Ügyszám: NAIH/2018/356/3/H.
Előzmény: NAIH/2017/3979/H

Tárgy: a BKK Budapesti Közlekedési Központ Zrt. adatkezelése

H A T Á R O Z A T

A BKK Budapesti Közlekedési Központ Zrt. (1075 Budapest, Rumbach Sebestyén utca 19-21.) (a továbbiakban: Kötelezett) fenti számú ügyében a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) az alábbi döntéseket hozza:

1. A Hatóság megállapítja a Kötelezett jogellenes adatkezelését és felszólítja az alábbiakra:

- Az adatkezelés megkezdését megelőző tájékoztatási kötelezettségének megsértése miatt az adatkezelési tájékoztatási gyakorlatát az Infotv. rendelkezéseire figyelemmel módosítsa, és a jövőben adjon megfelelő tájékoztatást az adatalanyok részére.
- Az adatbiztonság követelményének megsértése miatt tegye meg a szükséges intézkedéseket annak érdekében, hogy az adatvédelmi incidens körülményeit, valószínűsíthető kockázatait feltárja, és ezekről a 2017. július 24. előtti időszakban regisztrált felhasználókat tájékoztassa.
- Megfelelően gondoskodjon az adatbiztonsági követelmények teljesítéséről, és ennek keretében alkosson meg az incidensek kezelésével kapcsolatos belső eljárásrendet, valamint a megbízott adatfeldolgozót is lássa el az ehhez szükséges utasításokkal, és ezeket írásban rögzítse az adatfeldolgozásra vonatkozó szerződésben.

2. A Hatóság a Kötelezettet továbbá

10.000.000 forint, azaz tízmillió forint
adatvédelmi bírság

megfizetésére kötelezi.

A bírságot a határozat jogerőre emelkedését követő 15 napon belül a Hatóság központosított bevételek beszedése célelszámolási forintszámlája (10032000-01040425-00000000) javára kell megfizetni. Az összeg átutalásakor a NAIH/2017/3979/H. BÍRS. számra kell hivatkozni.

A Hatóság egyidejűleg elrendeli jelen határozatnak a honlapján – a védett adatnak minősülő adatok kitakarása mellett - azonosító adatokkal történő nyilvánosságra hozatalát.

A Kötelezett a megtett intézkedéseiről a bírósági felülvizsgálat kezdeményezésére irányadó keresetindítási határidő lejártától számított 30 napon belül haladéktalanul értesítse a Hatóságot. Az értesítéshez csatolja megtett intézkedéseket alátámasztó dokumentumokat.

Ha a Kötelezett a bírságfizetési kötelezettségének határidőben nem tesz eleget, késedelmi pótlékot köteles fizetni. A késedelmi pótlék mértéke minden naptári nap után a felszámítás időpontjában érvényes jegybanki alapkamat kétszeresének 365-öd része. 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.

3. Az adatvédelmi hatósági eljárást a T-Systems Magyarország Zrt. (Budapest 1117 Budafoki út 56.; a továbbiakban: TSM) ügyfél vonatkozásában – mivel a hivatalbóli eljárás jogsértést nem tárt fel – megszünteti.

E döntés ellen közigazgatási úton jogorvoslatnak helye nincs, de a közléstől számított 30 napon belül a Fővárosi Törvényszékhez 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. Az eljárás menete, a tényállás tisztázása

1. Az ügy tárgya és a hatósági eljárást megelőző vizsgálati ügy

A Hatósághoz bejelentések érkeztek a Kötelezett által üzemeltett online jegyértékesítési rendszerrel összefüggő adatkezeléssel kapcsolatban. A bejelentők azt kifogásolták, hogy a BKK online jegyértékesítési rendszere nem felel meg az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 7. §-ában foglalt adatbiztonsági követelményeknek. Több panaszban kifogásolták továbbá, hogy a sajtóban megjelent hírek[1] alapján valószínűsíthető, hogy a regisztráció során megadott személyes adataikhoz harmadik személyek jogosulatlanul hozzáférhettek.

A 24.hu internetes hírportál munkatársa 2017. július 24-én megküldte a Hatóság részére, (a kezelésében lévő példány egyidejű törlése mellett) azon dokumentumokat, amelyek állításuk szerint bizonyítják, hogy a Kötelezett által üzemeltetett online jegyértékesítési rendszer adatbázisából kigyűjtött, a regisztrált felhasználók személyes adatait tartalmazó adatbázishoz arra jogosulatlan személyek is hozzáférhetnek. Ezt követően ugyanezen hírportálon 2017. július 25-én megjelent egy újságcikk, amely beszámolt arról, hogy milyen hiányosságai vannak a Kötelezett online jegyértékesítési rendszerének, amelyek nagy mennyiségű személyes adathoz való jogosulatlan hozzáférést tesznek lehetővé. A hírportál újságcikkében beszámolt arról is, hogy birtokába került az említett adatbázis, amelyet a Hatóság részére megküldtek, ezzel támasztva alá a rendszer hiányosságairól szóló állításokat.

A fentiek alapján a Hatóság NAIH/2017/3702/V. ügyszámon az Infotv. 52-58. §-aiban foglaltak alapján vizsgálati eljárást folytatott le. Ennek során a Hatóság megkeresésére adott válaszában a Kötelezett az adatbiztonsági követelményekkel összefüggésben úgy nyilatkozott, hogy „*az*

[1] http://index.hu/tech/2017/07/14/ez_nektek_e-jegy_kedves_bkk/;
http://index.hu/tech/2017/07/14/meghekkelheto_a_bkk_rendszere_barmennyiert_lehet_jegyet_venni/;
http://index.hu/tech/2017/07/14/meghekkelheto_a_bkk_rendszere_barmennyiert_lehet_jegyet_venni/;
http://index.hu/tech/2017/07/15/barki_feltorheti_a_bkk_elektromos_jegyvasarlo_rendszeret/;
http://index.hu/tech/helpdeszka/2017/07/17/bkk_e-jegyet_vett_azonnal_valtoztasson_jelszot/;
http://index.hu/belfold/budapest/2017/07/18/bkk_digitalis_berlet/;
http://index.hu/tech/2017/07/21/a_bkk_webshopja_biztonsagos/;
http://index.hu/tech/2017/07/21/barki_torolheti_a_bkk_rendszerebol_a_nevrokonainak_fiokjat/;
http://24.hu/tech/2017/07/25/regisztralt-a-bkk-e-jegy-rendszereben-hozzaferhettek-az-adataihoz/

adatbázis szervereket a rendszert szállító és üzemeltető TSM a saját maga által üzemeltetett infrastruktúrán tette lehetővé, ezekhez a szerverekhez a BKK Zrt. Informatikai Fejlesztés és Üzleti Támogatásnak nincs hozzáférése, ennek következménye, hogy adatvédelmi incidens szempontból a BKK Zrt. nem rendelkezik olyan hozzáféréssel (adatbázis, naplóállomány), mellyel egyáltalán detektálni és / vagy kivizsgálni tudnánk egy esetlegesen bekövetkező eseményt az online jegyértékesítési rendszerrel összefüggésben. Az adatbázisokhoz csak a TSM által kijelölt üzemeltető kollégák férnek hozzá".

A Kötelezett nem azonosította adatvédelmi incidensként a sajtóban megjelent azon eseményt, mely szerint az online jegyértékesítési rendszerből több ezer felhasználó személyes adatai kerülhettek illetéktelenek birtokába, ezzel kapcsolatban nem tett nyilatkozatot. Lehetséges incidensként kezelt azonban egy, a személyes adatok törlésére, vagyis érintetti jogok gyakorlására irányuló kérelmet, amely során felmerült, hogy a törlés elvégzését megelőzően nem került megfelelően azonosításra az érintett. Ezen lehetséges incidens elhárítása érdekében a Kötelezett felfüggesztette a személyes adatok törlésében részt vevő munkavállalók hozzáférését az online jegyértékesítési felület háttérrendszeréhez. Tájékoztatta a Hatóságot arról, hogy a további intézkedések megtételét attól tette függővé, hogy történt-e ténylegesen adatvédelmi incidens.

Tekintettel arra, hogy a fentiek alapján a Hatóság a bejelentésekben szereplő, valószínűsített jogsértéseket a vizsgálati eljárás alapján megalapozottnak látta, az Infotv. 55. § (1) bekezdés a) pontjának ab) alpontja alapján a vizsgálati eljárásokat lezárta, és 2017. július 31-én a 60. § (1) és (4) bekezdése alapján hivatalból adatvédelmi hatósági eljárást indított. Az adatvédelmi hatósági eljárás tárgya a kötelezett online értékesítési rendszerével összefüggő adatkezelése, különös tekintettel az adatbiztonsági követelményekre és az érintettek előzetes tájékoztatására.

2. A tényállás tisztázása

A Hatóság 2017. augusztus 2-án végzésben nyilatkozatra hívta fel a Kötelezettet, illetve az eljárásba bevont másik ügyfelet, a TSM-et, amely az adatkezelői és adatfeldolgozói minőség meghatározására, az adatkezeléssel kapcsolatos utasításadás, illetve az adatbiztonsági intézkedések feltárására irányult.

A Kötelezett úgy nyilatkozott, hogy az online jegyértékesítési rendszer kialakítására és üzemeltetésére vonatkozóan a Kötelezett és a TSM között 2013. szeptember 4-én létrejött „Jegykiadó-automaták (TVM: Ticket Vending Machine) gyártása, szállítása, telepítése és teljes körű üzemeltetése" tárgyban a közbeszerzésekről szóló 2011. évi CVIII. törvény XIV. fejezete szerint 2013. szeptember 4. napján megkötött Fő projektszerződés, és annak 2017. július 13. napján kelt 3. számú módosítása alkalmazandó, amelyeket a Hatóság rendelkezésére bocsátott.

A Kötelezett előadta, hogy a Fő projektszerződés alapján a Kötelezett adatkezelőnek, míg a TSM adatfeldolgozónak minősül. Következésképpen a Kötelezett „*hagyta jóvá a felek közötti konszenzus alapján – az Sztv.-ben foglaltakra figyelemmel – a kezelt adatok körét, illetve a kezelt adatok időtartamát.*"

Az eljárásban részt vevő másik ügyfél, a TSM 2017. augusztus 18-án, illetve 2017. szeptember 21-én kelt nyilatkozataiban részletesen bemutatta azon indokokat, mely alapján megállapítható, hogy az online jegyértékesítési rendszer vonatkozásában adatfeldolgozónak minősül. Ezzel kapcsolatban többek között hivatkozott a felületen közzétett adatkezelési tájékoztatóra, mely egyértelműen tisztázza az adatkezelő kilétét. Előadta többek között, hogy a TSM a rendszer működése során keletkezett adatokat, információkat, az ezekből felépített adatbázisokat, azok file-szerkezetét, file-neveit, az adatbázis kezelő szoftvert kizárólag az üzemeltetési szerződésben (a

Fő projektszerződésben és annak releváns módosításaiban) rögzített feladatatok teljesítésére használhatja fel, amely szintén alátámasztja, hogy a rendszer vonatkozásában a TSM adatfeldolgozónak minősül.

A TSM a végzésekben megjelölt kérdésekre válaszolva tájékoztatta a Hatóságot az általuk kifejlesztett rendszer vonatkozásában alkalmazott technikai intézkedésekről. Előadta, hogy „*az online értékesítési rendszer adatbázis és alkalmazás szerverét a TSM üzemelteti, a DMZ zónában lévő infrastruktúrát (webszerverek, határvédelmi megoldások, routerek) és a kliensoldali eszközök és hálózati infrastruktúra üzemeltetését a BKK végzi*." Kiemelte, hogy „*az általunk [TSM] üzemeltetett szerverek a BKK tűzfal és határvédelmi megoldásai mögött helyezkednek el NAT-olt környezetben*." Tájékoztatta a Hatóságot továbbá arról, hogy „*az online jegyértékesítési rendszer adatbiztonsági vizsgálatára 2017. július 26-án felkérte az Ernst & Young Tanácsadó Kft.-t, amely cég a megkötött szerződés keretében a BKK webes értékesítési rendszerének sérülékenység és adatszivárgás vizsgálatát, továbbá komplex IT biztonsági vizsgálatát végzi el*." Az elkészült vizsgálati jelentést a TSM a 2017. szeptember 21-én kelt válaszához mellékelve megküldte a Hatóság részére, és tájékoztatta a Hatóságot arról, hogy abban rögzítésre kerültek a rendszerrel kapcsolatban feltárt sérülékenységek, ugyanakkor hangsúlyozta, hogy a független tanácsadó társaság sem tárt fel az Infotv. szerinti adatvédelmi incidensre utaló jelet, bizonyítékot. A TSM a Ket. 69. § (2) bekezdése alapján kérte a jelentés vonatkozásában az iratbetekintés korlátozását.

A Hatóság több alkalommal nyilatkozatra hívta fel a Kötelezetett arra vonatkozóan, hogy az adatkezeléssel kapcsolatban, így például az adatbiztonsági intézkedésekről milyen módon, és milyen tartalmú utasításokat adott az általa megbízott adatfeldolgozónak, a TSM-nek.

A Kötelezett az utasításadás módjaként mind a 2017. augusztus 17-én, mind a 2017. szeptember 15-én kelt nyilatkozataiban a Fő Projektszerződés V.2.6. pontját jelölte meg. Ez alapján „*A Felek tudomásul veszik, amennyiben a Fő Projektszerződésben foglalt feladat teljesítése személyes, illetve különleges adatnak minősülő adatot érint, kötelesek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény vonatkozó rendelkezései szerint eljárni. A Vállalkozó [TSM] kötelezettséget vállal arra, hogy az adatok védelmét érintő rendelkezésekről, szabályokról, ezek alkalmazásáról a szükséges tájékoztatásokat elvégzi*."

Emellett a Kötelezett utalt a Fő Projektszerződés mellékletét képező Műszaki Leírásra, valamint a Fő Projektszerződés 3. számú módosítására és annak mellékleteire, mint amelyek alapján az adatkezelő megbízta az adatfeldolgozót, valamint előadta, hogy az adatkezeléssel kapcsolatban külön nyilatkozat nem került kiállításra, egyéb megállapodás nem került megkötésre.

A Kötelezett úgy nyilatkozott, hogy az online jegyértékesítési rendszerre vonatkozó jogosultságokkal kapcsolatos szabályokat a BackOffice felhasználói kézikönyv, valamint a „BKK Online Shop ügyfélkiszolgálási feladatairól" szóló 3/2017/M/Ük sz. Ügyfélkapcsolati Igazgatói munkautasítás tartalmazza.

A Hatóság, - annak érdekében, hogy megállapítsa, hogy a kapott adatbázis valóban a Kötelezett által működtetett online jegyértékesítési rendszerből származik, - végzésben kötelezte a Kötelezettet arra, hogy a rendszer üzembe helyezése és 2017. július 24. közötti időszakra vonatkozó adatbázist küldje meg a Hatóság részére. A Kötelezett tájékoztatta a Hatóságot arról, hogy a rendszer indításától 2017. július 24-ig terjedő időszakban 6315 regisztráció történt, azonban a Hatóság végzésében foglaltakat, vagyis teljes körű adatbázist nem tud előállítani, arra csak az üzemeltető, vagyis az adatfeldolgozó képes. Tekintettel arra, hogy a Kötelezett nyilatkozatai alapján adatkezelőnek minősül az adatkezelés vonatkozásában, így az adatfeldolgozó is az ő utasításai alapján köteles eljárni, a Hatóság ismételten végzésben hívta fel a Kötelezettet, illetve egyúttal a

TSM-et is arra, hogy küldjék meg számára a vonatkozó időszakban keletkezett adatbázist. Mind a Kötelezett, mind a TSM eleget tett ezen felszólításnak.

Válaszában a Kötelezett az online értékesítési rendszerrel összefüggő személyes adatok vonatkozásában a jogalapot akként jelölte meg, hogy az adatkezelésre egyrészt a felhasználók hozzájárulása alapján, másrészt az Sztv. 7. §-a alapján kerül sor. Az előzetes tájékoztatással kapcsolatos kötelezettség vonatkozásában a Kötelezett úgy nyilatkozott, hogy ezen kötelezettségnek az adatkezelési tájékoztató rendelkezésre bocsátásával tesz eleget, melyet a regisztráció során a felhasználók megismernek. Álláspontja szerint a tájékoztató egyértelműen és részletesen tájékoztatja az érintetteket az adataik kezelésével kapcsolatos tényekről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre jogosult személyéről, az adatkezelés időtartamáról, valamint kitér az érintettek jogaira és jogorvoslati lehetőségeire is.

A Kötelezett a vizsgálati eljárás során tett, valamint a 2017. augusztus 17-én kelt válaszaiban nem azonosította adatvédelmi incidensként a sajtóban megjelent azon eseményt, mely szerint az online jegyértékesítési rendszerből több ezer felhasználó személyes adatai kerülhettek illetéktelenek birtokába.

Az ügyben mindkét fél iratbetekintési kérelemmel élt: a TSM 2017. szeptember 6-án, míg a Kötelezett 2017. szeptember 12-én tekintett bele az adatvédelmi hatósági eljárás irataiba, így az annak részét képező bizonyítékba, a 24.hu hírportál által a Hatóság részére továbbított dokumentumokba is.

Az iratbetekintést követően, 2017. szeptember 15-én kelt válaszában a Kötelezett úgy nyilatkozott, hogy az iratbetekintés során megállapította, hogy a Hatóság részére a 24.hu hírportál által elküldött adatbázis azonos a Kötelezett online jegyértékesítési rendszerének adatbázisával, vagyis történt adatvédelmi incidens. Egyidejűleg tájékoztatta a Hatóságot arról, hogy az ezzel kapcsolatos belső adatvédelmi felelős által folytatott vizsgálat még folyamatban van. Előadta, hogy az érintett személyes adatok körét, az érintettek számát nem tudta megállapítani, arra álláspontja szerint csak a Hatóságnak van lehetősége. A Kötelezett hangsúlyozta továbbá, hogy pontos intézkedéseket kidolgozni csak az incidens körülményeinek ismerete mellett lesz lehetősége.

Azzal kapcsolatban, hogy sor került-e az érintettek tájékoztatására az adatvédelmi incidensről, illetve annak lehetséges következményeiről, a Kötelezett úgy nyilatkozott, hogy azon felhasználókat, akik tájékoztatást kértek az Infotv. 15. § (1) bekezdése alapján, tájékoztatták, hogy a lehetséges incidenssel kapcsolatos belső vizsgálat még folyamatban van.

A Hatóság 2017. október 25-én kelt végzésére válaszul a Kötelezett ismételten arról tájékoztatta a Hatóságot, hogy a belső adatvédelmi felelős által az adatvédelmi incidenssel összefüggésben folytatott vizsgálat folyamatban van, mivel továbbra sem tudta megállapítani pontosan az adatvédelmi incidens időpontját, körülményeit, valamint az incidenssel érintett személyes adatok körét, az érintettek számát. Álláspontja szerint tehát továbbra sem határozható meg pontosan, hogy mely intézkedések megtételére van szükség, tekintettel arra, hogy az incidens körülményei nem ismertek előtte.

A Hatóság kérdésére a Kötelezett úgy nyilatkozott, hogy sor került a tűzfal naplóállomány vizsgálatára, elsősorban az infrastruktúrát ért támadások alatt és azt követően, melynek célja elsősorban a támadások forrásainak beazonosítása, illetve az ahhoz tartozó tűzfalszabályok létrehozása és így további támadások megakadályozása volt. Előadta továbbá, hogy a Kötelezett munkatársai a folyamat közben is vizsgálták az esetleges adatszivárgások lehetőségét, de ilyet a logokból nem tudtak megállapítani. Válaszához mellékelve megküldte a Hatóságnak a rendszer

indítása és 2017. július 24. közötti időszakban keletkezett, az értékesítési felületen alkalmazott tűzfal naplóállományát.

A Hatóság NAIH/2017/3979/21/H. számú végzésében felhívta a Kötelezettet arra, hogy a tűzfal naplóállományának elemzésével kapcsolatos vizsgálatok körülményeit, és eredményeit részletezze, valamint az állításait alátámasztó bizonyítékokat bocsássa a Hatóság rendelkezésére. A Kötelezett 2017. december 11-én kelt válaszában előadta, hogy a naplóállományt megküldte a Hatóság részére, azonban tekintettel arra, hogy az adatbázis informatikai üzemeltetését nem Kötelezett végzi, *„a szerződéses szolgáltató végezhetett részletesebb vizsgálatot az adatszivárgás tekintetében, különös tekintettel azon körülményre, hogy az ehhez szükséges, kiemelkedően nagy humánerőforrás igény és szakértelem a szolgáltató részére állhatott rendelkezésre."*

II. Az eljárás során megvizsgált dokumentumok

1. A 24.hu hírportál által a Hatóság részére megküldött, állításuk szerint a Kötelezett online jegyértékesítési rendszerébe regisztrált felhasználók személyes adatait tartalmaz adatbázis;
2. „Jegykiadó-automaták (TVM: Ticket Vending Machine) gyártása, szállítása, telepítése és teljes körű üzemeltetése" elnevezésű Fő Projektszerződés és annak mellékletei;
3. „Jegykiadó-automaták (TVM: Ticket Vending Machine) gyártása, szállítása, telepítése és teljes körű üzemeltetése" elnevezésű Fő Projektszerződés 3. számú módosítása és annak mellékletei;
4. Az online jegyértékesítési rendszer felületén regisztráló felhasználók rendelkezésére bocsátott adatvédelmi tájékoztató;
5. Táblázat a beállított felhasználókról és jogosultságokról;
6. BackOffice felhasználói kézikönyv vonatkozó része;
7. 3/2017/M/Ük sz. Ügyfélkapcsolati Igazgatói munkautasítás;
8. Adatvédelmi incidens nyilvántartás;
9. Az online jegyértékesítési rendszer indulásától 2017. július 24-ig terjedő időszakban regisztrált felhasználók személyes adatait tartalmazó adatbázis;
10. Az online jegyértékesítési rendszer üzembe helyezésétől 2017. július 24-ig terjedő időszakban keletkezett, az értékesítési felületen alkalmazott tűzfal naplóállománya;
11. Az Ernst & Young Tanácsadó Kft. által a Kötelezett online értékesítési felületével kapcsolatos sérülékenység- és adatszivárgás vizsgálatról készült jelentés.

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".*

7. pontja értelmében *„hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat – teljes körű vagy egyes műveletekre kiterjedő –* kezeléséhez",

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

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

26. pontja alapján: „*adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés."*

Az Infotv. 4. és 5. §-a 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. […]
5. § (1) 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 az alábbiakat tartalmazza:
„7. § (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."

Az Infotv. 10. §-a az adatfeldolgozással kapcsolatban az alábbiakat tartalmazza:

„(1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.

(2) Az adatfeldolgozó az adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót.

(3) Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

(4) Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt."

Az Infotv. 15. § (1)-(1a) bekezdései alapján:

„(1) Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

(1a) Az adatkezelő - ha belső adatvédelmi felelőssel rendelkezik, a belső adatvédelmi felelős útján - az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat."

Az Infotv. 20. § (1) bekezdése szerint „*az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.*"

Az Infotv. 20. § (2) bekezdése alapján az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

A személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény (a továbbiakban: Sztv.) az adatkezeléssel kapcsolatban az alábbiakat tartalmazza:

„7. § (1) A személyszállítási szerződés teljesítésével összefüggésben a menetdíjat meg nem fizető, vagy az utazási feltételeket egyéb módon megszegő utas azonosíthatósága, a személyhez kötött utazási jogosultság ellenőrzése, valamint a közszolgáltatási utazási kedvezmények igénybevétele jogszerűségének megállapítása céljából

a) a közforgalmú személyszállítási szolgáltatást teljesítő közlekedési szolgáltató,

b) a nemzeti mobilfizetési tevékenységet végző szervezet,

c) a 35/A. §-ban meghatározott működtető, továbbá

d) - ha a bevételek beszedését a közlekedésszervező végzi - a közlekedésszervező

vagy ezek megbízottja jogosult a személyszállítási szolgáltatásban részt vevő utas azonosíthatóságához szükséges, a (4) bekezdésben meghatározott adatok megismerésére.

(2) Az (1) bekezdésben meghatározott szervezet az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti adatvédelmi jogok érvényesítése mellett, továbbá e törvényben meghatározott korlátozó rendelkezések megtartásával az elektronikus adathordozón rögzített, nem személyhez kötött utazási jogosultság igénybevételével történő, egy alkalomnál több utazásra jogosító személyszállítási szerződés teljesítése érdekében, a szerződés teljesítéséhez szükséges mértékben - a személyszállítási üzletszabályzatban közzétett feltételek mellett - a (4) bekezdés a) pontjában meghatározott adatok kezelésére vonatkozó adatkezelési megállapodást köthet a személyszállítási szolgáltatásban részt vevő személlyel.

(3) Az (1) bekezdésben meghatározott szervezet a közszolgáltatási utazási kedvezmény vagy személyhez kötött utazási jogosultság keretében teljesítendő, elektronikus adathordozón rögzített utazási jogosultság igénybevételével történő utazásra jogosító személyszállítási közszolgáltatásra vonatkozó személyszállítási szerződés teljesítésével összefüggésben jogosult a (4) bekezdésben meghatározott adatoknak a szerződés teljesítéséhez szükséges mértékben történő kezelésére.

(4) Az (1) bekezdésben meghatározott szervezet adatmegismerési, adatkezelési jogosultsága a személyszállítási szolgáltatás alapjául szolgáló szerződés teljesítése érdekében a következő adatokra terjed ki:

a) a jogosult természetes személyazonosító adatai (családi és utónév, születési családi és utónév, születési hely és idő, anyja születési családi és utóneve), lakcíme, valamint személyazonosításra alkalmas hatósági igazolványának típusa és száma - ha 14. életévét betöltötte, akkor - aláírása is, vagy a jogosult részére elektronikusan kiállított, utazásra jogosító közlekedési kártya esetén annak egyedi sorszáma és a jogosult arcképmása,

b) az e törvényben meghatározottak szerinti, a közszolgáltatási utazási kedvezményekről szóló jogszabály alapján biztosított utazási kedvezmény esetén a kedvezmény jogcíme, a jogcímet megalapozó okmány azonosítója, típusa, érvényessége, kibocsátója, a jogosult adóazonosító jele és társadalombiztosítási azonosító jele,

c) az utazási viszonylathoz kötött kedvezmény esetén az utazási viszonylat, meghatározott időponthoz vagy időszakhoz kötött érvényességű kedvezmény esetén az érvényesség időszaka vagy időpontja.

(5) A (3) bekezdésben meghatározott esetben az (1) bekezdésben meghatározott szervezet a (4) bekezdésben meghatározott adatokat a polgári jogi igények elévüléséig nyilvántartja és kezeli.

(6) Az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvényben (a továbbiakban: Nektv.) meghatározott működtető, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény hatálya alá tartozó természetes személynek, valamint az egyéb, a közlekedési kártyára jogosult személynek a Nektv.-ben meghatározott regisztrációs szerv által folytatott kártyafelhasználói regisztráció során felvételezett és kezelt természetes személyazonosító adatait, lakcímét, egységes arcképmás- és aláírás-felvételezés során rögzített arcképmását és - ha a 12. életévét betöltötte - aláírását, valamint az általa képzett kapcsolati kódot közlekedési kártya kártyakibocsátása és nyilvántartása céljából az (1) bekezdés b) pontjában meghatározott szervezet részére átadja. A közlekedési kártya tekintetében a Nektv. szerinti kártyakibocsátónak az (1) bekezdés b) pontja szerinti szervezet minősül.

(7) Az (1) bekezdés b) pontjában meghatározott szervezet a közlekedési kártya kibocsátása iránti kérelemben a jogosult által megadott adatok, valamint az általa kibocsátott közlekedési kártya megszemélyesítését végző szervezetek adatközlése alapján a 30. § (2) bekezdésben rögzített feltételek biztosítása, valamint az e törvény felhatalmazása alapján kiadott

kormányrendeletben meghatározott szolgáltatási kötelezettsége teljesítése céljából, a Nemzeti Személyszállítási Intelligens Közlekedési Rendszerek Platform keretein belül központi nyilvántartást vezet, amely tartalmazza:

a) a (6) bekezdés szerinti adatokat,

b) a közlekedési kártya egyedi sorszámát és elektronikus egyedi azonosítóját,

c) a közlekedési kártya érvényességére vonatkozó adatokat,

d) a közszolgáltatási utazási kedvezmények igénybevételére való jogosultsági adatokat, valamint

e) a közlekedési kártya egyes közlekedési szolgáltató szervezeteknél való érvényesítési adatait.

(8) Az (1) bekezdés b) pontjában meghatározott szervezet a (7) bekezdés a) és d) pontjában meghatározott adatokat a közlekedési kártya érvényességének vagy a polgári jogi igény érvényesíthetőségének időpontjáig kezeli."

IV. A Hatóság megállapításai

1. Az adatkezelői és adatfeldolgozói minőség meghatározása

A Kötelezett nyilatkozata alapján az online jegyértékesítési rendszer kialakítására és üzemeltetésére a Hatóság rendelkezésére is bocsátott Fő projektszerződés, és annak 2017. július 13. napján kelt 3. számú módosítása alkalmazandó, amely alapján a Kötelezett adatkezelőnek, míg a TSM adatfeldolgozónak minősül.

A Kötelezett nyilatkozataiban az utasításadás módjával kapcsolatban a Fő projektszerződés V.2.6. pontját jelölte meg, mely alapján „*A Felek tudomásul veszik, amennyiben a Fő Projektszerződésben foglalt feladat teljesítése személyes, illetve különleges adatnak minősülő adatot érint, kötelesek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény vonatkozó rendelkezései szerint eljárni. A Vállalkozó [TSM] kötelezettséget vállal arra, hogy az adatok védelmét érintő rendelkezésekről, szabályokról, ezek alkalmazásáról a szükséges tájékoztatásokat elvégzi.*" A technikai intézkedésekkel kapcsolatban szintén a Fő projektszerződés V.2.6. pontjában található általános kötelezettségre hivatkozott.

Tekintettel a Kötelezett és a TSM egybehangzó nyilatkozatára, illetve a megvizsgált dokumentumok tartalmára, a Hatóság megállapította, hogy az online jegyértékesítési rendszerrel összefüggésben megvalósuló adatkezelés vonatkozásában a Kötelezett adatkezelőnek, míg a TSM adatfeldolgozónak minősül.

A Hatóság továbbá megállapította, hogy a Fő projektszerződés és annak módosítása alapján az online jegyértékesítési rendszerrel összefüggésben a TSM szerepe kettős: egyrészt a Kötelezett őt bízta meg a rendszer kifejlesztésével, megalkotásával; másrészt a rendszer üzemeltetését végzi a szerződés alapján.

2. Az adatkezelés jogalapja és az érintettek előzetes tájékoztatása

2.1. Az adatkezelés jogalapja

A Kötelezett az online értékesítési rendszerrel összefüggő személyes adatok vonatkozásában a jogalapot akként jelölte meg, hogy az adatkezelésre egyrészt a felhasználók hozzájárulása alapján, másrészt az Sztv. 7. §-a alapján kerül sor, vagyis kötelező adatkezelésre kerül sor.

A Kötelezett a „BKK Online Shop értékesítéshez kapcsolódó adatkezelési tájékoztató" című dokumentumban (a továbbiakban: adatkezelési tájékoztató) ellentmondásosan fogalmazta meg az

adatkezelés jogalapját. Az online értékesítés az adatkezelési tájékoztató három különböző alcímébe is beletartozhat (2.1. A Felhasználó adatai, 2.2. A Felhasználó javára vásárlást teljesítő személy adatai, 2.3. A Bérletekkel kapcsolatos adatok). Ezek esetében a jogalapot a Kötelezett úgy fogalmazta meg, hogy „*a Felhasználó mint adatkezelő által az adattovábbítással adott felhatalmazás*". A Hatóság megállapította, hogy az Infotv. nem tartalmaz olyan jogalapot, amilyet a BKK a tájékoztatóban megjelölt, illetve a jogalap megfogalmazása is ellentétes az Infotv. definícióival, szóhasználatával. Az Infotv. 5-6. §-ai sorolják fel, hogy az adatkezelők milyen jogalapok alkalmazásával végezhetik az adatkezelést.

A Hatóság megállapította, hogy az adatkezelési tájékoztatóban szereplő, a „*Felhasználó* (…) *felhatalmazása*" megfogalmazás az Infotv. 5. § (1) bekezdés a) pontja szerinti, az érintett hozzájárulására utalhat. Ugyanakkor meg kell jegyezni, hogy a Kötelezett szóhasználata e tekintetben is ellentétes az Infotv.-nyel, hiszen az érintett (az adatkezelési tájékoztatóban: Felhasználó) fogalmilag kizárt, hogy adatkezelő is legyen a saját személyes adataival kapcsolatban, illetve az érintett aktív cselekményét, beleegyezését nem lehet „adattovábbításnak" tekinteni, hiszen az Infotv. 3. § 11. pontja arra vonatkozóan egy teljesen más természetű definíciót tartalmaz. A jogalapok között ráadásul az adatkezelési tájékoztató egyáltalán nem tartalmazza az Sztv. 7. §-át, amelyet egyébként válaszlevelében az adatkezelés egyik jogalapjaként jelölt meg, abban csak a tevékenységére vonatkozó jogszabályok között említi az Sztv.-t.

A Hatóság álláspontja alapján egy adatkezelés nem alapulhat egyszerre mind a kettő, az Infotv. 5. § (1) bekezdésében említett jogalapon, hiszen amennyiben jogszabály, jelen esetben az Sztv. egy adott adatkezelésre vonatkozóan kötelezően előírja a kezelendő adatok körét, és az adatkezelés egyéb körülményeit, akkor értelemszerűen kizárt az, hogy az érintett akaratát önkéntesen és határozottan kinyilváníthassa az adatkezeléssel kapcsolatban.[2] Emellett a Hatóság azt is kiemeli, hogy az is gyakran előfordulhat, hogy adatkezelési célonként más az adatkezelés jogalapja. Így például egy online értékesítési tevékenységhez kapcsolódóan az értékesítés teljesítéséhez vagy a szerződés létrejöttéhez kapcsolódó adatkezelés jogszabályi rendelkezésen alapulhat, míg például a regisztráció vagy a felhasználókkal való kapcsolattartással összefüggő adatkezelés az érintett hozzájárulásán.

A Hatóság az eljárás során megállapította, hogy a Kötelezett nem differenciálta az adatkezelését aszerint, hogy definiálja, milyen tevékenységéhez kapcsolódóan milyen adatkezelési célt szükséges meghatároznia, illetve ehhez kapcsolódóan mi az adatkezelés jogalapja. A Hatóság megállapította, hogy ebből a mulasztásból fakadóan a Kötelezett az online jegyértékesítéssel összefüggésben hibásan határozta meg az adatkezelés jogalapját, az adatkezelési tájékoztatóban – az Infotv. definícióival ellentétes megfogalmazással – a hozzájárulást jelölte meg az adatkezelés jogalapjaként.

A Hatóság megállapította, hogy az érintett és a Kötelezett között az Sztv. szerinti, a személyszállítási szolgáltatás alapjául szolgáló szerződés jön létre akkor, amikor az az érintett jegyet vagy bérletet vásárol az online jegyértékesítési rendszeren keresztül. Etekintetben tehát az online jegyértékesítéssel együtt járó adatkezelésre az Infotv. 5. § (1) bekezdés b) pontját és az Sztv. rendelkezéseit kell alkalmazni.

A Kötelezettnek akár az Sztv., akár más jogalap szerint végzett adatkezelés esetében is teljesítenie kell az Infotv. 20. § (2) bekezdésében foglalt előzetes tájékoztatás kötelezettségét, vagyis az

[2] Infotv. 3. § 7. pont

adatkezelés megkezdése előtt az érintettet tájékoztatni kell az adatkezeléssel kapcsolatos minden tényről.

2.2. Az előzetes tájékoztatással kapcsolatos általános követelmények

Az előzetes, megfelelő tájékoztatás az adatkezelés jogszerűségében kiemelt jelentőségű. Az érintettek ezen keresztül ismerhetik meg a személyes adataikra vonatkozó adatkezelést, illetve ezáltal érvényesülhet az érintettek információs önrendelkezési joga: az az adatkezelés lehet jogszerű, amelynek körülményei az érintettek előtt maradéktalanul ismertek.

Az átláthatóság követelménye megjelenik az adatvédelmi irányelv[3] 29. cikke szerint létrehozott Adatvédelmi Munkacsoportnak (a továbbiakban: 29-es Munkacsoport) a hozzájárulás fogalom-meghatározásáról szóló 15/2011. számú Véleményében (a továbbiakban: 15/2011. számú Vélemény), melyben a 29-es Munkacsoport kiemelte, hogy az előzetes tájékoztatás átláthatóságot biztosít az érintett számára, amely átláthatóság az érintetti ellenőrzés gyakorlásának és a hozzájárulás érvényességének egyik feltétele. A Véleményben a 29-es Munkacsoport hangsúlyozza azt is, hogy az érintettnek világos és érthető módon, pontos és teljes körű tájékoztatást kell adni valamennyi releváns kérdésről, például a kezelt adatok természetéről, az adatkezelés céljáról, a lehetséges adattovábbítás címzettjeiről, valamint az érintettek jogairól. Az érintett az előzetes, megfelelő tájékoztatás alapján képes felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára, vagyis a megfelelő tájékoztatáson keresztül ismerheti meg a személyes adataira vonatkozó adatkezelést, és ezáltal érvényesülhet az információs önrendelkezési joga.

Az előzetes, megfelelő tájékoztatás keretében az adatkezelőnek eleget kell tennie az Infotv. 20. §-ában megfogalmazott kötelezettségeknek. A tájékoztatás követelményének központi eleme az Infotv. 20. § (2) bekezdése, amely felsorolja azokat az alapvető adatkezelési körülményeket, amelyekről az adatkezelőnek tájékoztatást kell nyújtania. Ez a bekezdés azonban csak egy példálózó felsorolást tartalmaz, az adatkezelőnek minden olyan körülményről felvilágosítást kell nyújtania, amely az adatkezelés teljes körű megismeréséhez szükséges, és amely alapján az érintett képes felismerni azt, hogy az adatkezelés milyen hatással jár az információs önrendelkezési jogára. Az előzetes tájékoztatásnak emellett alkalmasnak kell lennie arra is, hogy annak alapján az érintettek ellenőrizhessék azt, hogy az adatkezelők mennyiben tartják meg az adatvédelmi követelményeket.

Az adatkezelőnek biztosítania kell a tájékoztatás közérthetőségét. Nem fogadható el az a gyakorlat, hogy a tájékoztatóban az adatkezelő pusztán szó szerint megismétli a jogszabályok szövegét. Az adatkezelési tájékoztató lényege ugyanis az, hogy tájékoztassa az érintetteket arról, hogy az adatkezelő milyen módon tartja meg a jogszabályban foglalt követelményeket. A jogszabályi rendelkezések puszta átvétele számos esetben bonyolulttá és nehézkessé teszi az adatkezelési tájékoztató szövegét. Egy normaszöveg többnyire rövid, tömör szöveg, melynek értelmezéséhez az egész jogszabály, illetve az adott jogterület alapelveinek az ismerete is szükséges. A tájékoztató megszövegezésénél – a jogszabályi szöveget kiindulópontként használva – célszerű tehát az egyes adatkezelési körülményeket rövid, a hétköznapi életben gyakran használt szavakkal körülírni. Az adatkezelőnek kerülnie kell a többszörösen összetett tagmondatból álló, bonyolult, hosszú mondatok használatát. Emellett egy

[3] A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv

összetettebb adatkezelés megértését jelentősen elősegíti az, ha az adatkezelő példákon keresztül mutatja be az adatkezelést.

A tájékoztatásnak világosnak és egyértelműnek kell lennie. Az adatkezelőnek ügyelnie kell arra, hogy a tájékoztató egyes rendelkezéseit egyféle módon lehessen értelmezni, illetve a tájékoztatás alapján az érintett könnyen azonosítani tudja az adatkezelés terjedelmét, a személyes adatokra és a magánszférára gyakorolt hatását.

Ezen túlmenően az adatkezelőnek biztosítania kell a tájékoztató olvashatóságát. A tájékoztatónak ezért strukturáltnak, könnyen áttekinthetőnek kell lenni, amelyet elsődlegesen a szöveg megfelelő szintű tördelésével, felsorolás alkalmazásával lehet elérni.

Az adatkezelési tájékoztatóban, a Hatóság álláspontja szerint, pontokba szedve, legalább az alábbi adatkezelési körülményekre szükséges utalnia az adatkezelőnek:

- az adatkezelő neve, elérhetőségei,
- az adatkezelés célja, a kezelt személyes adatok köre,
- az adatkezelés jogszabályi háttere, jogalapja,
- az adatokon végzett adatkezelési műveletek,
- az adatkezelés időtartama,
- az adatokhoz hozzáférő más állami szervek vagy szervezetek (például más munkáltatók),
- az adatfeldolgozó igénybevétele,
- az adatkezelő által meghozott adatbiztonsági intézkedések (hogyan teljesíti az Infotv. 7. §-ában foglalt követelményeket),
- az érintettet megillető jogok (az Infotv. 14-19. §-a és az Infotv. 21. §-a alapján),
- jogorvoslati lehetőségek.

2.3. A Kötelezett által alkalmazott adatvédelmi tájékoztató hiányosságai

A Hatóság megvizsgálta a Kötelezett által az érintettek rendelkezésére bocsátott adatkezelési tájékoztatót, melyről a Hatóság álláspontja szerint általánosságban elmondható, hogy az nem közérthető, nem egyértelmű, illetve nem könnyen áttekinthető az érintettek számára az alább kifejtett indokok miatt.

Az adatkezelési tájékoztató 2. pontjában – amint azt a Hatóság a határozat 2.1. pontja részletezi – nem megfelelő a jogalapról szóló tájékoztatás, mivel a Kötelezett hibásan a hozzájárulást jelöli meg jogalapként, illetve az adatkezelési tájékoztató megfogalmazása is ellenétes az Infotv. szóhasználatával. A Hatóság álláspontja szerint az adatkezelési tájékoztató tehát nem tartalmaz a jogalapra vonatkozóan egyértelmű tájékoztatást.

A tájékoztató 1.1 pontjában bár meghatározza a „Felhasználó" fogalmát, azonban a későbbiekben ezt az „érintett" fogalma mellett használja, amely azt eredményezi, hogy nem érthető, hogy mely fogalmat pontosan mely személyi körre, milyen jelentéssel alkalmazza.

A Hatóság álláspontja szerint nem érthető például a tájékoztató 1.1. pontjában szereplő mondat, mely szerint *„A BKK az adatok átadásának jogszerűségét (az adatkezelés jogalapjának meglétét) nem vizsgálja, annak biztosítása kizárólag a Felhasználó kötelezettsége. Ennek megfelelően, ha az adatkezelés jogalapja az érintett hozzájárulása, akkor annak beszerzésének kötelezettsége kizárólag a Felhasználót terheli.*" Előzőleg ugyanis a tájékoztató meghatározza, hogy *„a BKK az Online Shopon keresztül történő Bérletek értékesítése során kizárólag a regisztrált felhasználótól (a továbbiakban: Felhasználó) származó személyes adatokat kezeli, közvetlenül az érintettektől*

(regisztrált felhasználóktól) veszi fel az adatokat." Nem világos a tájékoztató szövege alapján az, hogy mit jelent a „Felhasználó" és az „érintett" közötti különbségtétel, hiszen a tájékoztatóban, illetve az eljárás során, maga a Kötelezett nyilatkozott úgy, hogy a személyes adatokat az érintettől szerzi be. A jogalappal kapcsolatban is félrevezető a fent idézett mondat, hiszen az online jegyértékesítési rendszer kapcsán a jogalapot magának a Kötelezettnek – vagyis az adatkezelőnek – kell azonosítania, tehát nem értelmezhető egy olyan mondat, amely ezt másnak a felelősségi körébe utalja. Összességében a tájékoztató 1.1-1.3. pontjai nem egyértelműek, nem világosak, illetve nem tekinthetők közérthetőnek sem.

A Kötelezett az adatkezelési tájékoztató 1.7. alpontjában deklarálja, hogy „*a BKK adatkezelési alapelvei összhangban állnak az adatvédelemmel kapcsolatos hatályos jogszabályokkal*", majd ezt követően példálózó jelleggel kiemel néhány jogszabályt. A Hatóság gyakorlata szerint segítheti az érintettek tájékoztatását az, ha az adatkezelő megjelöli azt, hogy milyen jogszabályok vonatkoznak az adatkezelésre. Ebben az esetben azonban érdemes súlyozni, mely jogszabályoknak van fontos szerepe az adatkezelés megértésében, és mely jogszabályok azok, amelyek csak áttételes szereppel rendelkeznek az adatkezelésre. Így például az adatkezelési tájékoztatóban szerepel Magyarország Alaptörvényének VI. cikke is, amelynek önmagában történő megjelölése elenyésző szereppel bír az adatkezelési tájékoztató megértésében. Ugyancsak kifogásolható az is, hogy a Kötelezett az adatkezelési tájékoztató 1.7. pontjában felsorolja a Polgári Törvénykönyvről szóló 2013. évi V. törvényt, amely több mint másfélezer rendelkezésből álló jogszabály, melynek azonban mindössze néhány rendelkezése tekinthető adatvédelmi szempontból relevánsnak. Ugyanez vonatkozik mind az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényre, mind pedig a számvitelről szóló 2000. évi C. törvényre, amely jogszabályoknak szintén csak néhány rendelkezése bír adatvédelmi jogi relevanciával.

A Hatóság megállapította, hogy a Kötelezett az adatkezelési tájékoztató 1.7. pontjában felsorolt jogszabályok között nem súlyozott aszerint, hogy melyik jogszabály mely rendelkezésének van jelentősége az érintett számára az adatkezelés tényleges megértésében, ami szintén a tájékoztató közérthetősége ellen hat.

Az adatkezelési tájékoztató 2.1.-2.3. pontjai alatt a Kötelezett különböző adatkezelési célokat jelöl meg. Így például a 2.1. alpont alatt négy különböző, egymástól független adatkezelési cél szerepel: „a BKK Online Shop keretében a Bérletek értékesítésére vonatkozó Szerződés megkötése", „a Felhasználó azonosítása", „az online értékesítéshez kapcsolódó cselekmények ellenőrzése", illetve „a Felhasználó könnyebb elérhetősége". Valamennyi adatkezelési cél esetében más-más adatkezelési körülmények állapíthatók meg: eltérő az adatkezelés jogalapja, időtartama és a kezelt adatok köre is. A Kötelezett az adatkezelési tájékoztató 2.1.4. alpontjában ugyanis felsorolja a kezelt adatok körét anélkül, hogy – az Inftov. 4. § (1)-(2) bekezdéséből fakadó kötelezettsége ellenére – egyértelműen meghatározná, mely adatkezelési cél esetében mely személyes adatok kezelése tekintethető elengedhetetlenül szükségesnek.

A Hatóság megállapította azt is, hogy nem elég egyértelmű, milyen személyes adatok, milyen jogalapon végzett, milyen jellegű kezelését jelenti „*az online értékesítéshez kapcsolódó cselekmények ellenőrzése*". Az adatkezelési tájékoztató megfogalmazása nem tekinthető közérthetőnek az érintettek számára, ezen leírásból az érintettek nem ismerik fel azt, hogy a Kötelezett adatkezelése jogszerűnek tekinthető-e.

A Hatóság emellett megállapította azt is, hogy az adatkezelési tájékoztató 2.1.-2.3. alpontjai címeinek elnevezései is aláássák a tájékoztató közérthetőségét, illetve nem biztosítanak megfelelő strukturáltságot. Az egyes címek („A Felhasználó adatai", a „Felhasználó javára vásárlást teljesítő

személyek adatai", „Bérletekkel kapcsolatos adatok") és az alatta található szövegrészek között nincs koherencia, az érintettek nem ismerik fel, hogy milyen adatkezeléseket jelentenek ezek a Kötelezett részéről. Szintén félrevezető a 2.4. pont elnevezése („Egyéb adatkezelések"), mivel tartalmát tekintve egyébként nem további adatkezelési műveleteket, hanem az adatkezeléssel kapcsolatos egyéb információkat tartalmaz.

Problémaként azonosította továbbá a Hatóság, hogy a tájékoztatóban nem szerepel egyértelműen arra vonatkozó információ, hogy a Kötelezett igénybe vesz-e adatfeldolgozót, illetve amennyiben igen, akkor pontosan mely adatfeldolgozót, milyen műveletek elvégzésére. A tájékozató 3.6. pontjában utal egyrészt „együttműködő partnerek"-re, illetve „üzemeltetőre", azonban egyértelműen nem tájékoztatja az érintetteket arról, hogy adatfeldolgozót vesz igénybe, illetve annak kilétéről sem, annak ellenére, hogy az eljárás során tisztázásra került, hogy az online értékesítési rendszer üzemeltetésével adatfeldolgozóként a TSM-et bízta meg.

A Hatóság az adatkezelési tájékoztató 5.1. alpontjával kapcsolatban megállapította, hogy a Kötelezett nem tett eleget az Infotv. által előírt követelményeknek, mivel nem mutatja be, hogy az egyes érintetti jogok mit jelentenek, és milyen módon tudja az érintett a jogait gyakorolni.

A Hatóság az előzetes tájékoztatásról szóló ajánlásában kitért arra, hogy milyen adatvédelmi követelmények állapíthatók meg az érintetti jogokra (Infotv. 14-18. §) vonatkozó előzetes tájékoztatási kötelezettségekkel kapcsolatban. A Hatóság kimondta, hogy az érintetteket az adatkezeléssel összefüggésben megillető jogokról szóló tájékoztatásban az adatkezelőnek ki kell térnie arra, hogy milyen elérhetőségen keresztül tudja a személy a kérelmét benyújtani, és az adatkezelő mennyi időn belül tesz eleget az érintetti kérelemnek. Emellett célszerű kifejteni az egyes érintetti jogok tartalmát is (akár egy példa bemutatásán keresztül), hiszen az egyes jogokat a magánszemélyek az elnevezésük alapján nem biztos, hogy ismerik (például a tiltakozás joga pontosan mire terjed ki). Emellett az adatkezelőnek ki kell térnie az érintetti joggyakorlás egyes sajátosságaira.

A Hatóság az előzetes tájékoztatással kapcsolatban megállapította, hogy a Kötelezett által az érintettek rendelkezésére bocsátott adatkezelési tájékoztató nem tartalmaz az adatkezeléssel kapcsolatos mindent tényt, körülményt, illetve egyes pontokat tekintve nem a valóságnak megfelelő információkat tartalmazza. Emellett a megfogalmazása miatt absztrakt, elvont szöveg, amely az átlagos felhasználók számára nehezen érthető, nem áttekinthető. Ezáltal a Kötelezett az adatkezelésről nem adott megfelelő tájékoztatást az érintettek számára, és ezzel megsértette az Infotv. 20. § (1)-(2) bekezdéseit.

3. Az adatvédelmi incidens – adatbiztonsági követelmények

3.1. Adatvédelmi incidens

A Hatóság a részére a 24.hu hírportál által küldött, valamint az ügyfelektől kapott adatbázisokat manuálisan vizsgálta meg egy több száz elemes mintán keresztül, annak érdekében, hogy megállapítsa, hogy a kiszivárgott adatbázis valóban a Kötelezett által működtetett online jegyértékesítési rendszerből származik.

A 24.hu hírportál által a Hatóságnak megküldött adatbázis 3479 felhasználói e-mail címet tartalmaz, a nagyrészt ABC sorrendbe rendezett, beillesztett listarész láthatóan nem teljes.

Az ügyfelek által átadott felhasználói adatbázis körülbelül 6300 személy adatait tartalmazza, melyben nem található meg teljes mértékben a hírportáltól kapott adatbázis állománya, bizonyos

eltéréseket észlelt ezzel kapcsolatban a Hatóság, amely azonban betudható egyrészt a mintavétel mértékének és módszerének, illetve annak, hogy az eltelt időszakban az érintettek gyakorolhatták a személyes adatok törlésére irányuló érintetti jogaikat.

A Hatóság emellett megvizsgálta, hogy a panaszosok, akik beadványukban úgy nyilatkoztak, hogy regisztráltak, tehát érintettek az online jegyértékesítési rendszer adatkezelése vonatkozásában, megtalálhatóak-e az adatbázisban. Tizenhárom esetben a Hatóság azonosította a 24.hu hírportáltól kapott adatbázisban a bejelentők személyes adatait, így különösen az általuk a regisztráció során megadott e-mail címeket.

A fentiek alapján a Hatóság megállapította, hogy a 24.hu hírportál által a Hatóság részére eljuttatott adatbázis túlnyomó többsége azonosítható a Kötelezett, illetve a TSM által rendelkezésre bocsátott éles adatbázisban. Az adatvédelmi incidens Infotv.-beli meghatározása[4] alapján adatvédelmi incidensnek kell tekinteni különösen a személyes adatokhoz való jogosulatlan hozzáférést.

Az említett hírportál az adatkezelés vonatkozásában harmadik személynek minősül, akinek ismeretlen forrásból kezelésébe került egy adatbázis, amelyről egyértelműen megállapítható, hogy a Kötelezett online jegyértékesítési rendszerének adatbázisából származik, és amely a rendszerben regisztrált több, mint 3000 felhasználó személyes adatait tartalmazza. Ezáltal a Kötelezett által kezelt több, mint 3000 személyes adat vonatkozásában sor került jogosulatlan hozzáférésre.

A Hatóság megállapítását támasztotta alá az is, hogy a Kötelezett az iratbetekintést követően, 2017. szeptember 15-én kelt válaszában úgy nyilatkozott, hogy az iratbetekintés során megállapította, hogy a Hatóság részére a 24.hu hírportál által elküldött adatbázis azonos a Kötelezett online jegyértékesítési rendszerének adatbázisával, vagyis adatvédelmi incidens történt.

A fentiek alapján a Hatóság megállapította, hogy sor került az adatbiztonság olyan sérülésére, amely a Kötelezett által kezelt adatokhoz való jogosulatlan hozzáférést eredményezte, vagyis az Infotv. 3. § 26. pontja szerinti adatvédelmi incidens történt.

Tekintettel arra, hogy a Kötelezettnek az Infotv. 7. §-a szerinti kötelezettséggel kapcsolatos mulasztásai a rendelkezésre álló bizonyítékok alapján is megállapíthatóak, a Hatóság nem tartotta szükségesnek annak részletes vizsgálatát, hogy pontosan mi okozta az adatvédelmi incidens bekövetkezését.

3.2. Az adatbiztonsággal kapcsolatos általános követelmények

Az adatbiztonsággal kapcsolatban a 29-es Munkacsoport 3/2014 számú Véleményében kiemeli annak fontosságát, hogy az adatkezelők proaktívak legyenek és megfelelően tervezzék meg az adatbiztonsági intézkedéseiket. Az adatvédelmi irányelv 17. cikke[5] előírja, hogy az adatkezelőnek megfelelő műszaki és szervezeti intézkedéseket kell tennie, és ezen intézkedéseknek olyan szintű

[4] Infotv. 3. § 26. pont

[5] Az adatvédelmi irányelv 17. cikk (1) bekezdése úgy rendelkezik, hogy „*a tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen. Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének*."

biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás [helyesen: adatkezelés] által jelentett kockázatoknak. A 29-es Munkacsoport véleménye alapján ebből az következik, hogy az adatkezelőnek megfelelő előzetes tervet kell készítenie az adatvédelmi incidensek kezelésére, amelyek biztosítják, hogy gyorsan és hatékonyan reagáljon egy incidensre. Ha az adatbiztonsággal kapcsolatos előírásokat megfelelően teljesítik, vagyis az adatkezelés megkezdése előtt a személyes adatok megsértéséhez kapcsolódó kockázatokat előzetesen tekintetbe veszik és csökkentik, akkor kisebb gyakorisággal következnek be incidensek, és azok enyhébb következménnyel járhatnak az érintettekre nézve. Az adatvédelmi irányelv említett cikkét az Infotv. 7. §-a ülteti át a nemzeti jogba.

A IV. 1. pontban kifejtetteknek megfelelően az adatkezelés vonatkozásában a Kötelezett minősül adatkezelőnek. Következésképpen a Kötelezett köteles biztosítani azt, hogy az Infotv. 7. §-ában előírtakat teljesítse az adott adatkezelés vonatkozásában, vagyis köteles gondoskodni a személyes adatok biztonságáról, illetve amennyiben úgy dönt, hogy adatfeldolgozót vesz igénybe, akkor őt olyan utasításokkal ellátni, amelyek garantálják az adatok biztonságát.

3.3. A Kötelezett adatbiztonsági intézkedései az online jegyértékesítési rendszerrel összefüggő adatkezelés vonatkozásában

3.3.1. A Kötelezett mulasztása az online jegyértékesítési rendszer üzembe helyezése előtt

A Hatóság megállapította, hogy a Kötelezett sem a vizsgálati eljárás során tett nyilatkozatában, sem azt követően nem nevezett meg egyetlen olyan konkrét intézkedést sem, amellyel az adatkezelés tervezése valamint végrehajtása során biztosítja, hogy az adatkezelés megfeleljen az Infotv. 7. §-ában foglalt követelményeknek. Sőt, a vizsgálati eljárás során tett nyilatkozatában arra utalt, hogy az általa megbízott adatfeldolgozónak „van hozzáférése”, tehát van lehetősége ilyen intézkedések meghozatalára.

A Hatóság megvizsgálta a tényállás tisztázása során rendelkezésére bocsátott dokumentumokat, és ilyen, az adatok biztonságát szolgáló intézkedésként azonosította a Kötelezett nyilatkozatában említett, a „BKK Online Shop ügyfélkiszolgálási feladatairól” szóló 3/2017/M/Ük sz. Ügyfélkapcsolati Igazgatói munkautasítást. Ennek „Online Shop háttér rendszeréhez való hozzáférés” elnevezésű 2.1. pontja tartalmaz szabályozást arra nézve, hogy milyen módon kell eljárnia a rendszerhez hozzáféréssel rendelkező munkavállalóknak.

A fenti szabályzaton kívül azonban nem volt megállapítható egyéb olyan intézkedés, amelyet a Kötelezett az online jegyértékesítési rendszer üzembe helyezését megelőzően tett, ilyen intézkedés nem azonosítható sem a Kötelezett nyilatkozatai alapján, sem a rendelkezésre álló bizonyítékok alapján.

A Hatóság álláspontja szerint az online jegyértékesítési rendszer üzembe helyezése előtt, a Kötelezettet terheli valamennyi, az Infotv. 7. §-ában megfogalmazott adatbiztonsági előírás, tekintettel arra, hogy a meg nem kezdett adatkezelés előtt – még mielőtt az érintettek elkezdték volna használni a felületet, és személyes adatokat adtak volna meg az adatkezelő számára – a rendszert fejlesztő TSM még nem minősül sem adatfeldolgozónak, sem adatkezelőnek. A rendszert megrendelő Kötelezett felelőssége tehát az, hogy a TSM által fejlesztett online jegyértékesítési rendszer megfeleljen az Infotv. 7. §-ában megfogalmazott adatbiztonsági kritériumoknak. Ennek megvalósulása érdekében a Kötelezettnek megfelelő módon tesztelnie kellett volna a rendszert adatvédelmi szempontból, az így felismert, például adatbiztonsággal kapcsolatos hibákat a fejlesztővel ki kellett volna javíttatnia, ennek végrehajtását ellenőriznie.

A Kötelezett a Hatóság számára nem tudta igazolni azt, hogy az online értékesítési rendszer átvétele előtt megfelelő módon meggyőződött volna arról, hogy az által átvett rendszer megfelel az Infotv. 7. §-ából fakadó követelményeknek.

A Hatóság álláspontja szerint a rendszer üzembe helyezése, vagyis az adatkezelés megkezdését megelőzően is fennálló hiányosságok vonatkozásában a Kötelezettnek az adatkezelés megtervezése keretében kellett volna észlelni, és megtenni a szükséges intézkedéseket a megszüntetésük érdekében.

A Hatóság a fentiek alapján megállapította, hogy a Kötelezett az adatkezelés megtervezése során nem tette meg azokat a technikai és szervezési intézkedéseket, és nem alakította ki azokat az eljárási szabályokat, amelyek az adatok biztonságát szolgálják, így különösen védik azokat a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. Az ilyen intézkedések hiányát bizonyítja az is (ahogy azt a Hatóság a 3.3.3. alpontban is megállapította), hogy a Kötelezett nem tudta megállapítani azt, hogy az általa végzett adatkezelés vonatkozásában adatvédelmi incidensre került sor, illetve jelen határozat keltéig annak körülményeit, így különösen az érintettekre gyakorolt hatását sem tudta megállapítani. A Kötelezettnek az adatbiztonsági intézkedések körében gondoskodnia kellett volna arról is, hogy megállapítsa az esetleges adatvédelmi incidens bekövetkezésekor alkalmazandó eljárásrendet is, amelyre a Kötelezett nyilatkozatai, valamint rendelkezésre bocsátott dokumentumok alapján nem került sor.

A Hatóság hangsúlyozza, hogy az adatkezelés, tekintettel annak jellegére, így különösen a kezelt adatok körére, valamint arra, hogy egy ilyen online jegyértékesítési rendszerrel összefüggésben potenciálisan több tízezer, akár százezer érintett adatainak kezelésére is sor kerülhet, magas kockázatúnak minősül, amely miatt kiemelt figyelmet kellett volna az adatkezelőnek fordítania arra, hogy az adatkezelés tervezése során megfelelő intézkedéseket hozzon az adatok biztonságának garantálására.

3.3.2. A Kötelezett mulasztása abból fakadóan, hogy nem adott megfelelő adatbiztonsági intézkedésre vonatkozó utasításokat az adatfeldolgozó számára

A Hatóság a tényállás feltárás során tisztázni kívánta, hogy az adatkezelő, vagyis a Kötelezett ellátta-e utasításokkal az adatfeldolgozót az adatok biztonságával kapcsolatban, illetve a közöttük fennálló szerződésben erre kitértek-e.

A Kötelezett a tényállás feltárása során tett nyilatkozataiban a Fő Projektszerződést és annak módosítását jelölte meg olyan dokumentumként, amely rendezi a felek között az adatkezeléssel kapcsolatos kérdéseket, az adatkezeléssel kapcsolatban külön nyilatkozat nem került kiállításra, egyéb megállapodás nem került megkötésre.

A Hatóság megvizsgálta a dokumentumokat, és megállapította, hogy a Fő Projektszerződés és annak mellékletei az online jegyértékesítési rendszerre vonatkozóan nem tartalmaznak konkrét rendelkezéseket, ilyen csupán a 3. számú módosításban jelenik meg. A vizsgált adatkezelésben alkalmazott rendszerre tehát a Fő Projektszerződés 3. számú módosítása és annak mellékletei alkalmazandók. A Hatóság azonban megállapította, hogy a módosítás 2. számú mellékletét képező Műszaki leírásban sem azonosíthatóak konkrét, az adatkezelésre, így különösen az adatok biztonságát szolgáló intézkedésekre vonatkozó utasítások, rendelkezések.

A Hatóság tehát megállapította, hogy a Kötelezett az adatfeldolgozóval kötött szerződésben nem tért ki az adatkezeléssel kapcsolatos kérdésekre, így abban nem rögzítettek adatbiztonsági

előírásokat, követelményeket sem. A Kötelezett a szerződés megkötését követően sem adott utasításokat az általa igénybe vett adatfeldolgozónak az adatbiztonsági intézkedések vonatkozásában.

3.3.3. A Kötelezett mulasztásai az adatvédelmi incidenssel kapcsolatban

A tényállás feltárása során tett nyilatkozatai alapján a Kötelezett a 2017. szeptember 12-i iratbetekintést megelőzően nem tudta megállapítani, hogy történt-e adatvédelmi incidens, így különösen azt, hogy sor került-e az általa kezelt személyes adatokkal kapcsolatban jogosulatlan hozzáférésre.

Nyilatkozatai alapján a Kötelezett az iratbetekintés során megállapította, hogy történt adatvédelmi incidens, azonban az ezzel kapcsolatos belső adatvédelmi felelős által folytatott vizsgálatot nem tudta lezárni, az folyamatban van. A Kötelezett emellett több alkalommal hangsúlyozta, hogy pontos intézkedéseket kidolgozni csak az incidens körülményeinek ismerete mellett lesz lehetősége.

A fentieket támasztja alá az, hogy a Hatóság részére 2017. augusztus 17-én megküldött válaszához mellékelt adatvédelmi incidens nyilvántartás 9. oszlopában – „Adatvédelmi incidens történt (Igen/Nem)" – az a bejegyzés szerepel, hogy „A vizsgálat még folyamatban van". A nyilvántartás későbbi, 2017. szeptember 15-én megküldött, módosított változatában az említett oszlopban az „Igen" szó szerepel, vagyis ebben az időpontban a Kötelezett már adatvédelmi incidensként azonosította a sajtóban megjelent eseményt.

A Kötelezett tehát a Hatóság eljárásában rendelkezésre álló bizonyíték, a hírportál által megküldött adatbázis megtekintését követően volt képes azt felderíteni, hogy az adatbázis, melyhez harmadik személyek jogosulatlanul hozzáfértek, valóban a Kötelezett rendszeréből származik, és ezt követően vonta le azt a következtetést, hogy történt adatvédelmi incidens. Azonban ezt követően sem tudta lezárni az erre vonatkozó, a belső adatvédelmi felelős által folytatott vizsgálatot, továbbra sem tudta megállapítani pontosan az adatvédelmi incidens időpontját, körülményeit, valamint az incidenssel érintett személyes adatok körét, az érintettek számát, illetve a kockázatok csökkentése érdekében szükséges intézkedéseket.

Tekintettel arra, hogy az adatvédelmi incidenssel kapcsolatos vizsgálat, a tűzfal naplóállományának vizsgálatával kapcsolatban általánosságban tett csak nyilatkozatot, azonban a Hatóság felhívása ellenére azt nem részletezte, illetve az erről készült bizonyítékokat sem bocsátotta a Hatóság rendelkezésére, a Hatóság nem tudott azonosítani olyan konkrét intézkedéseket, amelyeket a Kötelezett annak érdekében tett, hogy feltárja az adatvédelmi incidens körülményeit.

A Kötelezett nyilatkozatai alapján az online jegyértékesítési rendszer üzembe helyezését követően az alábbi egyéb intézkedésekre került sor:

- A Kötelezett belső adatvédelmi felelőse az esetleges adatvédelmi incidenssel kapcsolatban 2017. július 27-én vizsgálatot indított, amelynek eredményéről azonban a Kötelezett nem nyilatkozott, mivel még folyamatban van.
- A rendszert ért túlterheléses támadás elhárítása érdekében, mely 2017.07.21. 12:00 órától 2017.07.23. 16:00 óráig tartott a Kötelezett az alábbi intézkedéseket tette:
  - Internet bérelt vonal szolgáltató által biztosított DDOS védelem finomhangolása,
  - a tűzfalon beazonosított sérülékenységet kihasználó támadások kiszűrése,
  - Geoprotection beüzemelése a nem Magyarországról érkező támadások kiszűrése érdekében,

    - a tűzfal mögött található szolgáltatások esetében a felismert sérülékenységek javítása.
- A Kötelezett leállította az online jegyértékesítési rendszert, abba 2017. július 23-át követően nem lehetett regisztrálni. A Kötelezett a Hatóság részére 2017. szeptember 15-én megküldött adatvédelmi incidens nyilvántartásban rögzítette olyan intézkedésként, amelyet az incidens elhárítása érdekében tett.

A Hatóság a fentiek alapján megállapította, hogy a Kötelezett az adatvédelmi incidensekkel kapcsolatosan általánosságban nem alkotott meg előzetesen olyan belső eljárásrendet, szabályzatot, amelynek alkalmazásával egy esetleges incidens feltárható és kezelhető. Az adatbiztonsággal kapcsolatos tervezés és a szükséges intézkedések felismerésének hiányát támasztja alá az is, hogy a Kötelezett által meghozott egyetlen konkrét intézkedés az online rendszer leállítása, vagyis az online értékesítéssel összefüggő további adatkezelések megelőzése volt.

A Kötelezett a konkrét adatvédelmi incidens kapcsán sem járt el kellő körültekintéssel: csak az iratbetekintést követően (2017. szeptember 12.) volt képes annak megállapítására, hogy adatvédelmi incidensre sor került. Az incidens valószínűsített időpontját (2017. július 24.) követően tehát másfél hónap telt el annak azonosításáig, illetve ezt követően annak körülményeit a határozat keltéig sem tárta fel, annak ellenére, hogy viszonylag rövid időszakra eső adatkezelés megvizsgálása lett volna szükséges.

Ebből következően a Hatóság megállapította, hogy a Kötelezett mint adatkezelő nem tett meg mindent annak érdekében, hogy a konkrét adatvédelmi incidens körülményeit, súlyosságát, valamint az érintettekre gyakorolt hatását kivizsgálja, és a szükséges adatbiztonsági intézkedéseket megtegye. A kockázatokat olyan módon csökkentette, hogy az online rendszert leállította, azonban az adatvédelmi incidensről, így különösen annak lehetséges következményeiről nem értesítette az érintetteket, akiknek így sérült az információs önrendelkezési joga.

A Hatóság a fentiek alapján megállapította, hogy a Kötelezett megsértette az Infotv. 7. § (1)-(3) bekezdéseit, mivel nem úgy tervezte meg, illetve hajtotta végre az adatkezelési műveleteket, hogy az érintettek magánszférájának védelmét biztosítsa. Emellett nem tette meg azokat a technikai és szervezési intézkedéseket és nem alakított ki olyan eljárási szabályokat, amelyek a személyes adatok biztonságát garantálják, és biztosítják az érintettek magánszférájának védelmét.

4. A TSM-re vonatkozó megállapítások

Ahogy a Hatóság a IV. 1. pontban megállapította, a Fő projektszerződés és annak módosítása alapján az online jegyértékesítési rendszerrel összefüggésben a TSM szerepe kettős: egyrészt a Kötelezett őt bízta meg a rendszer kifejlesztésével, megalkotásával; másrészt a rendszer üzemeltetését végzi a szerződés alapján az üzembe helyezést követően.

4.1. A rendszer fejlesztése

A rendszer fejlesztése nem jár együtt személyes adatok kezelésével, a TSM azzal kapcsolatos tevékenységére kizárólag a Kötelezett és a TSM közötti szerződés alapján került sor. Nyilvánvalóan a TSM-nek mint fejlesztőnek az információbiztonsági és az adatbiztonsági követelmények és szakmai szabályok alapján kellett a fejlesztést elvégeznie, és ha ez nem, vagy nem megfelelően történt, azért a szerződés keretén belül felelősséggel tartozik. Azonban a Kötelezettnek (mint a szerződés vonatkozásában megrendelő) a rendszer fejlesztése során, illetve átvételekor meg kellett

vizsgálnia, hogy a rendszer megfelel-e a szerződésben foglaltaknak. Ezen felül, tekintettel arra, hogy az adott rendszer használatával adatkezelést tervezett, meg kellett győződnie arról, hogy a rendszer alkalmas-e arra, hogy azzal az Infotv.-nek, így különösen az adatbiztonsági előírásoknak megfelelő adatkezelésre kerüljön sor. A tényállás feltárása során a Kötelezett nem igazolta, hogy ilyen ellenőrzést bármilyen módon elvégzett volna.

A TSM a Hatóságnak megküldte a rendszer üzembe helyezését követően (2017. július 26-án) általa megbízott független tanácsadó társaság által lefolytatott vizsgálatot, és az ennek eredményeként készített jelentést. A jelentés a sérülékenységi és adatszivárgási vizsgálata során feltárt olyan, többek között adatvédelmi sérülékenységeket is, amelyek már a rendszer üzembe helyezésekor fennálltak. Ezeket a hiányosságokat a rendszer átvételekor, vagyis az adatkezelés megkezdése előtt kellett volna feltárnia a Kötelezettnek, illetve a TSM-nek.

A TSM első, a fejlesztéssel kapcsolatos tevékenységével kapcsolatban a fentiek alapján nem állapítható meg jogsértés, mivel a TSM nem adatkezelő és nem is adatfeldolgozó ennek során, a fejlesztésért csak a szerződés keretén belül felelős.

4.2. A rendszer üzemeltetése

A TSM az online jegyértékesítő rendszer által megvalósított adatkezelés vonatkozásában, annak üzemeltetése során a IV. 1. pontban tisztázottak alapján adatfeldolgozónak minősül. Ez azt jelenti, hogy szerződés alapján a Kötelezett megbízásából adatok feldolgozását végzi, és a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Infotv. és az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.[6]

A Hatóság megállapította, hogy a TSM adatfeldolgozói minőségében a Kötelezett által elfogadott, rendszert üzemeltette, melynek során a Kötelezett utasításai alapján köteles eljárni. A Kötelezett mint adatkezelő, az általa tervezett adatkezeléshez igénybe vett adatfeldolgozót köteles lett volna megfelelő utasításokkal ellátni annak érdekében, hogy biztosítsa az adatkezelési műveletek végrehajtása során biztosított legyen az érintettek magánszférája[7].

A TSM tevékenységi köre tehát annak a rendszernek az üzemeltetése, amelyet bár ő maga fejlesztett ki, de azt a Kötelezett mint adatkezelő elfogadott, és amely így a Kötelezett álláspontja szerint megfelel a közöttük létrejött szerződésben foglaltaknak. Ahogy az a 4.1. pontban is kifejtésre került, a TSM által megbízott társaság a vizsgálata során feltárt a rendszerrel kapcsolatos sérülékenységeket, amelyek már az üzembe helyezést megelőzően fennálltak, vagyis nem a TSM adatkezeléssel kapcsolatos tevékenységi körében merültek fel.

Ahogyan arról a TSM is nyilatkozott, „*a jelentésben rögzített sérülékenységek döntő többsége elvileg sem teszi lehetővé az adatok kiszivárgását. Az adatvédelmi szempontból releváns sérülékenységekkel kapcsolatban az E&Y tényleges adatszivárgásra utaló nyomot nem tudott kimutatni*."

A Hatóság a fentiek alapján megállapította, hogy a TSM megfelelő intézkedéseket tett az adatvédelmi incidens körülményeinek feltárása érdekében, melyek alapján nem állapítható meg,

[6] Infotv. 10. § (1) bekezdés
[7] Infotv. 7. § (1) bekezdés

hogy a rendszer üzemeltetése körében felmerülő hiányosság okozta volna az adatvédelmi incidens bekövetkezését.

A fentiek alapján a Hatóság a TSM vonatkozásában jogsértést nem tárt fel, így az adatvédelmi hatósági eljárást a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.) 31. § (1) bekezdés j) pontja alapján etekintetben megszünteti.

V. Alkalmazott szankció és indokolása

A Hatóság a tényállás tisztázása során megállapította, hogy a Kötelezett nem tett eleget az adatalanyokkal szemben fennálló tájékoztatási kötelezettségének, megsértve az Infotv. 20. § (1)-(2) bekezdését; a Kötelezett emellett az adatkezelés vonatkozásában nem megfelelően biztosította a személyes adatok biztonságát, ennek érdekében nem hozott megfelelő intézkedéseket, ezzel megsértette az Infotv. 7. § (1)-(3) bekezdéseit.

A fentiekre tekintettel a Hatóság az Infotv. 61. § (1) bekezdés a) és g) pontja alapján a rendelkező részben foglaltak szerint döntött, és jelen határozatban megállapította a személyes adatok jogellenes kezelését. Felszólította a Kötelezetett arra, hogy az adatkezelési tájékoztatási gyakorlatát az Infotv. rendelkezéseire figyelemmel módosítsa, az adatbiztonság követelményének megsértése miatt tegye meg a szükséges intézkedéseket annak érdekében, hogy az adatvédelmi incidens körülményeit, valószínűsíthető kockázatait feltárja, és ezekről a 2017. július 24. előtti időszakban regisztrált felhasználókat tájékoztassa, illetve a jövőbeli adatkezelések során megfelelően gondoskodjon az adatbiztonsági követelmények teljesítéséről. A Hatóság továbbá a Kötelezettet adatvédelmi bírság megfizetésére is kötelezte. Egyidejűleg az érintettek érdekeinek védelme érdekében az Infotv. 61. § (2) bekezdése alapján elrendelte a határozatnak a Hatóság honlapján történő nyilvánosságra hozatalát.

Az Infotv. 61. § (1) bekezdésének g) pontja értelmében a Hatóság az Infotv. 61. § (3) bekezdése szerinti, százezertől húszmillió forintig terjedő bírság kiszabására jogosult jogellenes adatkezelés megállapítása esetén.

Abban a kérdésben, hogy indokolt-e adatvédelmi bírság kiszabása, a Hatóság az Infotv. 61. § (4) bekezdése alapján mérlegelte az ügy összes körülményét. A Hatóság szükségesnek tartotta a bírság kiszabását, mivel a Kötelezett nem megfelelő tájékoztatás alapján nagyszámú érintett adatát kezeli, valamint megsértette az adatbiztonsági követelményeket.

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

Ennek során figyelembe vette a jogsértéssel érintettek körét: a Kötelezett nyilatkozata alapján 2017. július 24-ig 6315 személy regisztrált a rendszerbe; valamint a Hatóság megállapítása alapján az adatvédelmi incidenssel érintett adatbázis 3479 felhasználó email címét tartalmazza.

A Hatóság szerint a jogsértés súlyos, ennek megállapítása során a következőket vette figyelembe:

- A Kötelezett által elkövetett jogsértés (az adatkezelés jogalapjának hibás meghatározása, az adatkezelési tájékoztató csak részben felelt meg az adatvédelmi követelményeknek, illetve abban kirívó hibák is szerepeltek, az adatkezelés megtervezése több tekintetben is hiányos volt) azt mutatja, hogy a Kötelezett alacsony szinten tudja alkalmazni a tevékenységére vonatkozó jogszabályi és adatvédelmi követelményeket.
- Egy olyan erőforrásokkal rendelkező cég esetében, mint a Kötelezett, illetve egy olyan természetű adatkezelés megkezdése előtt, mint amilyen az online jegyértékesítési rendszer

volt, elvárható lett volna a Kötelezett gondosabb magatartása, az adatkezelés magasabb szintű, gondosabb megtervezése és kivitelezése.
- Különösen amiatt tekinthető súlyosnak a Kötelezett jogsértése, mivel az online jegyértékesítési rendszer a Kötelezett tervei szerint több tízezer, sőt a későbbiekben több százezer érintettet adatainak a kezelésére irányult volna.
- A Kötelezett egy évente több millió utast kiszolgáló, közlekedési közszolgáltató vállalat, amelytől ezért elvárható, hogy kiemelt figyelmet fordítson az adatvédelmi követelmények érvényesítésére.

A Hatóság tekintettel volt a Kötelezett gazdasági helyzetére, piacon betöltött szerepére is: a Kötelezett a 2016-os naptári évben több, mint 89 milliárd forintos árbevételt ért el.

Tekintettel a bírság kiszabásának indokoltságára és a bírság mértékét befolyásoló tényezőkre, a Hatóság bírság összegét 10.000.000 Ft összegben határozta meg. A kiszabott bírság összege az Infotv.-ben meghatározott maximum összeg 50 %-a.

A Ket. 69. § (2) bekezdése alapján az ügyfél az adatok megjelölésével kérheti az iratbetekintési jog korlátozását üzleti és más méltányolható magánérdekének védelmében. A Hatóság a kérelemnek – a körülmények körültekintő mérlegelése alapján – akkor ad helyt, ha az adatok megismerésének hiánya az iratbetekintésre jogosultakat nem akadályozza jogaik gyakorlásában.

Az Infotv. 61. § (2) bekezdése alapján a határozat nyilvánosságra hozatalát az érintettek érdekeinek védelme érdekében rendeli el a Hatóság. A közigazgatási szerv törvénysértést megállapító határozata közérdekű adat, és ebben az esetben a határozat nyilvánosságra hozatalára a Kötelezett azonosító adataival kerül sor.

VI. Eljárási szabályok:

Az Infotv. 61. § (2) bekezdése alapján a határozat Hatóság honlapján történő nyilvánosságra hozatalát a Hatóság az adatalanyok érdekeinek védelme érdekében rendelte el. A közigazgatási szerv törvénysértést megállapító határozata közérdekű adat, és ebben az esetben a határozat nyilvánosságra hozatalára a Kötelezett azonosító adataival kerül sor.

A vitatott adatkezeléssel érintett adatok törlésének, illetve megsemmisítésének tilalmi időszakára vonatkozó tájékoztatás az Infotv. 61. § (5) bekezdésén alapul.

Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 143. § (1) bekezdése értelmében e törvény rendelkezéseit a 2018. január 1-jét követően indult és megismételt eljárásokban kell alkalmazni. Az Ákr. hivatkozott rendelkezésére tekintettel jelen eljárás során a Hatóság a Ket. rendelkezéseit alkalmazta. A határozat a Ket. 71. § (1) bekezdésén és a 72. § (1) bekezdésén alapul, a fellebbezést a Ket. 100. § (1) bekezdés d) pontja zárja ki. E határozat a Ket. 73/A. § (3) bekezdése alapján a közlés napján jogerőre emelkedik.

A határozat nem tanúsítja a Kötelezett által végzett adatkezelés jogszerűségét azon kérdésekben, melyek vizsgálatára az adatvédelmi hatósági eljárás során nem került sor.

A határozat bírósági felülvizsgálatának lehetőségét a Ket. 100. § (2) bekezdése biztosítja, a Fővárosi Törvényszék illetékességét a Közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) 12. § (2) bekezdés a) pontja és a Kp. 13. § (11) bekezdése alapján állapította meg. 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 és a 124. § (5) 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 bírságot a megfelelő számlaszámra megfizetni a pénzforgalom lebonyolításáról szóló 35/2017 (XII.14.) MNB rendelet (a továbbiakban: MNB rendelet) 28. § 2 a) pontjának aa) alpontjában (átutalás), b) pontjának bb) alpontjában (készpénzbefizetés fizetési számlára), c) pontjában (készpénzátutalás) felsorolt fizetési módok formájában lehet.

Az államháztartásról szóló 2011. évi CXCV. törvény 42. § (3) bekezdése szerint „*Törvény eltérő rendelkezése hiányában - a bíróság, ügyészség által kiszabott eljárási bírság és rendbírság kivételével - a jogerősen, illetve véglegesen kiszabott és meg nem fizetett bírság, valamint a meg nem fizetett bírság miatt jogerősen vagy véglegesen kiszabott és meg nem fizetett késedelmi pótlék köztartozásnak minősül, és azt az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 134. §-ában foglaltak szerint, vagy ha az nem az Ákr. hatálya alá tartozó eljárásban került megállapításra, akkor adók módjára kell behajtani.”*

Az Ákr. 143. § (2) bekezdésének a) pontja értelmében a 2018. január 1-jét követően elrendelt végrehatásra is az Ákr. rendelkezéseit kell alkalmazni. Az Ákr. hivatkozott rendelkezésére tekintettel 134. § (1) bekezdése szerint „*a végrehajtást – ha törvény, kormányrendelet vagy önkormányzati hatósági ügyben helyi önkormányzat rendelete másként nem rendelkezik – az állami adóhatóság foganatosítja.”*

Az Ákr. 135. §-a alapján, *„ha a Kötelezett pénzfizetési kötelezettségének határidőben nem tesz eleget, illetve az állam által előlegezett költség után a megelőlegezés időtartamára a jogosultnak a törvényes kamatnak megfelelő mértékű késedelmi pótlékot fizet”.*

A Hatóság az ügyintézési időbe be nem számítandó időszakok figyelembe vételével az ügyintézési határidőt 18 nappal lépte túl, melynek oka a pontos tényállás felderítésének nehézségei, valamint az ügy körülményeinek összetettsége.

A TSM vonatkozásában a Hatóság döntése a Ket. 31. § (1) bekezdés j) pontján alapult.

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

Budapest, 2018. január 22.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár