Az adatkezeléssel összefüggő felelősség egyes kérdései, különös tekintettel az adatvédelmi bírság kiszabásának európai gyakorlatára

Certicky Mário*

Az Európai Unió általános adatvédelmi rendelete (GDPR) a személyes adatok kezelésének szigorú szabályait állapítja meg. Az adatkezelőknek az adatkezelésük során azonban nem csupán a GDPR, hanem a nemzeti szabályozásra és a folyamatosan fejlődő adatvédelmi jogi gyakorlatra is figyelemmel kell lenniük. A szabályozás széttagoltsága nehezíti az adatkezelésre vonatkozó normáknak való megfelelést. Az adatkezelő felelőssége több irányban is felmerülhet, így elkülöníthetjük a magánjogi és közjogi felelősséget. A tanulmány tárgya ez utóbbi körébe tartozó közigazgatási felelősség vizsgálata, amelynek keretében az adatvédelmi bírság kiszabásának elméleti és gyakorlati kérdéseit elemzi. A bírság kiszabásának gyakorlatához az egyes európai adatvédelmi hatóságok által hozott döntések kerülnek bemutatásra és ezekből a levonásra kerülnek a következtetések.
Kulcsszavak: adatvédelem, GDPR, adatvédelmi bírság, adatvédelmi felelősség, felelősség az adatkezelésért.

Certain issues of liability relating to data processing with regard to the practice of imposing data protection fines

The European Union's general data protection regulation ensures a high level of protection of personal data. The data controllers, during their data processing practice, must take into account not only the provisions of the Regulation but also national regulations and evolving data protection practice. Regulatory fragmentation makes it more difficult to comply with data processing standards. The responsibility of the data controller can arise in several directions, first of all, we can separate civil and public liability. The subject of this study is the examination of administrative liability within the scope of the latter, in the framework of which it analyses the theoretical and practical issues of imposing a data protection fine. For the practice of imposing fines, the decisions taken by each European Data Protection Supervisor are presented and conclusions are drawn from them.
Keywords: data protection, GDPR, administrative fine, data protection liability, liability for data processing.

https://doi.org/10.32980/MJSz.2022.5.2195

* Egyetemi tanársegéd. Miskolci Egyetem, Állam- és Jogtudományi Kar, Civilisztikai Tudományok Intézete, Kereskedelmi Jogi Intézeti Tanszék.

1. Bevezetés

Közel három éve, hogy 2018. május 25 napjától alkalmazni kell az Európai Unió általános adatvédelmi rendeletét (a továbbiakban: GDPR vagy Rendelet)[1]. Az alkalmazásra a GDPR hatálya alá tartozó adatkezelőnek több, mint két éve volt (t.i. 2016. május 17 napjától) felkészülni. A Rendelet a személyes adatok védelmére vonatkozó számos garanciális rendelkezést rögzít, mindemellett hangsúlyozza, hogy *„minden alapvető jogot tiszteletben tart, és szem előtt tartja a Chartában elismert és a Szerződésekben rögzített szabadságokat és elveket, különösen a (…) a vállalkozás szabadságához (…) való jogot."*[2] Ennek ellenére számos adatkezelő egyfajta veszélyforrásként tekint a Rendeletre. Tény, hogy a GDPR szigorú követelményeket támaszt a személyes adatok védelme érdekében azok kezelése tekintetében, amelyeknek azonban nem célja az adatkezelő működésének ellehetetlenítése, hanem kizárólag az adatkezelés jogszerű mederbe terelése és az érintett önrendelkezési jogának lehető legszélesebb biztosítása.

A tanulmány célja, hogy röviden felvázolja az adatkezelők adatkezeléssel összefüggésben felmerülő felelősségére vonatkozó szabályozást, különös tekintettel a közjogi felelősségre. Ennek keretében különösen nagy hangsúlyt kap a felelősség megállapítása esetén alkalmazható szankciók rendszerének bemutatása, ezen belül pedig a közigazgatási bírság jellegű szankció, az adatvédelmi bírság kiszabásának elméleti szabályai, valamint a gyakorlati alkalmazása. Az adatvédelmi bírság kiszabásával összefüggésben az Európai Unió egyes tagállamainak adatvédelmi hatóságai által hozott és az Európai Adatvédelmi Testület (a továbbiakban: EDPB) által közzétett döntéseit vizsgálom meg.

A tanulmány második fejezetében az adatvédelmi normák komplex rendszerét vázolom fel. A harmadik fejezetben az adatkezeléssel összefüggésben felmerülő felelősség különböző irányait vizsgálom meg, amely számos jogterületet érinthet, így a polgári jog, a versenyjog, a büntetőjog és közigazgatási jog területét. A felelősség különböző irányai közül a közigazgatási felelősséget szeretném mélyebben vizsgálni, s ezen belül is a szabályozás szankciórendszerét. Az alkalmazható szankciók közül az adatvédelmi bírság kerül górcső alá, amelynek nem csak a jogi szabályozását, hanem a gyakorlatát is megvizsgálom. Ez utóbbi körében a tanulmány lezárásának napjáig az egyes európai adatvédelmi hatóságok által hozott döntéseket vázolom fel.

2. Az adatvédelmi jog „kútfői"

Mielőtt az adatvédelmi bírság kiszabására vonatkozó részletes szabályokat elemezzük, meg kell vizsgálni az adatvédelmi jog forrásait. Az adatkezelésekre vonatkozó szabályok „Alfája és Omegája" a GDPR, amely egy kötelező erejű uniós

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1–88. o.).

[2] Lásd a GDPR (4) preambulumbekezdését.

jogforrás, s amelyet a hatálya alá tartozó adatkezelőknek 2018. május 25. napjától kezdve közvetlenül alkalmazni kell. Hangsúlyozandó, hogy a GDPR rendelkezéseit kizárólag a hatálya alá tartozó adatkezelések esetén, illetve a hatálya alá tartozó adatkezelőknek kell alkalmazniuk. A GDPR hatályának részletes ismertetésétől eltekintve röviden az alábbiak szerint vázolható fel az alkalmazási köre. A Rendeletet *„a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni."*[3] Ez tehát azt jelenti, hogy azon nem automatizált módon (tehát manuálisan) végzett adatkezelések esetén, amely olyan személyes adatokra terjed, amelyet nem kívánnak nyilvántartás részévé tenni, illetve nem is részei nyilvántartásnak, a GDPR nem alkalmazandó.[4] Az azonban nem feltétel, hogy a nyilvántartási rendszer már az adatkezelés idején rendelkezésre álljon, sőt az is feltétel, hogy az adatkezelés folyamán bármikor is nyilvántartási rendszer formát kapjon, a Rendeletet alkalmazni kell abban az eseteben is, ha valamilyen elv alapján az adott személyes adatok rendszerezhetőek.[5] Mindemellett a GDPR számos olyan adatkezelést is kifejezetten felsorol, amelyek nem tartoznak a tárgyi hatálya alá,[6] ilyen pl. többek között a személyes vagy otthoni tevékenység keretében végzett adatkezelések.[7] A tárgyi hatály mellett fontos megvizsgálni a Rendelet területi és egyben személyi hatályát is, amely szerint *„a személyes adatoknak az Unióban tevékenységi hellyel*[8] *rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem."*[9] Ez alapján tehát az unióban tevékenységi hellyel rendelkező adatkezelőknek akkor is alkalmazniuk kell a Rendeletet, ha ténylegesen nem az Unió területén végzik az adatkezelést. E mellett fontos kiemelni a GDPR extraterritoriális hatályát is, amely szerint a Rendelet abban az esetben is alkalmazandó, ha az Unióban tevékenységi hellyel nem

[3] Lásd a GDPR 2. cikk (1) bekezdését.

[4] A nyilvántartási rendszer fogalmát a GDPR 4. cikk 6. pontja állapítja meg, amely szerint *„a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető."*

[5] Jóri András: A Rendelet hatálya, in: *A GDPR magyarázata* (szerk. Jóri András), Budapest, HVG-Orac, 2018, 103. o.

[6] Lásd a GDPR 2. cikk (2) és (3) bekezdéseit.

[7] Értelemszerűen nem minősül otthoni, személyes tevékenységnek, ha a munkavállaló, vagy bármely más módon foglalkoztatott személy a munkáltatója, illetve megbízója érdekkörében eljárva végez valamilyen adatkezeléssel járó tevékenységet. A GDPR példálózóan felsorol néhány személyes adatkezelésnek minősülő tevékenységet [Vö. GDPR (18) preambulumbekezdés], így pl. a személyes célból történő elektronikus levelezés, vagy a mobiltelefonszámok mobiltelefonban történő tárolása. Azonban, ha a mobiltelefonszámok tárolása munkavégzési célból is történik, már nem minősülhet személyes, otthoni adatkezelésnek, hiszen ez esetben már a munkáltató érdekkörében is áll az adatkezelés. Az otthoni és a nem otthoni adatkezelés elhatárolása körében lásd továbbá az Európai Unió Bírósága által a C-25/17. sz. előzetes döntéshozatal tárgyában hozott ítéletet (ún. Jehova-tanúi ügy).

[8] A tevékenységi hely tekintetében a GDPR (22) preambulumbekezdése rögzíti, hogy az *„valamely tevékenység tényleges és valós, tartós jelleget biztosító keretek közötti gyakorlását feltételezi. E keretek jogi formája – legyen szó akár fiókteleprő̈l vagy jogi személyiséggel rendelkező leányvállalatról – e tekintetben nem meghatározó tényező."*

[9] Lásd GDPR 3. cikk (1) bekezdés.

rendelkező adatkezelő az adatkezelési tevékenysége áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.[10] Amennyiben tehát harmadik országban tevékenységi hellyel rendelkező adatkezelő az Unióban is nyújtani szeretné a szolgáltatását, úgy a Rendeletet maradéktalanul be kell tartania.

Az adatkezelésre vonatkozó jogforrások közül másodsorban az egyes nemzeti jogszabályokat kell kiemelni, amelyek szektoriális normákat tartalmaznak, az egyes konkrét adatkezelések tekintetében. E normáktól elvárt követelmény, hogy nem lehet ellentétes a GDPR rendelkezéseivel, kizárólag azzal összehangban állapíthatnak meg szabályokat és csak azokban az esetekben, amelyekre a Rendelet felhatalmazást tartalmaz.[11]

Bár jogi kötőerővel nem rendelkeznek, mégis az adatvédelmi jog gyakorlatát leginkább formáló források az Európai Adatvédelmi Testület iránymutatásai és ajánlásai, amelyek a GDPR egyes rendelkezéseit magyarázzák, illetve az alkalmazásuktól elvárt követelményeket fogalmazzák meg, illetve e normákat töltik meg tartalommal. Annak ellenére, hogy ezek a dokumentumok nem rendelkeznek jogi kötőerővel az egyes döntésekben rendszeresen hivatkoznak azok tartalmára, az abban foglalt elvárt követelményekre. Erre tekintettel az adatkezelőknek figyelemmel kell fordítaniuk az EDPB által elfogadott dokumentumokra, s az adatkezelési gyakorlatukat ennek megfelelően kell kialakítaniuk.

A GDPR (10) preambulumbekezdésében foglaltaknak megfelelően *„a természetes személyeknek a személyes adataik kezeléséhez kapcsolódó alapvető jogai és szabadságai védelmére vonatkozó szabályok következetes és egységes alkalmazását az Unió egész területén biztosítani kell."* Ennek értelmében felmerül a kérdés, hogy az uniós tagállamok adatvédelmi hatóságainak figyelemmel kell-e kísérniük a többi hatóság által ugyanolyan vagy hasonló ügyben hozott döntéseit? Esetleg más tagállam hatóságai által hozott döntések, illetve az egyes döntésekben tett megállapítások szolgálhatnak-e hivatkozási alapként az adott ügyben? Úgy gondolom, hogy kizárólag akkor valósulhat meg a Rendelet egységes alkalmazása, ha nem csak az EDPB ajánlásaira és iránymutatásaira lennének tekintettel az egyes adatvédelmi hatóságok, hanem egymás döntéseire is.[12] Ez nem feltétlenül jelent precedens alapú döntéshozatalt, hanem a GDPR egyes rendelkezéseinek azonos

[10] Lásd GDPR 3. cikk (2) bekezdés.

[11] Ezzel összefüggésben a GDPR (10) preambulumbekezdés tartalmazza, hogy *„A tagállamok számára lehetővé kell tenni, hogy az e rendeletben foglalt szabályok alkalmazását pontosító nemzeti rendelkezéseket tartsanak fenn vagy vezessenek be, ha a személyes adatok kezelésére jogi kötelezettség teljesítéséhez, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges."*

[12] Ezt a megközelítést alátámasztja az adatvédelmi bírság kiszabása tekintetében hozott wp253 számú iránymutatásban foglalt azon javaslat miszerint *„A felügyeleti hatóságok a formális és informális információcsere elősegítése érdekében a rendeletben lefektetett együttműködési mechanizmusok révén együttműködnek egymással és – adott esetben – az Európai Bizottsággal, például munkaértekezletek rendszeres tartása útján. Ez az együttműködés a bírságkiszabási hatáskörök alkalmazásával kapcsolatos tapasztalataikra és gyakorlatukra összpontosít, végső soron a nagyobb egységesség megteremtése érdekében."* Lásd: https://www.naih.hu/files/wp253_hu.pdf [letöltve: 2021. 01. 05.].

értelmezését és alkalmazását, ezáltal az átlátható és előrelátható döntéshozatalt eredményezne valamennyi hatóság munkájában.

Végső soron meg kell említeni azokat a normákat, amelyek nem konkrét adatkezelésre vonatkozó rendelkezéseket írnak elő, hanem olyan magatartást, tevékenységet, amelyek adatkezeléssel járnak. Ilyennek minősülnek pl. a cégek tekintetében előírt nyilvántartási kötelezettségek, illetve egyéb adminisztratív kötelezettségek (pl. jegyzőkönyvek), amelyeket a jogi kötelezettség alapján végezni, vezetni kell. Nem szabad azonban elfelejteni, hogy mindezek során is személyes adatok kezelésére kerül sor, amelyekre alkalmazni kell a GDPR és az egyéb normák előírásait, így pl. ezen adatkezelési folyamat tekintetében is eleget kell tenni a tájékoztatási kötelezettségnek, az adatbiztonsági követelményeknek stb.

Mindezek alapján megállapítható, hogy az adatkezelőnek valamennyi a fentiekben említett kötelező erejű normának maradéktalanul meg kell felelniük, illetve folyamatosan figyelemmel kell kísérniük az adatvédelmi szabályok gyakorlati érvényesülését is. Mindezt be kell építeniük a napi operatív működésbe, hiszen az adatvédelmi megfeleltetésnek folyamatosnak kell Lennie. Ez egy rendkívül nehezen teljesíthető elvárás, amelynek az adatkezelők úgy felelhetnek meg, ha a működésük során folyamatosan igénybe veszik adatvédelmi szakember segítségét.

3. Az adatkezelésért való felelősség és a szankciórendszer

Az adatvédelmi felelősség vizsgálata körében első körben meg kell határozni a felelősség címzettjét. Az adatkezelésért való felelősség körében két személyi kör merülhet fel, az adatkezelő és az adatfeldolgozó. E két személyi kör részletes elhatárolását[13] mellőzve alapvetően úgy különböztethetjük meg őket, hogy adatkezelőnek minősül *„az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.”*[14] Ezzel szemben az a személy, aki az adatkezelő érdekében végzi az adatkezelést adatfeldolgozónak minősül.[15] Tekintettel arra, hogy az adatfeldolgozó az adatkezelő érdekében és utasításai szerint jár el, az adatkezelésért való felelősség elsősorban az adatkezelőt terheli. Az adatkezelő felelősséggel tartozik azért, hogy az adatkezelés teljes mértékben megfelel a vonatkozó jogszabályi előírásoknak. Hangsúlyozni kell, hogy az adatfeldolgozó magatartásáért is az adatkezelő felel, amennyiben az adatkezelő utasításainak megfelelően jár el. Mi több az adatkezelő felelősségi körébe tartozik az is, hogy kizárólag olyan adatfeldolgozót vegyen igénybe, amely biztosítani tudja a GDPR-nak való megfelelést. Mindennek érdekében az adatkezelő és az adatfeldolgozó között a GDPR 28. cikk (3) bekezdésének megfelelően az

[13] Az adatkezelő és az adatfeldolgozó személyének részletes elhatárolása tekintetében lásd az EDPB 7/2020. számú iránymutatását. Lásd: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf [letöltve: 2021. 01. 05.].

[14] Lásd a GDPR 3. cikk (7) bekezdését.

[15] Lásd a GDPR 3. cikk (8) bekezdését.

adatfeldolgozás részleteit rögzítő szerződésnek kell létrejönnie, amelyben a teljes adatfeldolgozási folyamatot részletesen szabályozzák a felek. Nem megfelelő az a gyakorlat, amely szerint a 28. cikk (3) bekezdés a) – h) pontjaiban foglalt rendelkezéseket megismétlik a felek a szerződésükben, hanem ezen rendelkezések mentén adatfeldolgozás specifikusan kell meghatározniuk a konkrét elvárásokat, s jellemzően ezeknek az adatkezelő elvárásainak kellene lennie.

Az adatfeldolgozó önálló felelőssége kizárólag abban az esetben merülhet fel, ha az adatfeldolgozás során birtokába kerülő személyes adatokon olyan adatkezelést végez, amelynek önálló célja van, tehát az adatkezelő utasításától eltér, úgy az ilyen adatfeldolgozót adatkezelőnek kell tekinteni, s így önálló felelősséggel tartozik az adatkezelésért.[16]

Az adatkezelésért való felelősség egy szigorú, objektív felelősségnek minősül, amelyet a GDPR bármely rendelkezésének megsértése megalapozhat. Az adatkezelési szabályok megsértésének számos szankciója lehet[17], amelyeket a felügyeleti hatóság korrekciós hatáskörében[18] eljárva alkalmazhat. Ezek közül a figyelmeztetést és az adatvédelmi bírságot, mint a szankciók két „végletét" szeretném kiemelni. Az adatvédelmi hatóság figyelmeztetésben részesíti az adatkezelőt amennyiben az ügy körülményeire tekintettel azt állapítja meg, hogy a jogsérelem helyreállítása érdekében a figyelmeztetés elegendő, hatékony, a jogsérelemmel arányos és visszatartó erővel is rendelkezik.[19] Amennyiben a hatóság azt állapítja meg, hogy a figyelmeztetés nem elegendő a speciális és a generális prevenció és egyben a represszív célok eléréséhez, úgy adatvédelmi bírságot szabhat ki, amelynek a mértékét diszkréciós jogkörben maga határozza meg.

A GDPR 83. cikke alapján a felügyeleti hatóság az általa lefolytatott vizsgálat során mérlegeli, hogy szükség van-e adatvédelmi bírság kiszabására. A 83. cikk (2) bekezdés számos vizsgálandó körülményt felsorol, amelyet a hatóságnak elsősorban azon kérdés megvizsgálása körében kell figyelembe venni, hogy szükség van-e az adatvédelmi bírság kiszabására, majd másodsorban – ha az első vizsgált kérdésre igenlő választ kap – a bírság mértékének meghatározása során szintén e körülményeket kell megvizsgálnia. Fontos követelmény, hogy minden ügyben az egyedi körülményekre tekintettel kell megállapítania a szankciók alkalmazásának szükségességét, viszont a vonatkozó Iránymutatás is rögzíti, hogy azt el kell kerülni, hogy hasonló ügyekben eltérő korrekciós intézkedést alkalmazzanak a felügyeleti hatóságok.[20] A teljesség igénye nélkül a 83. cikk (2) bekezdés az alábbi

[16] Lásd a GDPR 28. cikk (10) bekezdését.

[17] Ezek többek között reparatív és preventív célú szankciók. Lásd részletesebben: Jóri: i.m. 416. o.

[18] Vö.: GDPR 58. cikk (2) bekezdés.

[19] A magyar adatvédelmi hatóság 2020 végén hozott és közzétett döntésében (lásd: NAIH/2020/3479. számú döntés) a jogsértés jellegére és körülményeire tekintettel hatékonynak és arányosnak ítélte meg a figyelmeztetés alkalmazását. A vizsgált esetben a NAIH megállapította, hogy az adatkezelő megsértett az érintett személyes adatának helyesbítéséhez való jogát, illetve megsértette a GDPR 5. cikk (1) bekezdés d) pontja szerinti pontosság elvét is, amikor az érintett kérelme ellenére a hírlevél küldéséhez alkalmazott adatbázisban nem helyesbítette az érintett e-mail címét és a régi e-mail címére küldött két hírlevelet. A hatóság megállapította, hogy a jogsértés alacsony súlyú, amelyet az adatkezelő gondatlan magatartása okozott, de az eljárásra tekintettel orvosolt, illetve a jogsértés miatt nem merült fel kár.

[20] Lásd a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról szóló Iránymutatást (wp253), https://www.naih.hu/files/wp253_hu.pdf [letöltve: 2021. 01. 05.].

körülményeket veszi figyelembe: i) a jogsértés jellegét, súlyosságát és időtartamát, figyelembe véve a szóban forgó adatkezelés jellegét, körét vagy célját, továbbá azon érintettek számát, akiket a jogsértés érint, valamint az általuk elszenvedett kár mértéket; ii) a jogsértés szándékos vagy gondatlan jellegét; iii) az érintettek által elszenvedett kár enyhítése érdekében tett bármely intézkedést; iv) az adatkezelő vagy az adatfeldolgozó által korábban elkövetett releváns jogsértések;[21] v) a felügyeleti hatósággal a jogsértés orvoslása és a jogsértés esetlegesen negatív hatásainak enyhítése érdekében folytatott együttműködés mértéke; vi) a jogsértés által érintett személyes adatok kategóriái[22] stb.

Az adatvédelmi bírság mértékét befolyásoló további tényező, hogy az adott jogsértés a GDPR 83. cikk (4) vagy (5) bekezdésének hatálya alá eső jogsértésnek minősül. Előbbi körében ugyanis az enyhébb megítélésű, míg utóbbi körébe a komolyabban szankcionálható jogsértések tartoznak. Előbbi esetén a bírság maximális mértéke 10 millió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeg,[23] míg utóbbi esetében 20 millió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeg.[24] Mindkettő esetben irányadó, hogy a két számítás alapján kapott összeg közül a magasabb összeget kell kiszabni. A jelen tanulmányban vizsgált jogesetek kivétel nélkül a második, szigorúbb megítélés alá eső jogsértések közzé tartoznak.

A polgári jogi felelősség[25] tekintetében első körben a GDPR 82. cikk (1) bekezdésében foglalt rendelkezést kell kiemelni, amely szerint a *„minden olyan személy, aki e rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult."*[26] A GDPR elkülöníti az adatkezelő és az adatfeldolgozó kártérítési felelősségére vonatkozó szabályokat. Ez alapján a felelősség elsődlegesen az adatkezelőt terheli. Amennyiben az adatkezelő az adatkezeléshez adatfeldolgozót vesz igénybe, úgy az *„csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be az e rendeletben meghatározott,*

[21] E körben megemlíthető a NAIH/2020/3479. számú döntés (lásd 19. számú lábjegyzet) amelyben a hatóság a jogkövetkezmények alkalmazásának indokolása körében többek között azt is megvizsgálta, hogy az adatkezelővel szemben hozott e már marasztaló döntést. Annak ellenére, hogy az adatkezelőt a hatóság már marasztalta valamely adatkezeléssel összefüggő jogsértésért megállapította, hogy a vizsgált esetben ez a döntés nem releváns.

[22] Ez alapján a jogsértés szigorúbb megítélés alá esik, ha a jogsértéssel érintett személyes adatok a különleges adatok kategóriájába tartoznak. Ennek oka, hogy az ilyen adatok kezelése magasabb kockázatot jelent az adatkezelő részére, így az adatkezelőnek is kiemelt figyelmet kell fordítania, fokozottabb védelemben kell részesítenie azokat.

[23] Vö.: a GDPR 83. cikk (4) bekezdés.

[24] Vö.: a GDPR 83. cikk (5) bekezdés.

[25] Az adatvédelmi és a polgári jogi felelősség részletes összehasonlítása tekintetében lásd pl. Truli, Emmanuela: The General Data Protection Regulation and Civil Liability, in: *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?* (eds.: Mor Bakhoum – Beatriz Conde Gallego – Mark-Oliver Mackenrodt – Gintare Surblyte-Namaviciene), Berlin – Heidelberg, Springer, 2018, 303–329. o. DOI: https://doi.org/10.1007/978-3-662-57646-5_12; Cordeiro, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR, *European Data Protection Law Review (EDPL)*, 5(4), 492–499. o. DOI: https://doi.org/10.1007/978-3-662-57646-5_12

[26] Lásd a GDPR 82. cikk (1) bekezdését.

kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.[27] Ez alapján tehát az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelésért, ha a GDPR 28. cikk (10) bekezdése szerint adatkezelői minőségben jár el. Mind az adatkezelő, mind az adatfeldolgozó tekintetében rögzíti a GDPR, hogy *„az adatkezelő, illetve az adatfeldolgozó mentesül az e cikk (2) bekezdése szerinti felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.* [28] E rendelkezés célja és helyes értelmezése, különösen a felelősség tartalma tekintetében rendkívül kérdéses.[29]

A személyes adatok kezelésével összefüggésben a büntetőjog területét illetően a Büntető törvénykönyv 219. §-ban[30] foglalt „személyes adattal visszaélés" bűncselekménye említhető meg. A bűncselekmény elkövetője bárki lehet, így tekintettel arra, hogy adatkezelői minőségben a természetes személyek is megjelenhetnek, így akár ők, de a vonatkozó jogszabály[31] alapján a jogi személy is lehet bűncselekmény elkövetője.[32]

Említésre méltó a magyar Gazdasági Versenyhivatal által a Facebook Ireland Ltd.-vel szemben hozott marasztaló döntése,[33] amely egyrészről az abban kiszabott bírság összege (t.i. 1,2 milliárd forint volt a büntetés összege) miatt, másrészről adatvédelmi szempontból figyelemre méltó megállapítást tett. A határozat szerint megtévesztő a facebook azon állítása miszerint ingyen nyújtja a fogyasztók részére a szolgáltatását, mivel a fogyasztók tulajdonképpen a személyes adataikkal fizetnek a szolgáltató részére, mert azokat saját bevételszerzési célból felhasználja. Adatvédelmi szempontból az ügy rendkívül érdekes, hiszen egy hatósági döntésben került rögzítésre az egyébként nagyon komoly elméleti kérdéseket és vitákat generáló tétel, miszerint egyrészről a személyes adatok értékkel rendelkeznek, másrészről azokra kvázi „fizetőeszközként" tekinthetünk.

4. Az adatvédelmi bírság kiszabásának európai gyakorlata

A jelen alfejezetben az Európai Adatvédelmi Testület központi honlapján elérhető az egyes európai adatvédelmi hatóságok által hozott olyan döntéseket vizsgáltam meg,

[27] Lásd a GDPR 82. cikk (2) bekezdését.
[28] Lásd a GDPR 82. cikk (3) bekezdését.
[29] Úgy gondolom, hogy a magyar jog tekintetében a Ptk. rendelkezései irányadóak a felelősség alóli mentesülés körében. Azonban annak a kérdése nem egyértelmű, hogy vajon a deliktuális vagy a kontraktuális felelősség szabályait kell-e alkalmazni a felelősség alóli mentesülés esetén.
[30] *"Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva*
a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy
b) az adatok biztonságát szolgáló intézkedést elmulasztja,
vétség miatt egy évig terjedő szabadságvesztéssel büntetendő."
[31] Lásd a jogi személlyel szemben alkalmazható büntetőjogi intézkedésekről szóló 2001. évi CIV. törvényt.
[32] Vö.: a 2001. évi CIV. törvény 2. § (1) bekezdésével.
[33] Lásd a magyar Gazdasági Versenyhivatal VJ/85/2016. számon hozott döntését.

amelyekben adatvédelmi bírság kiszabására került sor.[34] Megjegyzem, a tanulmánynak nem célja valamennyi közzétett döntés bemutatása, sokkal inkább a gyakori adatkezelések tekintetében a hatóságok által feltárt adatvédelmi hiányosságok szemléltetése, mindezt annak érdekében, hogy az olvasó segítséget kapjon az egyes adatkezelési folyamatainak kialakításához.

A döntéseket tárgyuk szerint öt kategóriába soroltam, amelynek legfőbb szempontja a jogsértés természete, jellege volt. Az első kategóriába azon jogsértéseket soroltam, amelyek tekintetében hozott döntésekben a hatóságok az egyes adatvédelmi alapelvek megsértését domborították ki. A jogsértések második csoportjába az érintetti jogok megsértése, míg a harmadik csoportba a jogalap nélkül végzett adatkezelések tekintetében hozott döntéseket soroltam. A negyedik kategóriába azon esetek kerültek, amelyek tárgya az adatvédelmi incidens miatt kiszabott adatvédelmi bírság volt, míg az ötödik csoportba az egyéb olyan jogsértések kerültek, amelyek egyik előző kategóriába sem sorolhatóak be vagy akár több kategóriába is besorolhatóak lennének, viszont fontosnak tartottam megemlíteni, mert a tárgyuk az adatkezelők tevékenységétől függetlenül szinte valamennyi adatkezelőt érintik.

4.1. Az adatkezelés alapelveinek megsértése. A GDPR 5. cikke hat alapelvet rögzít, amelyeknek az egyes adatkezeléseknek maradéktalanul meg kell felelnie. Hangsúlyozandó, hogy valamennyi alapelv azonos megítélés alá esik, azonban az alapelveket érintő jogsértések közül kiemelendő a célhoz kötöttség elvének[35], a jogszerűség, tisztesség és átláthatóság elvének[36], az adattakarékosság elvének[37], valamint az integritás és bizalmas jelleg követelményének[38] megsértésével kapcsolatos esetek. Meg kell jegyezni azonban, hogy alapvetően bármelyik jogsértés egyúttal egy vagy több adatvédelmi alapelvbe ütközőnek is minősül, mi több, valamennyi jogsértés az adatkezelés jogszerűségének alapelvébe ütköző jogsértésnek is minősül.

A 2019-es év végén a berlini adatvédelmi hatóság 14,5 millió eurós bírságot szabott ki a Deutsche Wohnen nevű társasággal szemben a GDPR megsértése miatt. A hatóság megállapította, hogy a társaság olyan archívumban tárolta a bérlőire vonatkozó személyes adatokat, amely nem tette lehetővé a már szükségtelen adatok törlését, ezzel megsértve a célhoz kötöttség és az adattakarékosság elveit.[39]

---

[34] A tanulmány kézirata 2021. január 10. napján került lezárásra, tehát a vizsgálat tárgyát e nappal bezárólag közzétett hatósági döntések képezték.

[35] Lásd a GDPR 5. fejezet (1) bekezdés b) pontját: *„A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon."*

[36] Lásd a GDPR 5. fejezet (1) bekezdés a) pontját *„A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni."*

[37] See Article 5(1)(c) *"personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*

[38] See Article 5(1)(f) *"personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

[39] Lásd: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_hu [letöltve: 2021. 01. 05.].

A Litván Adatvédelmi Hatóság 2020 októberében a Vilnius fővárosi önkormányzatra szabott ki tizenötezer eurós bírságot a GDPR 5. cikk (1) bekezdés d) és f) pontjában foglalt alapelvek megsértése miatt, mivel nem biztosítottak megfelelő technikai és szervezési intézkedéseket az örökbefogadással, különösen az örökbefogadó szülők személyes adataival kapcsolatosan végzett adatkezelés során.[40]

A magyar adatvédelmi hatóság 2020 végén közzétett döntésében[41] megállapította a célhoz kötöttség és az adattakarékosság elvének megsértését, mivel az adatkezelő a telephelyén személy- és vagyonvédelmi célból telepített kamerák közül egy alkalmas volt arra, hogy a munkavállalókat megfigyelje, ezáltal őket ellenőrizze, mindezt a munkavállalók előzetes tájékoztatása nélkül.[42] A NAIH 700.000, - forint adatvédelmi bírságot szabott ki az adatkezelőre, amely során súlyosító körülményként vette figyelembe többek között, hogy az adatkezelővel szemben a hatóság már korábban is állapított meg jogsértést, illetve az adatkezelőtől a piacon betöltött pozíciója miatt fokozottan elvárt a munkahelyi adatkezelésekkel összefüggő adatvédelmi követelményeknek való megfelelés, továbbá a jogsértés hosszabb ideig való fennállását. A határozat alapján felívnám a figyelmet egy fontos megállapításra, miszerint önmagában annak a ténye, hogy az adatkezelő érdek- és felelősségi körében üzemelő kamera alkalmas a munkavállalók megfigyelésére, sérti a célhoz kötöttség elvét, s mivel olyan területet is megfigyel, amelyre nem terjed ki az adatkezelés jogalapja, ezért sérti az adattakarékosság elvét is. A határozat fontos megállapításai közzé tartozik, hogy a kamerás megfigyelés esetén az érintettek tájékoztatása nem általános jelleggel kell, hogy történjen, hanem *[az adatkezelőnek] „minden egyes kamera vonatkozásában pontosan meg kell jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. A munkáltató ezzel tudja igazolni a munkavállalók számára azt, hogy miért tekinthetőszükségesnek az adott terület megfigyelése. Nem fogadható el az a gyakorlat, amikor a munkáltató általánosságban tájékoztatja a munkavállalókat arról, hogy elektronikus megfigyelőrendszert alkalmaz a munkahely területén."* A hatóság ezen megállapítását nagyon fontosnak tartom, különösen azért, mert a gyakorlati tapasztalataim alapján az adatkezelők a kamerás megfigyeléssel végzett adatkezelések tekintetében nem felelnek meg a szabályoknak, különösen az adatkezelés egyedi jellegére tekintettel betartani szükséges szabályoknak. Ez alatt olyan hiányosságokat értek, amelyeket a hatóság a fenti döntésében is hangsúlyozott, nevezetesen, hogy jellemző az általános tartalmú szabályzatok, adatkezelési tájékoztatók alkalmazása az adatkezelés specifikus dokumentumok helyett.

4.2. Az érintetti jogok megsértése. Az adatvédelmi jogsértések egyik legérzékenyebb területe az érintetti jogokkal kapcsolatos, amelyet az is hangsúlyoz,

---

[40] Lásd: https://edpb.europa.eu/news/national-news/2020/lithuanian-dpa-imposes-fine-improperly-processed-personal-data-parents_hu [letöltve: 2021. 01. 05.].

[41] Lásd: NAIH/2020/2729/15. számú döntés.

[42] Tudniillik a GDPR 12. és 13. cikkeivel összhangban a munka törvénykönyvéről szóló 2012. évi I. törvény 9. § (2) bekezdése, illetve a 11/A. § (1) bekezdése szerint is előzetes tájékoztatási kötelezettség terheli a munkáltatót a munkavállalókkal szemben, amelynek írásban kell eleget tennie.

hogy ezek a jogsértések a szigorúbb bírság kategóriába tartoznak. Az alábbiakban ismertetett jogesetekben a leggyakoribb jogsértések az érintett átlátható tájékoztatásához fűződő jogával [GDPR 12-14. cikkek], a hozzáféréshez való jogával [GDPR 15. cikk], valamint az érintett törléshez, populárisabb elnevezésén „elfeledtetéshez" való jogával [GDPR 17. cikk] függtek össze.

A belga adatvédelmi hatóság a Google-el szemben lefolytatott vizsgálat eredményeképpen szabott ki 600.000, - euró összegű bírságot, mivel az adatkezelő elutasította az érintett arra irányuló kérelmét, hogy az adatkezelő által üzemeltett keresőmotorban tegye elérhetetlenné azon az érintett személyére negatív tartalmú linkek elérhetőségét, amelyeket a nevére történő keresés esetén a keresőmotor találatként listáz. A hatóság megállapította, hogy a Google megsértett az érintett elfeledtetéshez való jogát, mivel a linkeket elérhetetlenné kellett volna tennie.[43]

A magyar adatvédelmi hatóság a Raiffeisen Bankkal szemben szabott ki 25 millió forintos bírságot, tekintettel arra, hogy az adatkezelő nem tett eleget a GDPR 12. és 13. cikkben foglalt tájékoztatási kötelezettségének, mivel nem adott megfelelő tájékoztatást a MiFID-kérdőívekben felvett személyes adatok kezeléséről, s mindemellett számos ügyfelére vonatkozó személyes adatot jogalap nélkül kezel.[44] Megjegyzem az adatkezelő jogorvoslati eljárás során kérte a határozat felülvizsgálatát, amely keresetét azonban a Fővárosi Törvényszék elutasított tekintettel arra, hogy mindenben megfelelőnek találta a NAIH döntését.[45] A NAIH egy másik döntésében a Deichmann Kft.-vel szemben lefolytatott adatvédelmi hatósági vizsgálatában állapította meg az érintett jogainak megsértését, amelynek eredményeképpen 20 millió forint adatvédelmi bírságot szabott ki. A hatóság megállapította, hogy az adatkezelő megsértette az érintett hozzáféréshez való jogát és az adatkezelés korlátozásához való jogát, azzal, hogy az adatkezelő nem biztosította a kamerás megfigyelés során rögzített felvételekbe történő betekintést, valamint az érintett kérelmének beérkezését követően nem tett eleget az adatkezelés korlátozására vonatkozó követelménynek sem.[46]

4.3. Felelősség a jogszerűtlen adatkezelésért. Jogszerűtlen adatkezelésnek minősül az olyan adatkezelés, amelynek jogszerűségét az adatkezelő nem tudja igazolni a GDPR 6. cikkében foglalt valamely jogalappal. A többi alfejezetben foglalt jogsértések és a jogalap nélkül végzett adatkezelések között konkrétan az a különbség, hogy a többi jogsértés esetén az adatkezelés jogszerűsége nem vitás, hanem valamely más GDPR-ban foglalt rendelkezést sértő magatartást tanúsít az adatkezelő, ellenben a jelen alfejezetben kifejezetten azon jogsértéseket vizsgálom meg, amelyekben az adatkezelés már eredendően jogszerűtlennek minősült.

Az egyik leggyakrabban előforduló jogalap nélkül végzett adatkezelések miatt lefolytatott hatósági vizsgálatok közzé a közvetlen üzletszerzési célból végzett adatkezelésekkel kapcsolatos ügyek tartoznak. Az Olasz Adatvédelmi Hatóság egy direkt marketing tevékenységet végző vállalatot 27 millió eurós bírsággal sújtott,

[43] Lásd: https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu600000-fine-google-belgium-not-respecting-right-be_hu [letöltve: 2021. 01. 05.].
[44] Lásd a NAIH/2019/3107/7. számú határozatot.
[45] Lásd a Fővárosi Törvényszék 106.K.700.570/2019/24. számú döntése.
[46] Lásd a NAIH/2020/2204/8. számú határozatot.

mivel 2017 és 2019 között több millió érintett részére küldött direkt marketing célú üzeneteket az érintettek hozzájárulása nélkül.[47]

Hasonló esetben folytatott vizsgálatot a Spanyol Adatvédelmi Hatóság (AEPD) a Vodafone Espana vállalattal szemben, amely a saját ügyfelei részére küldött direkt marketing célú SMS üzenetet annak ellenére, hogy az érintettek kérték az adataik törlését. A hatóság megállapította, hogy a vállalat megsértette a GDPR 6. cikke (1) bekezdését és 75.000 eurós bírságot szabott ki.[48] Mindkét említett esetben az érintett hozzájárulása [GDPR 6. cikk (1) bekezdés a) pont] tehette volna jogszerűvé a direkt marketing tevékenységgel összefüggő adatkezelést.

A Norvég Adatvédelmi Hatóság 2020. október végén kicsivel több, mint tizenháromezer eurónak megfelelő norvég korona bírságot szabott ki egy adatkezelőre, amely egy egyéni vállalkozó tekintetében végzett hitelképesség ellenőrzést. Az eset kuriózuma nem önmagában a bírság ténye, hanem azon megállapítás, amelyet a hatóság a döntésében is kidomborít, nevezetesen, hogy az egyéni vállalkozóra vonatkozó adatok személyes adatoknak minősülnek, mivel az egyéni vállalkozás és az azt végző természetes személy közvetlenül azonosulnak, és ez közvetlenül kapcsolódik a tulajdonos magántulajdonához.[49]

A Svéd Adatvédelmi Hatóság 2020. december végén 27,500 eurónak megfelelő svéd korona adatvédelmi bírságot szabott ki egy társasházat üzemelő társaságra, amely jogalap nélkül végzett kamerás megfigyelést az egyik társasház folyosóján. A jogvita tárgyát az képezte, hogy az adatkezelő a folyosón több lakás bejárati ajtaját is megfigyelte, amely így alkalmas volt arra, hogy rögzítse a lakók mozgását. A hatóság megállapította, hogy bár annak ellenére, hogy a társasháznak jogos érdeke áll fenn a kamerák üzemeltetésére, így az adatkezelés a folyosók megfigyelése tekintetében jogszerű, azonban a bejárati ajtók megfigyelése az érintettetek magánszféráját sértő adatkezelést eredményez, így az jogszerűtlen.[50] Az eset tanúsága, hogy az adatkezelő jogos érdeke nem teljes körű, a jogos érdek vizsgálata tekintetében lefolytatott érdekmérlegelése tesztnek arra is ki kell terjednie, hogy mely területek kerülnek megfigyelésre.

4.4. Adatvédelmi incidenssekkel kapcsolatos jogesetek. Az adatkezeléssel összefüggő legnagyobb kockázatot az adatvédelmi incidens bekövetkezésének lehetősége jelenti. A GDPR 4. cikk 12. pontja szerint az adatvédelmi incidens *„a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi."* Az adatkezelőket terhelő alapvető kötelezettségek közzé tartozik az adatvédelmi incidens bekövetkezése esetén az incidens bejelentésének

[47] Lásd: https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_hu [letöltve: 2021. 01. 05.].

[48] Lásd: https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-75000-eur-vodafone_hu [letöltve: 2021. 01. 05.].

[49] Lásd: https://edpb.europa.eu/news/national-news/2020/norwegian-dpa-fines-odin-flissenter-performing-credit-check-sole_hu [letöltve: 2021. 01. 05.].

[50] Lásd: https://edpb.europa.eu/news/national-news/2020/300000-sek-fine-against-housing-company_hu [letöltve: 2021. 01. 05.].

kötelezettsége, amely alapján az adatkezelő – a hatósággal és az érintettel együttműködve – elháríthatja az incidens következményeit.[51] Mindezt megelőzően fontos, hogy az adatkezelő azonosítani tudja az adatvédelmi incidens bekövetkezését, illetve a bekövetkezés esetén felmérje az incidens következményeit. Az adatkezelőknek az adatkezelési folyamatuk kialakítása során előzetesen fel kell mérniük egy adatvédelmi incidens bekövetkezésének lehetséges következményeit, s minden szükséges intézkedést meg kell tenniük annak érdekében, hogy elsősorban az incidenst elkerüljék, azonban olyan intézkedéseket is be kell vezetniük, amelyeket az incidens bekövetkezése esetén a következmények elhárítása érdekében tanúsítaniuk kell. Mindez egy előzetes kockázatfelméréssel és megfelelő önszabályozással megvalósítható. Az alábbiakban néhány adatvédelmi incidenssel kapcsolatos jogesetet vázolok fel.

A hamburgi adatvédelmi biztos (Hamburg Commissioner for Data Protection and Freedom of Information) 35,3 millió eurós bírságot szabott ki a H&M nevű gazdasági társasággal szemben, mivel az adatkezelő a munkavállalói magánéletére vonatkozó személyes adatokat, többek között a magánéleti tevékenységekre, egészségi állapotra, vallási hovatartozásra vonatkozó és egyéb más különleges adatnak minősülő információkat gyűjtött, amelyeket egy elektronikus felhő alapú adatbázisban tárolt.[52] Mindeddig jogalap nélkül végzett, azaz jogosulatlan adatkezelésnek minősült volna az eset, viszont az adatbázis a társaságon belül egy konfigurációs hiba miatt több órán keresztül elérhetővé vált arra nem jogosult személyek részére is. Az eljáró hatóság a GDPR több rendelkezésének megsértése miatt, így a jogalap nélküli adatkezelés és az adatvédelmi incidens bekövetkezése miatt megbírságolta az adatkezelőt. A jogeset tanulsága – mindamellett, hogy a munkáltató által végzett jogosulatlan adatkezelésre rendkívül jó példaként szolgál – mégis az, hogy adatvédelmi incidensnek kell tekinteni azt az esetet is, ha egy adott munkáltatón belül dolgozó személyek részére válnak elérhetővé a személyes adatok úgy, hogy arra a szervezeten belül egyébként nem lennének jogosultak.

A magyar adatvédelmi hatóság 7,5 millió forint mértékű adatvédelmi bírságot szabott ki egy egészségügyi szolgáltatást végző adatkezelővel szemben, mivel az nem tett eleget a GDPR 32. cikk (1) bekezdés b) pontjában,[53] a 33. cikk (1) bekezdésében[54] és a 34. cikk (1) bekezdésében[55] foglalt kötelezettségének. A jogeset tárgya az volt, hogy az adatkezelő honlapjáról nyilvánosan elérhetővé vált az adatkezelő adatbázisa, amelyben az érintettekre vonatkozó körülbelül tizenötezer egészségügyi adatot tároltak, illetve ezek jogosultsággal nem rendelkező személyek

[51] Árvay Viktor: Adatvédelmi incidens, in: *Magyarázat a GDPR-ról* (szerk.: Péterfalvi – Buzás – Révész), Budapest, Wolters Kluwer, 2018, 214. o.

[52] Lásd: https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_hu [letöltve: 2021. 01. 05.].

[53] Amely szerint nem biztosította a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegét, ezáltal nem tett eleget az elvárt adatbiztonsági követelményeknek. , rendelkezésre állását és ellenálló képességét;

[54] Amely szerint nem tett eleget az adatvédelmi incidens bejelentésére vonatkozó kötelezettségének.

[55] Amely szerint nem tett eleget az adatvédelmi incidens bekövetkezésére vonatkozó az érintettek irányában fennálló tájékoztatási kötelezettségének.

részére letölthetőek voltak.[56] Az adatkezelő a döntéssel szemben bírósági felülvizsgálatot kezdeményezett, azonban az adatkezelő keresetét mint alaptalant a Fővárosi Törvényszék elutasította.[57]

Egy másik ügyben a NAIH a Digi Távközlési és Szolgáltató Kft.-vel szemben százmillió forint adatvédelmi bírságot szabott ki, amely a magyar hatósági gyakorlat legmagasabb bírsága.[58] Az ügy lényege az volt, hogy az adatkezelő az elsősorban hibaelhárítási célból létrehozott teszt adatbázist nem törölte, ezáltal cél nélkül kezelte az adatokat, amely lehetővé tette az adatvédelmi incidens bekövetkezését, ugyanis az adatkezelő e mellett egy kilenc éve ismert sérülékenységet nem javított ki, amelynek következtében a tesztadatbázis nyilvánosan hozzáférhetővé vált bárki számára. Az ügy érdekessége, hogy a hibát egy etikus hacker „támadása" alapján tárták fel, s az adatkezelő az adatvédelmi incidens bekövetkezésének felismerését követően a saját bejelentése alapján került sor a hatósági vizsgálat lefolytatására.

A Brit Adatvédelmi Hatóság (ICO) 1,25 millió font adatvédelmi bírságot szabott ki a Ticketmaster UK Ltd. nevű társaságra, miután a vizsgálata során feltárta, hogy az adatkezelő nem tett megfelelő intézkedéseket az ügyféladatok védelme érdekében. Az adatkezelő fizetési rendszerét érintő kibertámadás következtében közel 9,4 millió ügyfél személyes adatait, így a nevüket és a fizetéshez szükséges adatokat (kártya száma, lejárati ideje és a CVV kód) jogosulatlan személyek megszerezték.[59]

4.5. A GDPR egyéb rendelkezéseinek megsértése. Az adatkezelésre vonatkozó szabályok megsértésének ezen kategóriájába azokat a jogeseteket soroltam, amelyekben az adatkezelők a GDPR 32. cikkében foglalt adatbiztonsági követelményeket sértő – főképpen passzív – magatartást tanúsítottak.

A német szövetségi adatvédelmi hatóság közel 10 millió eurós bírságot szabott ki az 1&1 Telecom GmbH elnevezésű telekommunikációs szolgáltatásokat nyújtó társaságra, mivel az nem alkalmazott megfelelő szervezési és technikai intézkedéseket a „hotline" szolgáltatás során kezelt személyes adatok illetéktelen személyek részére történő hozzáférhetővé tétele érdekében. Ennek keretében kiemelte az is, hogy ilyen intézkedésnek minősülne az adatvédelmi tisztviselő kinevezése is, amely kötelezettségnek szintén nem tett eleget az adatkezelő annak ellenére, hogy a GDPR 37. cikk alapján ez kötelező lett volna.[60]

A magyar adatvédelmi hatóság által lefolytatott egyik hatósági eljárásban megállapításra került, hogy a könyvelő irodaként működő adatkezelő nem alkalmazott megfelelő szervezési és technikai intézkedéseket az ügyfélkapuról kinyomtatott ügyfeleire vonatkozó személyes adatokat tartalmazó dokumentumok megőrzése és selejtezése érdekében. A NAIH megállapította, hogy ez a magatartás sérti a GDPR 32. cikk (1) bekezdésében foglalt adatbiztonsági követelményeket és

[56] Lásd a NAIH/2020/952/ számú döntést.
[57] Lásd a Fővárosi Törvényszék 106.K.705.072/2020/6. számú döntése.
[58] Lásd a NAIH/2020/1160/10. számú döntést.
[59] Lásd: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/ [letöltve: 2021. 01. 05.].
[60] Lásd: https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_hu [letöltve: 2021. 01. 05.].

500.000, - Ft. adatvédelmi bírság megfizetésére kötelezte az adatkezelőt.[61] Alapvetően megállapítható, hogy a bírság összege alacsony volt, de a jogeset és a bírság mögött húzódó generális prevenció alapján hangsúlyozandó, hogy az adatkezelőknek nem csupán az elektronikus módon, hanem a papír alapon végzett adatkezelésekre, különösen az iratok tárolására, a selejtezésre, a dokumentumok megsemmisítésére is ugyanolyan figyelmet kell fordítaniuk.

A lengyel adatvédelmi hatóság 2021 elején körülbelül 250.000, - eurónak megfelelő bírságot szabott ki az ID Finance Poland nevű társaságra, amelynél adatvesztés következett be. Ennek oka, hogy az adatkezelés körülményeire tekintettel nem alkalmaztak megfelelő szervezési és technikai intézkedéseket az adatvesztése elkerülése, illetve bekövetkezése esetén a károk elkerülése érdekében.[62]

5. Zárszó

Összességében megállapítható, hogy a GDPR-ban foglalt követelményeknek való megfelelés rendkívül nehéz, de nem megvalósíthatatlan. Ennek eléréséhez az adatkezelőknek javasolt megfelelő szakértelemmel rendelkező személyt igénybe venni, vagy amennyiben az adatkezelő tevékenysége is indokolja javasolt a szervezeten belül külön csoportot létrehozni az adatkezelési kérdések napi szintű figyelemmel kísérése és megoldása érdekében.

Az egyes szervezeteknek rendkívül nagy hangsúlyt kell fektetniük a tevékenységük adatvédelmi előírásoknak való megfeleltetésére, hiszen ennek elmaradása esetén magas összegű bírságra is számíthatnak. Az adatvédelmi bírság potenciális kiszabása kockázatként jelenik meg a szervezetek tevékenységében, amelyet kezelniük kell. E kockázat kezelésére számos módszer megjelent már a gyakorlatban, így pl. vannak olyan szervezetek, amelyek külön alapot hoztak létre a felügyeleti hatóság által esetlegesen kiszabott bírság fedezetére. E mellett a biztosítási piacon megjelentek olyan termékek is, amelyek az adatkezeléssel összefüggő egyes kockázatok fedezetére szolgálnak.

Természetesen a leghatékonyabb módja az adatkezeléssel járó kockázatok csökkentésére, mi több a kockázat annulálására, az adatkezelésre vonatkozó jogszabályoknak való folyamatos és teljes megfelelés.

Irodalomjegyzék

- Árvay Viktor: Adatvédelmi incidens, in: *Magyarázat a GDPR-ról* (szerk.: Péterfalvi – Buzás – Révész), Budapest, Wolters Kluwer, 2018.
- Cordeiro, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR, *European Data Protection Law Review (EDPL)*, 5(4), pp. 492–499. DOI: https://doi.org/10.21552/edpl/2019/4/7

[61] Lásd a NAIH/2020/1137. számú döntést.

[62] Lásd: https://edpb.europa.eu/news/national-news/2021/polish-dpa-id-finance-poland-checking-potential-system-vulnerabilities_hu [letöltve: 2021. 01. 05.].

- Jóri András: A Rendelet hatálya, in: *A GDPR magyarázata* (szerk. Jóri András), Budapest, HVG-Orac, 2018.
- European Data Protection Board: Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Lásd: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf [letöltve: 2021. 01. 05.].
- Truli, Emmanuela: The General Data Protection Regulation and Civil Liability, in: *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?* (eds.: Mor Bakhoum – Beatriz Conde Gallego – Mark-Oliver Mackenrodt – Gintare Surblyte-Namaviciene), Berlin – Heidelberg, Springer, 2018. pp. 303–329. DOI: https://doi.org/10.1007/978-3-662-57646-5_12
- A 29. cikk szerinti adatvédelmi munkacsoport: Iránymutatás a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról (WP 253). Lásd: https://www.naih.hu/files/wp253_hu.pdf [letöltve: 2021. 01. 05.].