem ők látják el, nem ők felelősek érte. A FÁÜ Zrt. a kapott jelentés alapján, valamint a Createam Kft. felelősséget kizáró levelére tekintettel köteles lett volna tisztázni, hogy a jelentésben feltárt hiányosságok orvoslása kinek a feladata. A Hatóság megállapította, hogy a jogellenes magatartást súlyosbítja, hogy az incidens bekövetkezését megelőzően több mint egy évvel már tudomása volt az adatkezelőnek arról, hogy a promoció során felvett és tovább kezelt adatok védelme több ponton sebezhető.

A levelezésbe a Soda Team Kft. munkatársa annyiban kapcsolódott be, hogy jelezte, 2011. május 16-tól már nem látja el a Pepsi honlapjának fejlesztését, üzemeltetését. Ezzel szemben a FÁÜ Zrt. a Hatóság megkeresésére adott, 2013. augusztus 21-én érkezett válaszában arról tájékoztat, hogy a Soda Team Kft.-vel kötött szerződése 2012. év végén szűnt meg.

A FÁÜ Zrt. által hivatkozott szempontból, miszerint a forráskód a Createam Kft. birtokában volt, további következtetés nem vonható le, tekintettel arra, hogy a MySQL sajátossága, hogy szabad forráskodú. Ez tehát nem támasztja alá azt, hogy az aldomain üzemeltetéséért a Createam Kft. felelt.

A FÁÜ Zrt. továbbá arra hivatkozott, hogy a Soda Team Kft. azért sem lehetett az aldomain üzemeltetője, mert Microsoft alapú szervere van, a 3d.pepsi.hu oldal PhP és MySQL technológiákkal lett fejlesztve és két rendszer egymással nem kompatibilis. Ezzel szemben a MySQL és PhP technológiák platform független technológiák, melyek minden ismert környezetben használhatóak, tehát Microsoft alapú környezetben is.

A Createam Kft. által csatolt 2011. október 18-i levelezés azt támasztja alá, hogy a Createam Kft.-nek nem volt tudomása az aldomain és a szerver közötti kapcsolatról. Az említett levelezés értelmében a Createam Kft. abban a hiszemben volt, hogy az aldoimaint 2011. október 31-vel megszünteti a Soda Team Kft. és az oldalt a promóciót megelőző állapotba állítja vissza. Tekintettel arra, hogy ezt a levelet a FÁÜ Zrt. munkatársa is megkapta, amennyiben ez egy félreértés volt a Createam részéről, úgy elvárható lett volna a FÁÜ Zrt.-től annak tisztázása, hogy az oldalt ki fogja törölni és megszüntetni a szerverre való rámutatást. Az aldomain és szerver közötti kapcsolat annak ellenére élt tovább, hogy az adatkezelés célja már megváltozott.

A Hatóság arra az álláspontra helyezkedik, hogy a FÁÜ Zrt.-nek kellett volna gondoskodnia a 3d.pepsi.hu aldomain törléséről és az adatokra való rámutatás megszüntetéséről.

Tehát az Infotv. 7. § (3) bekezdésére tekintettel a FÁÜ Zrt. nem tett meg minden megfelelő intézkedést annak érdekében, hogy a személyes adatokat a jogosulatlan hozzáféréstől és nyilvánosságra hozataltól megvédjék.

5.4. Az egyesült királysági központ által készített jelentésből az a következtetés vonható le, hogy az adatok távoli hozzáférés útján voltak leginkább sebezhetőek. A felelősség súlyát növeli az a tény, hogy ennek az információnak a birtokában volt mind a FÁÜ Zrt., mind pedig a Createam Kft. az incidens bekövetkezése előtt egy évvel.

5.5. Az adatokat egyik szereplő által sem vitatottan olyan módon, illetve a világhálóról elérhető olyan felületen tárolták, amely nem nyújtotta az Infotv. által előírt védelmet. Az Infotv. adatbiztonságra vonatkozó szabályai megkövetelték azt, hogy az adatokat egyrészt olyan módon és helyen tárolják, ahol az illetéktelen hozzáféréstől való védelem biztosított, másrészt pedig az egyéb, elvárható technikai adatbiztonsági intézkedéseket alkalmazzák. Függetlenül attól, hogy az előző mondatban megfogalmazott második kitétel érvényesült-e, tehát a szükséges egyéb technikai adatbiztonsági intézkedéseket megtették-e, az első pontban megfogalmazott követelmény sérelme megvalósult: az adatokat sérülékeny, a világhálóról elérhető felületen hagyták („felejtették”), ami magas fokú biztonsági intézkedések egyidejű alkalmazása mellett is, önmagában is jogsértő, a mulasztás és a bekövetkezett jogsérelem közötti kapcsolat egyértelműen kimutatható.

A világhálón köztudottan jelenlévő kockázatok minden szereplő számára ismertek voltak. Az internetes promóciós kampányokat üzletszerűen kezdeményező, arra megbízást adó gazdasági

szereplő részéről ez a mulasztás nagyfokú gondatlanságként értékelendő, amelynek a következménye a fent leírt „sikeres” hackertámadás volt. Az adatbiztonsági intézkedések hiányossága révén adatvédelmi jogi értelemben tehát egyértelműen megragadható az adatkezelő jogellenes közrehatása abban, hogy az egyébként szintén jogellenes hackertámadás elérje célját, és a személyes adatok nyilvánosságra kerüljenek. Meg kell említeni azt a nemzetközi gyakorlatban is számon kért elvárást, amely szerint az ügyek elbírálása során tekintettel kell lenni az érintettek elvárásaira, várakozásaira személyes adataik (magánszférájuk) védelmével kapcsolatban. A vizsgált esetben az érintettek alappal számíthattak arra, hogy a promóció során kezelt adataik biztonságban vannak. Az adatalanyok számára teljesen életszerűtlen és indokolhatatlan volt az incidenshez vezető adatbiztonsági mulasztás, hangsúlyozva, hogy a promóció lezárását követő egy évvel, az adatbiztonsági jelentés megállapításainak ellenére sérülékeny felületen tárolták az adatokat.

V. Eljárási szabályok

A fentiekre tekintettel, a Hatóság a rendelkező részben foglaltak szerint döntött, és jelen határozatban a FÁÜ Zrt.-t adatvédelmi bírság megfizetésére kötelezte. Jelen határozat a Ket. 71. § (1) bekezdésén és a 72. § (1) bekezdésén alapul.

Az Infotv. 61. § (1) bekezdésének f) pontja értelmében a Hatóság az Infotv. 61. § (3) bekezdése szerinti, százezer forinttól tízmillió forintig terjedő bírság kiszabására jogosult jogellenes adatkezelés megállapítása esetén. A bírság összegét a Hatóság jogszabályon alapuló mérlegelési jogkörében eljárva az Infotv. 61. § (4) bekezdése alapján határozta meg.

A Hatóság a bírság kiszabása során figyelembe vette az eset összes körülményét. A bírság kiszabását indokolta, hogy a FÁÜ Zrt. megsértette az Infotv. adatbiztonságra vonatkozó rendelkezéseit. A bírság összegét növelő tényezőként vette figyelembe a Hatóság, hogy több mint 50 ezer személy adatát tulajdonították el és tették közzé, illetve a jogsérelem több mint 9 hónapon keresztül fennállt. Ugyanakkor a Hatóság a javára értékelte, hogy az incidens bekövetkezését követően minden célszerű intézkedést megtett a károk enyhítése és azok elmaradása érdekében.

Az adatvédelmi hatósági eljárásnak az Infotv. 60. § (5) bekezdésében meghatározott, egy alkalommal meghosszabbított ügyintézési határideje 5 nappal került túllépésre figyelembe véve, hogy a tényállás tisztázásához szükséges adatok beszerzésére irányult felhívásoktól azok teljesítéséig terjedő idő az eljárási határidőbe nem számít be.

A határozatnak a Hatóság honlapján történő nyilvánosságra hozatalát a érintettek nagy számára, valamint a jogsértés súlyára tekintettel az Infotv. 61. § (2) bekezdése alapján rendeltem el.

A határozat a Ket. 73/A. § (3) bekezdése alapján a közlés napján jogerőre emelkedik. A fellebbezést a Ket. 100. § (1) bekezdésének d) pontja zárja ki. A határozat bírósági felülvizsgálatának lehetőségét a Ket. 100. § (2) bekezdése biztosítja, a Fővárosi Közigazgatási és Munkaügyi Bíróság illetékességét a polgári perrendtartásáról szóló 1952. évi III. törvény (továbbiakban: Pp.) 326. § (7) bekezdése alapján állapítottam meg. A keresetlevél benyújtásának helyét és idejét a Pp. 330. § (2) és (3) bekezdése határozza meg.

A pénzfizetési kötelezettség önkéntes teljesítésének elmaradása esetén a Ket. 129. §-a szerint a kötelezett szabad rendelkezése alatt álló, pénzügyi intézménynél kezelt összeget kell végrehajtás alá vonni.

A bírságot a megfelelő számlaszámra megfizetni a pénzforgalom lebonyolításáról szóló 18/2009. (VIII. 6.) MNB rendelet (a továbbiakban: MNB rendelet) 25. § a) pontjának aa) alpontjában (átutalás), b) pontjának bb) alpontjában (készpénzbefizetés fizetési számlára), c) pontjának ca) alpontjában (készpénzátutalás) felsorolt fizetési módok formájában lehet. A kötelezettség teljesítése során irányadó az MNB rendelet VI. fejezete, azzal a kitétellel, hogy a Hatóság épületében nincs lehetőség a bírságösszeg befizetésére.

A késedelmi pótlék mértékéről szóló tájékoztatásom az adózás rendjéről szóló 2003. évi XCII. törvény 165. § (2) bekezdésében foglaltakon alapul. Az államháztartásról szóló 2011. évi CXCV. törvény 42. § (3) bekezdése szerint a jogerősen kiszabott és meg nem fizetett bírság, valamint a meg nem fizetett bírság miatt jogerősen kiszabott és meg nem fizetett késedelmi pótlék köztartozásnak minősül, és adók módjára kell behajtani.

A Ket. 74. §-a alapján a Kötelezett a teljesítési határidő lejárta előtt benyújtott kérelmében annak igazolásával kérheti a Hatóságtól a pénzfizetési kötelezettség teljesítésére halasztás vagy a részletekben történő teljesítés (a továbbiakban együtt: fizetési kedvezmény) engedélyezését, hogy rajta kívül álló ok lehetetlenné teszi a határidőre való teljesítést, vagy az számára aránytalan nehézséget jelentene.

A határidő lejárta után az ügyfél - feltéve, hogy a végrehajtást még nem indították meg - az igazolási kérelem egyidejű benyújtásával kérhet fizetési kedvezményt. Ha a Hatóság elutasítja az igazolási kérelmet és a fizetési kedvezmény iránti kérelmet, egyidejűleg dönt a végrehajtás megindításáról is.

Amennyiben részletfizetésre vonatkozó kérelmet kíván előterjeszteni, úgy az illetékekről szóló 1990. évi XCIII. törvény (Itv.) 28. § (1) bekezdésére tekintettel illetéket kell fizetni, mivel a fizetési könnyítésre vonatkozó eljárás nem tartozik a 33. § (2) bekezdésében foglalt alkotmányos jogok érvényesítése okán illetékmentes eljárások körébe. Az Itv. 29. § (1) bekezdés szerint a kérelemre indult elsőfokú eljárás illetéke 3000 Ft, melyet a kérelem beterjesztésével egyidejűleg kell leróni.

Az illeték mértékéről és az illetékfeljegyzési jogról való tájékoztatás az illetékekről szóló 1990. évi XCIII. törvény 43. §-ának (3) bekezdésén, valamint a 62. § (1) bekezdésének h) pontján alapul.

A Hatóság feladat- és hatáskörét, valamint illetékességi területét az Infotv. szabályozza.

Budapest, 2013. november 7.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár